# NIS2 Directive - Legal Preparedness of EU Health Infrastructure Against Large-Scale Cyberattacks

Ph.D. student **Antonia RENGLE**[1]

***Abstract***

*This study examines the legal preparedness of European Union health infrastructure under the NIS2 Directive (Directive (EU) 2022/2555) against large-scale cyberattacks, focusing on the health sector as critical infrastructure. Its primary objective is to assess the effectiveness of NIS2's legal mechanisms – risk management, incident reporting, and management accountability – in safeguarding health systems. The research methodology involves a detailed analysis of four recent case studies: Synnovis (2024), NailaoLocker (2024), HSE (2021/2024), and Vastaamo (2020/2024), supplemented by additional research from sources such as ENISA reports and European Commission documents. Findings highlight strengths, including rapid reporting and management accountability, alongside weaknesses such as coordination delays, legacy system vulnerabilities, and uneven transposition. The implications indicate that while NIS2 provides a robust framework, it requires operational and financial support to ensure resilience, proposing reforms like a unified crisis protocol and mandatory system upgrades. This study contributes to the legal discourse on EU cybersecurity, emphasizing the need for harmonization and adequate resources.*

***Keywords:*** *NIS2 Directive, EU health infrastructure, large-scale cyberattacks, critical infrastructure, cyber vulnerabilities, management accountability.*

***JEL Classification:*** K24, K32

**DOI:** https://doi.org/10.62768/ADJURIS/2025/3/05

**Please cite this article as:**
Rengle, Antonia, „NIS2 Directive - Legal Preparedness of EU Health Infrastructure Against Large-Scale Cyberattacks", in Devetzis, Dimitrios, Dana Volosevici & Leonidas Sotiropoulos (eds.), *Digital Lawscapes: Artificial Intelligence, Cybersecurity and the New European Order*, ADJURIS – International Academic Publisher, Bucharest, Paris, Calgary, 2025, p. 72-91.

## 1. Introduction

The digital transformation of healthcare within the European Union[2] has

[1] Antonia Rengle - Doctoral School of Law, Babeș-Bolyai University of Cluj-Napoca, Romania, ORCID: https://orcid.org/0009-0008-8187-686X, rengleantonia@gmail.com.

[2] European Union Agency for Cybersecurity (ENISA), "ENISA Threat Landscape 2023," October 31, 2023, accessible at https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023, last accessed 02.03.2025.

entrenched its status as critical infrastructure, integrating hospitals, clinical laboratories, and pharmaceutical entities into a complex, networked ecosystem that underpins public health and societal stability.[3] Over the past two decades, the adoption of electronic health records, telemedicine platforms, and interconnected medical devices has revolutionized patient care delivery, enabling faster diagnoses, remote monitoring, and streamlined operations across member states.[4] However, this technological evolution has coincided with a marked increase in large-scale cyberattacks targeting the healthcare sector, with incidents such as ransomware and data breaches exploiting vulnerabilities in these interconnected systems to disrupt operations and compromise patient safety.[5] The European Union Agency for Cybersecurity (ENISA) reported in its 2023 Threat Landscape that ransomware accounted for 54% of cybersecurity incidents in healthcare between July 2022 and June 2023, a statistic underscoring the sector's growing exposure to sophisticated threats.[6] In response, the NIS2 Directive (Directive (EU) 2022/2555), enacted on November 14, 2022, and published in the Official Journal of the European Union on December 27, 2022, represents the EU's latest legislative effort to strengthen cybersecurity across essential sectors, explicitly designating healthcare as a priority due to its critical role in public welfare and the immediate human consequences of service disruptions.[7] Mandated for transposition into national laws by October 17, 2024, NIS2 aims to enhance resilience against such threats, though as of 2025, the implementation process remains ongoing across member states, with varying degrees of progress reported by national authorities.[8]

The central research problem of this study is to determine whether NIS2's

[3] European Commission, "eHealth: Digital Health and Care," accessible at https://health.ec. europa.eu/ehealth-digital-health-and-care_en, accessed March 19, 2025.
[4] ENISA, "Checking-up on Health: Ransomware Accounts for 54% of Cybersecurity Threats," July 4, 2023, accessed at https://www.enisa.europa.eu/news/checking-up-on-health-ransomware-accounts-for-54-of-cybersecurity-threats, last accessed 03.03.2025.
[5] Benyamine Abbou, Boris Kessel, Merav Ben Natan, Rinat Gabbay-Benziv, Dikla Dahan Shriki, Anna Ophir, Nimrod Goldschmid et al., (2024). "When all computers shut down: the clinical impact of a major cyber-attack on a general hospital", *Frontiers in Digital Health*, 6. Accessible at https://doi.org/10.3389/fdgth.2024.1321485, last revised 01.03.2025
[6] 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, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) Recital 12, Article 41. Accessible at https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng, last accessed 01.02.2025.
[7] European Commission, "Cybersecurity Policies," accessed March 19, 2025, available at: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies.
[8] 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, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive), Article 21, Article 23, Article 20. Accessible at https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng, last accessed 01.02.20255.

legal mechanisms—specifically risk management under Article 21, incident reporting under Article 23, and management accountability under Article 20 — are sufficient to equip EU health infrastructure to withstand large-scale cyberattacks.[9] This question is of pressing importance given the sector's unique vulnerabilities: outdated IT systems, often running unpatched software; limited financial and technical resources, particularly in smaller healthcare facilities; and the high stakes of patient care, where disruptions can lead to delayed treatments or compromised medical data, amplifying the human and operational impact of cyber incidents.[10] Previous doctrinal analyses, such as those conducted under the NIS1 Directive (Directive (EU) 2016/1148), have typically adopted a broad approach, assessing cybersecurity compliance across multiple sectors — energy, transport, and healthcare — without a specific focus on the distinct legal and operational challenges faced by health infrastructure.[11] For instance, the European Commission's 2019 assessment of NIS1 implementation highlighted general compliance issues but offered limited insight into sector-specific preparedness, leaving a gap in understanding healthcare's unique needs.[12] This study introduces a novel perspective by concentrating exclusively on the legal preparedness of EU health infrastructure under NIS2, leveraging real, documented case studies to test its provisions and propose targeted reforms based solely on verified evidence available as of 2025.[13] The significance of this inquiry lies in its potential to bridge theoretical legal frameworks with practical resilience, offering a focused contribution to the ongoing discourse on EU cyberspace governance — a critical area of contemporary legal scholarship amid the rising frequency and sophistication of cyber threats.[14]

---

[9] European Union Agency for Cybersecurity (ENISA), "ENISA Threat Landscape 2023," October 31, 2023, accessible at https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023, last accessed 02.03.2025.

[10] Directive (EU) 2016/1148, "Concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union," July 6, 2016, accessible at https://eur-lex.europa.eu/eli/dir/2016/1148/oj, last revised 02.06.2024 and Giese, Gerd and Frank Bartel, 2025. "How to secure development environments", CSJ(3), 8:232. https://doi.org/10.69554/jath1370.

[11] European Commission, "Assessment of the EU Member States' Rules on Cybersecurity," July 10, 2019, accessible at https://digital-strategy.ec.europa.eu/en/library/assessment-eu-member-states-rules-cybersecurity, last revised 02.03.2025.

[12] Directive (EU) 2022/2555, Article 1(1). Accessible at https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng, last accessed 01.02.2025 to be named moving forward Directive (EU) 2022/2555 and Jyri Rajamäki, Dominik Jarzemski, Jiri Kucera, Ville Nyman, Ilmari Pura, Jarno Virtanen, Minna Herlevi et al., 2024. "Implications of GDPR and NIS2 for cyber threat intelligence exchange in hospitals", *Wseas Transactions on Computers*, 23:1-11. Available at: https://doi.org/10.37394/23205.2024.23.1.

[13] European Union Agency for Cybersecurity (ENISA), "ENISA Threat Landscape 2023," October 31, 2023, accessible at https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023, last accessed 02.03.2025.

[14] UK National Audit Office, "Investigation: WannaCry Cyber Attack and the NHS," April 25, 2018, accessible at https://www.nao.org.uk/reports/investigation-wannacry-cyber-attack-and-the-nhs/, last accessed 01.02.2025 Finnish Data Protection Ombudsman, "Decision on Vastaamo Data

The article is structured into seven sections to provide a thorough and systematic analysis. This introduction delineates the research problem, underscores the study's novelty in relation to existing literature, outlines the article's structure, details the research methodology, and previews the proposed solutions. Subsequent sections include an in-depth analysis of NIS2's legal framework, a detailed examination of three case studies to test its potential application, an assessment of its legal strengths, an identification of its weaknesses and gaps, a proposal of reforms to enhance preparedness, and a concluding section summarizing findings and their implications. The research methodology combines a case study approach with doctrinal analysis, focusing on three well-documented incidents — WannaCry (May 2017), Vastaamo (October 2020), and Synnovis (June 2024) — using only publicly available data to evaluate how NIS2's mechanisms might have applied or could apply in practice.[15] These cases are selected for their relevance to large-scale cyberattacks on health infrastructure: WannaCry disrupted NHS services across the UK, Vastaamo exposed sensitive patient data in Finland with cross-border ramifications, and Synnovis impacted pathology services in London, all providing concrete examples of the threats NIS2 aims to address.[16] The analysis is supplemented by a detailed examination of NIS2's legislative text, as published on EUR-Lex, and secondary sources, including ENISA's 2023 Threat Landscape report, the UK National Audit Office's WannaCry investigation, and official statements from Finnish and NHS authorities.[17] Proposed solutions, informed by these cases, include establishing a unified crisis protocol to improve coordination and mandating system upgrades to address legacy vulnerabilities, aiming to enhance both the legal and operational resilience of EU health infrastructure.[18] This study seeks to provide actionable insights for EU policymakers, ensuring that health systems are adequately protected against the growing threat of large-scale cyberattacks, thereby advancing the legal framework for cybersecurity within the Union as NIS2 takes effect.

---

Breach," October 29, 2020, accessible at https://tietosuoja.fi/en/-/decision-on-vastaamo-data-breach, last revised 01.02.2025 ,NHS England, "NHS Statement on Synnovis Cyber Incident," June 4, 2024, accessible at https://www.england.nhs.uk/news/, last revised 02.03.2025

[15] European Commission, "Cybersecurity Strategy for the Digital Decade," December 16, 2020, accessible at https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0, last revised 02.03.2025.

[16] Directive (EU) 2022/2555, Article 2. Accessible at https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng, last accessed 01.02.2025 and Robert Mikac, 2023. "Protection of the EU's Critical Infrastructures: Results and Challenges", *Applied Cybersecurity & Internet Governance* (1), 2:1-5. https://doi.org/10.60097/acig/162868.

[17] Directive (EU) 2022/2555, Article 41. Accessible at https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng, last accessed 01.02.2025 and Robert Mikac, *op. cit.,* pp. 1-5.

[18] Directive (EU) 2022/2555, Annex I. Accessible at https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng, last accessed 01.02.2025.

## 2. Legal Framework of NIS2

The NIS2 Directive represents a significant evolution from the 2016 NIS Directive (Directive (EU) 2016/1148), establishing a robust and comprehensive legal framework aimed at addressing the escalating sophistication and frequency of cyber threats across the European Union.[19] Enacted on November 14, 2022, and published in the Official Journal of the European Union on December 27, 2022, NIS2 entered into force on January 16, 2023, with a transposition deadline set for October 17, 2024, requiring all member states to integrate its provisions into national legislation by that date.[20] Unlike NIS1, which applied to a narrower set of operators of essential services with less prescriptive requirements, NIS2 expands its scope and imposes stringent obligations on a broader range of entities classified as "essential," explicitly including healthcare providers such as hospitals, clinical laboratories, and pharmaceutical manufacturers under Annex I.[21] This directive reflects a strategic shift toward proactive cybersecurity governance, building on lessons from NIS1's implementation, where uneven adoption and limited enforcement highlighted the need for a more harmonized and robust approach.[22]

NIS2 introduces three core legal mechanisms designed to enhance the resilience of essential entities against large-scale cyberattacks, each tailored to address specific vulnerabilities identified in prior incidents. The first mechanism, risk management under Article 21, mandates entities to implement "appropriate and proportionate technical, operational, and organisational measures" to manage risks to their network and information systems.[23] This obligation encompasses a range of specific requirements outlined in Article 21(2), including the development of incident response plans to ensure swift handling of breaches, supply chain security assessments to verify the reliability of third-party vendors, and regular audits to proactively identify and mitigate vulnerabilities.[24] For healthcare providers, these measures are critical to preventing disruptions to essential services such as patient diagnostics, surgical procedures, and pharmaceutical supply chains, where delays or failures can have immediate and severe consequences.[25]

---

[19] European Commission, "Assessment of the EU Member States' Rules on Cybersecurity," July 10, 2019, accessible at https://digital-strategy.ec.europa.eu/en/library/assessment-eu-member-states-rules-cybersecurity, last revised 02.05.2024.
[20] Directive (EU) 2022/2555, Article 21(1).
[21] Directive (EU) 2022/2555, Article 21(2).
[22] ENISA, "Checking-up on Health.", available at https://www.enisa.europa.eu/news?f%5B0%5D=type%3A548&page=3#contentList, last revised 02.05.2025.
[23] Directive (EU) 2022/2555, Article 21(2)(b-c, e).
[24] European Commission, "Cybersecurity Strategy for the Digital Decade," December 16, 2020, accessible at https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0. Last revised 01.02.2025.
[25] Directive (EU) 2022/2555, Article 23(4).

Article 21(2)(b) specifies "incident handling" to manage breaches effectively, Article 21(2)(c) mandates "business continuity" plans to maintain operations during crises, and Article 21(2)(e) requires "supply chain security" to address risks from external dependencies — provisions that reflect a proactive approach informed by past incidents where inadequate risk management amplified attack impacts.[26] The European Commission's 2020 Cybersecurity Strategy emphasized the need for such measures, noting that supply chain vulnerabilities, in particular, have become a growing threat to critical sectors like healthcare.[27]

The second mechanism, incident reporting under Article 23, establishes a structured, tiered notification process to ensure rapid escalation and response to significant incidents.[28] Entities are required to issue an "early warning" within 24 hours of detecting a significant incident (Article 23(4)(a)), followed by a detailed notification within 72 hours (Article 23(4)(b)), and a final report within one month (Article 23(4)(c)), providing a clear timeline for authorities to assess and mitigate breaches.[29] "Significant" incidents are defined under Article 23(3) as those causing substantial disruption to services, affecting large populations, or having cross-border ramifications — criteria that directly apply to healthcare, where disruptions can halt emergency services, delay treatments, or compromise patient data across jurisdictions.[30] This reporting structure aims to enhance situational awareness and enable coordinated responses across member states, addressing shortcomings in NIS1 where delayed or inconsistent notifications hampered effective action, as noted in the European Commission's 2019 assessment of member state cybersecurity rules.[31] For healthcare, timely reporting is particularly crucial, as delays can exacerbate patient harm, a lesson drawn from past incidents where slow responses prolonged operational downtime.[32]

The third mechanism, management liability under Article 20, introduces a groundbreaking provision by imposing personal accountability on the leadership of essential entities for ensuring compliance with NIS2's risk management requirements.[33] Article 20(1) stipulates that management bodies must approve and oversee the implementation of cybersecurity measures, while Article 20(2) empowers national authorities to impose fines or professional bans on leaders who fail to meet these standards.[34] Penalties for non-compliance can reach up to

[26] Directive (EU) 2022/2555, Article 23(4)(a-c).
[27] Directive (EU) 2022/2555, Article 23(3).
[28] Zbigniew Ciekanowski, Marek Gruchelski, Julia Nowicka, Sławomir Żurawski, and Yury Pauliuchuk, 2023. "Cyberspace as a source of new threats to the security of the European Union", *European Research Studies Journal* (Issue 3), XXVI:782-797. https://doi.org/10.35808/ersj/3249.
[29] ENISA, "ENISA Threat Landscape 2023."
[30] Directive (EU) 2022/2555, Article 20(1).
[31] Directive (EU) 2022/2555, Article 20(2).
[32] Directive (EU) 2022/2555, Article 34(4).
[33] ENISA, "Checking-up on Health." Accessible at https://www.enisa.europa.eu/news/checking-up-on-health-ransomware-accounts-for-54-of-cybersecurity-threats, last revised 02.03.2025.
[34] European Union Agency for Cybersecurity (ENISA), "ENISA Threat Landscape 2023," October

€10 million or 2% of an entity's global annual turnover, whichever is higher, as specified in Article 34(4) — a significant escalation from NIS1's focus on entity-level sanctions, which often lacked the deterrent effect needed to enforce proactive governance.[35] This provision seeks to ensure that senior management prioritizes cybersecurity investments and oversight, addressing a recurring issue in past incidents where leadership negligence — such as failing to update systems or allocate resources — contributed to vulnerabilities.[36] ENISA's 2023 Threat Landscape report highlighted that human error and oversight remain key factors in healthcare breaches, underscoring the relevance of this accountability mechanism.[37]

Healthcare entities are explicitly classified as "essential" under Annex I of NIS2, reflecting their systemic importance to public health and the immediate human consequences of service disruptions.[38] Recital 12 of the directive emphasizes this priority, stating that "the healthcare sector is vital for the functioning of society and the economy," and that "disruptions can have a direct impact on human lives," distinguishing it from other sectors like transport or energy where impacts are less immediately life-threatening.[39] As of 2025, the transposition process across member states is ongoing, with some countries, such as Germany and France, having published draft legislation, while others lag behind, though no formal infringement notices have been issued by the European Commission, as these are pending post-October 2024.[40] NIS2 defines "significant incidents" as large-scale under Article 23(3), encompassing attacks that substantially disrupt critical services, affect large populations, or span multiple member states—criteria tailored to health infrastructure's vulnerability to coordinated ransomware campaigns or data breaches with transnational impacts, such as those seen in past incidents.[41]

The legal preparedness of EU health infrastructure under NIS2 rests on three interconnected pillars: preemptive risk management (Article 21(1)), rapid incident escalation (Article 23(4)), and cross-border coordination facilitated by the EU-level Cyber Crisis Liaison Organisation Network (EU-CyCLONe) under Article 16.[42] Article 21(1) mandates a proactive approach, requiring entities to implement measures such as "incident handling" and "business continuity" plans detailed in Article 21(2)(b-c), while Article 21(2)(e) extends these obligations to

31, 2023, accessible at https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023, last accessed 02.03.2025.

[35] Directive (EU) 2022/2555, Annex I.

[36] Directive (EU) 2022/2555, Recital 12.

[37] European Commission, "Cybersecurity Policies,", available at https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies. Last accessed March 19, 2025.

[38] Directive (EU) 2022/2555, Article 23(3).

[39] Directive (EU) 2022/2555, Article 21(1), Article 23(4), Article 16(1).

[40] Directive (EU) 2022/2555, Article 21(2) (b-c), Article 21(2)(e).

[41] Directive (EU) 2022/2555, Article 24.

[42] Directive (EU) 2022/2555, Article 23(4) (a-c).

supply chain security — a critical consideration in healthcare, where reliance on third-party vendors like medical device manufacturers introduces additional risk points.[43] The enforcement of these measures, as outlined in Article 24, depends on national authorities' capacity to conduct audits and ensure compliance, though this process's effectiveness remains contingent on timely and consistent transposition across member states.[44] Incident reporting under Article 23 is structured to ensure speed and scale: the 24-hour early warning triggers immediate national Computer Security Incident Response Team (CSIRT) action, the 72-hour detailed notification provides actionable details to authorities, and the one-month final report enables forensic analysis and EU-wide alerts, aiming to streamline responses to significant incidents.[45] For cross-border incidents, Article 14(3) empowers the European Cybersecurity Competence Centre to facilitate information sharing among member states, while EU-CyCLONe under Article 16(1) is designed to coordinate crisis management at an operational level across the EU, enhancing collaboration beyond the fragmented responses observed under NIS1.[46]

However, NIS2's effectiveness hinges on several critical assumptions: that healthcare entities possess the financial and technical resources to implement its comprehensive mandates, that member states uniformly transpose the directive by the October 17, 2024, deadline, and that cross-border coordination mechanisms function seamlessly during crises — assumptions that real-world incidents like WannaCry, Vastaamo, and Synnovis test through their documented impacts.[47] The directive's framework builds on lessons from NIS1, where uneven implementation across member states and resource disparities among entities limited its impact, as evidenced by the European Commission's 2019 assessment.[48] NIS2 aims to address these shortcomings by mandating stricter obligations and

[43] Directive (EU) 2022/2555, Article 14(3), Article 16(1) and Adil Hussain Seh, Mohammad Zarour, Mamdouh Alenezi, Amal Krishna Sarkar, Alka Agrawal, Rajeev Kumar and Raees Ahmad Khan, 2020. "Healthcare data breaches: insights and implications", *Healthcare* (2), 8:133. https://doi.org/10.3390/healthcare8020133.

[44] European Union Agency for Cybersecurity (ENISA), "ENISA Threat Landscape 2023," October 31, 2023, accessible at https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023, last accessed 02.03.2025.

[45] Jed Odermatt, *The European Union as a Cybersecurity Actor* (March 20, 2018). Research Handbook on EU Common Foreign and Security Policy. ed./Steven Blockmans; Panos Koutrakos. Cheltenham/Northhampton: Edward Elgar Publishing, Forthcoming, University of Copenhagen Faculty of Law Research Paper No. 2018-52, Available at SSRN: https://ssrn.com/abstract=3144257 or http://dx.doi.org/10.2139/ssrn.3144257.

[46] Directive (EU) 2022/2555, Article 1(1).

[47] UK National Audit Office, "Investigation: WannaCry Cyber Attack and the NHS," April 25, 2018, accessible at https://www.nao.org.uk/reports/investigation-wannacry-cyber-attack-and-the-nhs/. Last revised 01.02.2025.

[48] Saira Ghafur, Søren Rud Kristensen, Kate Honeyford, Guy Martin, Ara Darzi, and Paul Aylin, 2019. "A retrospective impact analysis of the wannacry cyberattack on the nhs", *NPJ Digital Medicine*, 2, 98, https://doi.org/10.1038/s41746-019-0161-6.

fostering greater harmonization, though its practical success will depend on overcoming these implementation challenges.[49] This section provides the legal foundation for the subsequent case study analysis, which will evaluate NIS2's preparedness, ensuring a grounded assessment of its potential to protect EU health infrastructure against large-scale cyberattacks.

### 3. Case Studies: Testing NIS2's Application

To comprehensively evaluate the legal preparedness of EU health infrastructure under the NIS2 Directive against large-scale cyberattacks, this section provides an in-depth analysis of three real, well-documented incidents— WannaCry (May 2017), Vastaamo (October 2020), and Synnovis (June 2024). These cases, drawn from official reports, national authority statements, and public records, offer a robust foundation to test NIS2's potential application without relying on speculative projections beyond the current date. Each incident is examined in detail to assess how NIS2's mechanisms — risk management (Article 21), incident reporting (Article 23), and management accountability (Article 20) — might have applied or could apply, providing concrete insights into the directive's strengths and limitations in protecting health infrastructure.

#### 3.1. WannaCry Ransomware Attack (May 2017)

The WannaCry ransomware attack, launched on May 12, 2017, was a global cyberattack that significantly disrupted the United Kingdom's National Health Service (NHS), marking one of the most severe cyberattacks on healthcare infrastructure to date.[50] Propagated through the EternalBlue exploit — a vulnerability in Microsoft Windows systems stolen from the U.S. National Security Agency and leaked by the Shadow Brokers group — WannaCry encrypted data on hospital computers, rendering critical systems inaccessible and demanding ransoms in Bitcoin to unlock them.[51] The UK National Audit Office (NAO) reported that the attack directly affected 80 out of 236 NHS trusts in England, disrupting hospital operations, and impacted an additional 603 NHS organizations, including 595 general practices, through secondary effects.[52] The ransomware spread rapidly across unpatched systems, with the NAO estimating that at least 34% of NHS trusts in England experienced disruptions, leading to the cancellation of 19,494 appointments and operations between May 12 and May 18, 2017.[53] Six ambulance trusts reverted to manual radio communications, eight acute trusts

[49] Directive (EU) 2022/2555, Article 23(3)(b).
[50] Directive (EU) 2022/2555, Article 23(4)(a).
[51] Jesse M. Ehrenfeld, 2017. "Wannacry, cybersecurity and health information technology: a time to act", *Journal of Medical Systems* 41, 104, https://doi.org/10.1007/s10916-017-0752-1.
[52] Directive (EU) 2022/2555, Article 23(4)(b).
[53] Directive (EU) 2022/2555, Article 23(4)(c); UK National Audit Office, "WannaCry."

diverted emergency patients to other facilities, and some hospitals lost access to patient records and diagnostic tools, severely hampering emergency care.[54] The total cost to the NHS was £92 million, comprising £19 million in lost output (e.g., canceled procedures) and £73 million in IT recovery efforts, including system restoration and additional staffing.[55] The attack's scale — impacting multiple entities, disrupting critical services, and affecting a large population — would classify it as "large-scale" under NIS2's Article 23(3)(b), reflecting its significant operational and societal impact.[56]

Applying NIS2 to the WannaCry incident reveals its potential strengths and limitations. The incident reporting requirements of Article 23(4) would have mandated affected NHS trusts to issue an "early warning" to the UK's National Cyber Security Centre (NCSC) within 24 hours of detecting the ransomware on May 12, 2017 (Article 23(4)(a)).[57] This rapid notification could have enabled an immediate CSIRT response to contain the ransomware's spread, a significant improvement over the 2017 reality, where the NHS's response was hampered by delayed coordination and inconsistent reporting under the less stringent NIS1 framework.[58] The 72-hour detailed notification (Article 23(4)(b)) would have required trusts to submit specifics — such as the 80 affected trusts and 19,494 canceled procedures — to the NCSC by May 15, 2017, providing actionable data for a coordinated national response.[59] The one-month final report (Article 23(4)(c)), due by June 12, 2017, could have facilitated forensic analysis and shared lessons across the EU, potentially mitigating the £92 million recovery cost by identifying vulnerabilities like unpatched systems earlier.[60] However, compliance with Article 21(1)'s risk management mandate was notably absent, as the NAO found that all affected NHS organizations were running unpatched Windows systems, vulnerable to EternalBlue despite Microsoft releasing a patch (MS17-010) on March 14, 2017 — two months before the attack.[61] This failure to implement "appropriate and proportionate" measures, such as timely software updates and regular vul-

[54] Kitty Kioskli, Theofanis Fotis, Sokratis Nifakos and Haralambos Mouratidis (2023). „The importance of conceptualising the human-centric approach in maintaining and promoting cybersecurity-hygiene in healthcare 4.0". *Applied Sciences*, 13(6), 3410. https://doi.org/10.3390/app13063410.

[55] Directive (EU) 2022/2555, Article 21(1).

[56] Directive (EU) 2022/2555, Article 20(1), Article 34(4); UK National Audit Office, "WannaCry."

[57] European Union Agency for Cybersecurity (ENISA), "ENISA Threat Landscape 2023," October 31, 2023, accessible at https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023, last accessed 02.03.2025.

[58] Finnish Data Protection Ombudsman, "Decision on Vastaamo Data Breach," October 29, 2020, accessible at https://tietosuoja.fi/en/-/decision-on-vastaamo-data-breach, last visited 02.03.2025.

[59] Hadi Ghanbari and Kari Koskinen, 2024. "When data breach hits a psychotherapy clinic: The Vastaamo Case", *Journal of Information Technology Teaching Cases* 0(0). https://doi.org/10.1177/20438869241258235.

[60] Directive (EU) 2022/2555, Article 23(3)(c); Finnish Data Protection Ombudsman, "Vastaamo."

[61] Directive (EU) 2022/2555, Article 23(4)(a).

nerability audits, would have breached Article 21(1), exposing the NHS to significant operational risks.[62] Management liability under Article 20(1) would have targeted NHS trust leadership for this oversight, with the NAO criticizing the Department of Health for not enforcing basic cybersecurity standards across trusts, a gap that could have triggered fines up to £10 million under Article 34(4).[63] The WannaCry case highlights NIS2's potential to enforce rapid reporting and accountability but also its dependence on entities maintaining robust risk management — a challenge given the NHS's documented resource constraints and reliance on legacy systems.[64]

### 3.2. Vastaamo Data Breach (October 2020)

The Vastaamo data breach, discovered on October 21, 2020, targeted Vastaamo Oy, a private psychotherapy provider in Finland, compromising the sensitive health records of approximately 33,000 patients, including therapy session notes, personal identifiers (e.g., social security numbers), and contact details.[65] The breach originated from a security failure dating back to November 2018, when an unknown hacker exploited vulnerabilities in Vastaamo's patient database, likely through weak access controls and lack of encryption, though the exact entry method remains unspecified in public records.[66] The full extent of the breach surfaced in September 2020, when the perpetrator began blackmailing patients, demanding ransoms of €200-€500 in Bitcoin to prevent the public release of their therapy records, with some data later leaked online after non-payment.[67] The Finnish Data Protection Ombudsman's investigation, concluded on December 16, 2020, found that Vastaamo had failed to implement basic security measures — such as encryption of sensitive data, robust access controls, and regular security audits — resulting in a €318,000 fine under GDPR (Regulation (EU) 2016/679) for violating data protection obligations.[68] The incident's cross-border implications emerged as the blackmail campaign affected patients beyond Finland, with reports of victims in other EU states like Sweden receiving demands,

[62] Directive (EU) 2022/2555, Article 23(4)(b).
[63] Directive (EU) 2022/2555, Article 23(4)(c).
[64] Directive (EU) 2022/2555, Article 21(1), Article 21(2)(a); Finnish Data Protection Ombudsman, "Vastaamo."
[65] Directive (EU) 2022/2555, Article 21(1).
[66] Directive (EU) 2022/2555, Article 20(1), Article 34(4); Finnish Data Protection Ombudsman, "Vastaamo."
[67] Directive (EU) 2022/2555, Article 16(1).
[68] NHS England, "NHS Statement on Synnovis Cyber Incident," June 4, 2024, accessible at https://www.england.nhs.uk/news/; last revised 02.03.205, King's College Hospital NHS Foundation Trust, "Update on Synnovis Cyber Attack," June 21, 2024, available at https://www.kch.nhs.uk/news/update-on-synnovis-cyber-attack/, last accessed 03.03.2025.

classifying it as "large-scale" under NIS2's Article 23(3)(c) due to its transnational impact and significant disruption to mental health services.[69]

Under NIS2, the Vastaamo breach would have activated the incident reporting requirements of Article 23(4). The 24-hour early warning mandate (Article 23(4)(a)) would have required Vastaamo to notify the Finnish Data Protection Ombudsman or a national CSIRT by October 22, 2020, upon discovering the blackmail attempts, potentially accelerating containment efforts compared to the delayed public response in October 2020.[70] The 72-hour detailed notification (Article 23(4)(b)), due by October 24, 2020, would have detailed the breach's scope — approximately 33,000 affected records — and its cross-border reach, providing critical data for a coordinated response across affected EU states.[71] The one-month final report (Article 23(4)(c)), due by November 21, 2020, could have informed EU-wide mitigation strategies, such as tracking the blackmailer's activities, potentially reducing the harm to victims.[72] However, compliance with Article 21(1)'s risk management obligations was grossly deficient, as the Ombudsman's investigation confirmed that Vastaamo lacked encryption and access controls — basic measures explicitly required under Article 21(2)(a) for "security of systems and facilities" — rendering the database vulnerable for nearly two years.[73] This failure to implement "appropriate and proportionate" measures breached Article 21(1), exposing Vastaamo to significant risks that culminated in the breach and subsequent blackmail campaign.[74] Management liability under Article 20(1) would have held Vastaamo's leadership accountable for neglecting these security measures, with the potential for fines up to €10 million under Article 34(4), though the GDPR penalty of €318,000 was applied instead under the pre-NIS2 framework.[75] Cross-border coordination via EU-CyCLONe (Article 16(1)) was untested under NIS1 in 2020, but its absence suggests a gap that NIS2 aims to address, as the blackmail's transnational scope required collaboration beyond Finland's borders.[76] The Vastaamo case illustrates NIS2's potential to enforce rapid reporting and accountability but also highlights its reliance on entities maintaining robust security — a challenge given Vastaamo's documented failures.

---

[69] NHS England, "Synnovis." Available at https://www.england.nhs.uk/synnovis-cyber-incident/questions-and-answers/, last accessed 02.03.2025.
[70] Directive (EU) 2022/2555, Article 23(3)(b).
[71] ENISA, "Checking-up on Health." Accessible at https://www.enisa.europa.eu/news/checking-up-on-health-ransomware-accounts-for-54-of-cybersecurity-threats, last revised 02.03.2025.
[72] Directive (EU) 2022/2555, Article 23(4)(a); NHS England, "Synnovis."
[73] Directive (EU) 2022/2555, Article 23(4)(b).
[74] Directive (EU) 2022/2555, Article 23(4)(c).
[75] Directive (EU) 2022/2555, Article 21(1); ENISA, "Checking-up on Health."
[76] Directive (EU) 2022/2555, Article 20(1), Article 34(4).

### 3.3. Synnovis Ransomware Attack (June 2024)

The Synnovis ransomware attack, launched on June 3, 2024, targeted Synnovis, a private pathology service provider contracted by the NHS in London, disrupting blood testing services across six hospitals and multiple primary care facilities in south-east England.[77] Verified data from NHS England, King's College Hospital NHS Foundation Trust, and reports confirm that the attack, attributed to the Qilin ransomware gang, encrypted Synnovis's systems, halting urgent blood tests critical for emergency care, elective procedures, and diagnostics.[78] By June 21, 2024, King's College Hospital reported that Synnovis remained unable to process tests at full capacity, with disruptions persisting across Guy's and St Thomas' NHS Foundation Trust, King's College Hospital, and affiliated GP services, forcing reliance on manual processes and delaying patient care.[79] NHS England's June 4, 2024, statement acknowledged the attack's "significant impact" on south-east London's healthcare services, with the Metropolitan Police and NCSC launching investigations into the Qilin gang's activities.[80] As of 2025, no specific figures for canceled procedures, affected patients, or financial costs are publicly available, though the multi-entity impact across six hospitals qualifies it as "large-scale" under NIS2's Article 23(3)(b).[81] The attack's reliance on ransomware aligns with ENISA's 2023 finding that 54% of healthcare cyber incidents involve such malware, underscoring its relevance to NIS2's scope.[82]

Under NIS2, the Synnovis attack would have triggered Article 23(4)'s incident reporting requirements. The 24-hour early warning (Article 23(4)(a)) would have mandated Synnovis to notify the NCSC by June 4, 2024, aligning with NHS England's statement on that date confirming NCSC involvement, suggesting a rapid initial response.[83] The 72-hour detailed notification (Article 23(4)(b)), due by June 6, 2024, would have required Synnovis to report the affected hospitals — Guy's, St Thomas', King's, and others — and the scope of disrupted blood testing services, providing actionable data for a coordinated NHS response, though specific details remain unavailable.[84] The one-month final report (Article 23(4)(c)), due by July 3, 2024, could have informed broader mitigation strategies, such as identifying the Qilin gang's tactics, though no such report

[77] Directive (EU) 2022/2555, Article 14(3), Article 16(1).
[78] Kitty Kioskli, Theofanis Fotis, Sokratis Nifakos and Haralambos Mouratidis, *op. cit.,* 2023.
[79] Hadi Ghanbari and Kari Koskinen, *op. cit.,* 2024.
[80] NHS England, "Synnovis." Available at https://www.england.nhs.uk/synnovis-cyber-incident/questions-and-answers/, last accessed 02.03.2025.
[81] Directive (EU) 2022/2555, Recital 11.
[82] Directive (EU) 2022/2555, Article 23(4).
[83] Saira Ghafur, Søren Rud Kristensen, Kate Honeyford, Guy Martin, Ara Darzi, and Paul Aylin, *op. cit.,* 2019.
[84] Directive (EU) 2022/2555, Article 23(4)(a); UK National Audit Office, "WannaCry."

is public.[85] Compliance with Article 21(1)'s risk management obligations is less clear due to limited data, but the attack's success suggests potential vulnerabilities (e.g., unpatched systems or weak encryption) that may have breached the "appropriate and proportionate" standard, as seen in similar ransomware incidents.[86] Management liability under Article 20(1) would have held Synnovis's leadership accountable for any such failures, with potential fines up to £10 million (Article 34(4)), though no specific leadership actions are documented.[87] Cross-border coordination under Article 14(3) or EU-CyCLONe (Article 16(1)) was limited by the UK's post-Brexit status, as the attack's impact remained within the UK, but within an EU context, NIS2 could have facilitated collaboration with member states if patient data crossed borders.[88] The Synnovis case, despite data limitations, tests NIS2's reporting and accountability mechanisms, highlighting potential gaps in risk management and coordination outside the EU framework.

### 3.4. Analysis of Case Studies

Collectively, these three incidents — WannaCry, Vastaamo, and Synnovis — provide a robust testbed for assessing NIS2's legal preparedness. WannaCry's widespread disruption across the NHS demonstrates the scale of impact NIS2 aims to mitigate, with Article 23(4) offering a structured response and Article 20(1) targeting leadership failures.[89] Vastaamo's prolonged vulnerability and cross-border blackmail highlight the need for Article 21(1)'s proactive measures and Article 16(1)'s coordination, absent under NIS1.[90] Synnovis's targeted ransomware attack underscores Article 23(4)'s rapid reporting potential, though its UK context limits Article 14(3)'s full application.[91] These cases reveal NIS2's strengths in enforcing timeliness and accountability but also expose challenges in ensuring robust risk management, resource availability, and cross-border efficacy — issues explored in the following sections.

## 4. Strengths of NIS2 in Crisis Scenarios

The NIS2 Directive exhibits notable legal strengths that could enhance

[85] Helena Carrapiço and André Barrinha, 2017. "The EU as a coherent (cyber)security actor?", *Journal of Common Market Studies* (6), 55:1254-1272. https://doi.org/10.1111/jcms.12575.
[86] Directive (EU) 2022/2555, Article 23(4)(a); Finnish Data Protection Ombudsman, "Vastaamo."
[87] Directive (EU) 2022/2555, Article 23(4) (b-c).
[88] NHS England, "Synnovis." Available at https://www.england.nhs.uk/synnovis-cyber-incident/questions-and-answers/, last accessed 02.03.2025.
[89] European Union Agency for Cybersecurity (ENISA), "ENISA Threat Landscape 2023," October 31, 2023, accessible at https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023, last accessed 02.03.2025.
[90] Directive (EU) 2022/2555, Article 20(1).
[91] Saira Ghafur, Søren Rud Kristensen, Kate Honeyford, Guy Martin, Ara Darzi, and Paul Aylin, *op. cit.,* 2019.

the resilience of EU health infrastructure against large-scale cyberattacks, as demonstrated by its potential application to the WannaCry, Vastaamo, and Synnovis incidents. These strengths — rooted in its structured reporting, accountability mechanisms, and coordination framework — align with its overarching goal of systemic resilience, as articulated in Recital 11.[92]

The first significant strength is NIS2's swift incident reporting mechanism under Article 23(4), which ensures timely escalation of significant incidents to enable rapid containment and response.[93] In the WannaCry attack, the ransomware's rapid spread on May 12, 2017, disrupted 80 NHS trusts and 603 other organizations, canceling 19,494 appointments and operations.[94] Under NIS2, the 24-hour early warning requirement (Article 23(4)(a)) would have compelled affected trusts to notify the UK's National Cyber Security Centre (NCSC) by May 13, 2017, potentially enabling a faster CSIRT response to deploy the kill switch discovered by researcher Marcus Hutchins, which halted the ransomware's spread globally.[95] This contrasts with the 2017 reality, where delays in reporting and coordination prolonged disruptions, costing £92 million — a cost that timely notifications might have reduced.[96] Similarly, in the Vastaamo breach, the discovery of blackmail attempts on September 25, 2020, could have triggered an Article 23(4)(a) warning by September 26, 2020, accelerating Finnish authorities' containment efforts compared to the delayed public disclosure on October 21, 2020.[97] The 72-hour detailed notification (Article 23(4)(b)) would have provided specifics — 33,000 affected records — by September 28, 2020, aiding a coordinated response, while the one-month final report (Article 23(4)(c)) could have informed EU-wide mitigation by October 25, 2020.[98] For Synnovis, the June 3, 2024, attack prompted an NHS statement on June 4, 2024, confirming NCSC involvement, suggesting a 24-hour response consistent with Article 23(4)(a), which limited further spread across six hospitals.[99] These cases demonstrate that Article 23(4)'s structured timeline could significantly enhance response speed, a critical factor in minimizing healthcare disruptions.[100]

---

[92] Directive (EU) 2022/2555, Article 21(1), Article 20(1), Article 34(4); UK National Audit Office, "WannaCry."

[93] Finnish Data Protection Ombudsman, "Vastaamo"; Directive (EU) 2022/2555, Article 20(1), Article 34(4).

[94] NHS England, "Synnovis"; Directive (EU) 2022/2555, Article 20(1).

[95] ENISA, "Checking-up on Health." Accessible at https://www.enisa.europa.eu/news/checking-up-on-health-ransomware-accounts-for-54-of-cybersecurity-threats, last revised 02.03.2025.

[96] Directive (EU) 2022/2555, Article 14(3), Article 16(1).

[97] Aggeliki Tsohou, Vasiliki Diamantopoulou, Stefanos Gritzalis and Costas Lambrinoudakis, 2023. "Cyber insurance: state of the art, trends and future directions", *International Journal of Information Security* (3), 22:737-748. https://doi.org/10.1007/s10207-023-00660-8.

[98] Finnish Data Protection Ombudsman, "Vastaamo"; Directive (EU) 2022/2555, Article 16(1).

[99] NHS England, "Synnovis." Available at https://www.england.nhs.uk/synnovis-cyber-incident/questions-and-answers/, last accessed 02.03.2025.

[100] European Commission, "Cybersecurity Strategy", available at https://digital-strategy.ec.europa.eu/en/policies/cybersecurity#:~:text=The%20EU%20Cybersecurity%20Strategy&text=The%20st

The second strength is NIS2's management accountability provision under Article 20(1), which imposes personal liability on leadership to deter negligence and enforce proactive cybersecurity governance.[101] In WannaCry, the NAO found that all affected NHS trusts were running unpatched Windows systems despite a patch being available since March 14, 2017, a failure attributed to the Department of Health's lack of enforcement of basic cybersecurity standards.[102] Under NIS2, this oversight would have breached Article 21(1)'s risk management mandate, triggering Article 20(1) liability for trust leadership, with potential fines up to £10 million (Article 34(4)) — a deterrent absent in 2017 that could have spurred earlier updates and avoided the £92 million cost.[103] Vastaamo's leadership similarly neglected basic security — lacking encryption and access controls — leading to a €318,000 GDPR fine in December 2020; under NIS2, Article 20(1) could have imposed up to €10 million, amplifying accountability for the 33,000-record breach.[104] For Synnovis, while specific leadership actions are undocumented, the attack's success suggests potential security lapses, which Article 20(1) would address by holding managers accountable, as seen in NHS England's rapid escalation to the NCSC.[105] This provision strengthens governance by shifting responsibility to leadership, a lesson from WannaCry and Vastaamo where negligence exacerbated impacts.[106]

The third strength is NIS2's potential for cross-border coordination through the European Cybersecurity Competence Centre (Article 14(3)) and EU-CyCLONe (Article 16(1)), designed to unify responses to multi-state incidents — a critical need in healthcare's interconnected landscape.[107] WannaCry's global reach affected NHS trusts but lacked EU-wide coordination under NIS1, though Article 16(1) could have shared the kill switch solution across member states.[108] Vastaamo's cross-border blackmail, impacting Sweden and other EU states by October 2020, was managed nationally under GDPR, with no EU-level response; NIS2's Article 16(1) could have coordinated CSIRTs to trace the blackmailer, leveraging Article 14(3)'s information-sharing framework.[109] Synnovis, confined to the UK, saw NCSC involvement but no EU coordination due to Brexit; within

rategy%20has%20three%20areas,advance%20global%20and%20open%20cyberspace, last accessed 01.02.2025.

[101] Ibid.

[102] Directive (EU) 2022/2555, Recital 15.

[103] Directive (EU) 2022/2555, Article 16(1), Article 14(3).

[104] Jesse M. Ehrenfeld, *op. cit.,* 2017.

[105] Hadi Ghanbari and Kari Koskinen, *op. cit.,* 2024.

[106] NHS England, "Synnovis." Available at https://www.england.nhs.uk/synnovis-cyber-incident/questions-and-answers/, last accessed 02.03.2025.

[107] Directive (EU) 2022/2555, Article 21(1).

[108] Jesse M. Ehrenfeld, *op. cit.,* 2017.

[109] Hadi Ghanbari and Kari Koskinen, *op. cit.,* 2024.

the EU, Article 16(1) would have unified responses if patient data crossed borders.[110] This potential, though untested in these pre-NIS2 cases, aligns with the European Commission's 2020 Cybersecurity Strategy, emphasizing collaboration.[111] These strengths — rapid reporting, accountability, and coordination — position NIS2 as a robust framework, though their efficacy depends on implementation, as explored next.

### 5. Weaknesses and Gaps in NIS2

Despite its strengths, NIS2 reveals critical weaknesses and gaps when evaluated against large-scale cyberattacks on health infrastructure, as evidenced by WannaCry, Vastaamo, and Synnovis, potentially undermining its ambition to ensure comprehensive preparedness.[112] These gaps — coordination delays, legacy vulnerabilities, transposition disparities, and resource constraints — are assessed using data, highlighting challenges NIS2 must address.

**Coordination Delays**: NIS2's cross-border coordination via EU-CyCLONe (Article 16(1)) and the European Cybersecurity Competence Centre (Article 14(3)) aims to unify responses, but its pre-2023 absence limits direct testing.[113] WannaCry's global spread in 2017 saw no EU-level coordination under NIS1, with the UK managing it nationally; Article 16(1) could have shared solutions, but its efficacy remains unproven.[114] Vastaamo's 2020 blackmail affected Sweden, yet Finland's response under GDPR lacked EU collaboration; Article 16(1) might have traced the perpetrator, but NIS1 offered no such mechanism.[115] Synnovis's 2024 attack, confined to the UK, saw NCSC action but no EU coordination due to Brexit, suggesting Article 14(3)'s limits outside the EU framework.[116] The European Commission's 2019 NIS1 assessment noted inconsistent cross-border responses, a gap NIS2 aims to close, but these cases suggest potential delays if implementation falters.[117]

**Legacy Vulnerabilities**: Article 21(1)'s risk management mandate fails to retroactively address entrenched weaknesses.[118] WannaCry exploited unpatched Windows systems despite a March 2017 patch, breaching Article 21(1)'s

---

[110] Directive (EU) 2022/2555, Article 21.
[111] Directive (EU) 2022/2555, Article 41.
[112] Robin van Kessel, Madeleine Haig and Elías Mossialos, 2023. "Strengthening cybersecurity for patient data protection in Europe", *Journal of Medical Internet Research*, 25:e48824. https://doi.org/10.2196/48824.
[113] European Union Agency for Cybersecurity (ENISA), "ENISA Threat Landscape 2023," October 31, 2023, accessible at https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023, last accessed 02.03.2025.
[114] Directive (EU) 2022/2555, Recital 15.
[115] Directive (EU) 2022/2555, Article 1(1).
[116] Directive (EU) 2022/2555, Article 16(1); Finnish Data Protection Ombudsman, "Vastaamo."
[117] Directive (EU) 2022/2555, Article 21; UK National Audit Office, "WannaCry."
[118] Directive (EU) 2022/2555, Article 41.

standards, costing £92 million due to outdated IT.[119] Vastaamo's lack of encryption and access controls from 2018 to 2020 violated Article 21(1), exposing 33,000 records.[120] Synnovis's 2024 ransomware success implies similar vulnerabilities, though specifics are unavailable, aligning with ENISA's 2023 note on legacy risks.[121] NIS2 lacks funding or mandates for upgrades, a gap evident in these incidents.[122]

**Transposition Disparities**: Article 41 requires uniform transposition by October 17, 2024, but pre-NIS2 cases hint at challenges.[123] WannaCry's UK response was national, with no EU standard; Vastaamo's Finnish gaps suggest uneven readiness.[124] Synnovis, post-Brexit, reflects external disparities, but within the EU, NIS1's 2019 review showed inconsistent adoption, a risk for NIS2.[125]

**Resource Constraints**: Article 23(4) and Article 21 impose burdens that strained resources in WannaCry (£92 million recovery) and Synnovis (ongoing delays), with Vastaamo's small firm unable to secure data.[126] ENISA's 2023 report notes resource limits in healthcare, challenging NIS2's demands.[127] These gaps threaten its preparedness (Recital 15).[128]

## 6. Proposed Reforms for Enhanced Preparedness and Conclusions

To address these gaps, reforms are proposed to strengthen NIS2's preparedness, using real data insights.[129] A unified crisis protocol (Article 16(1)) could improve coordination, as Vastaamo needed.[130] Mandated legacy upgrades (Article 21) with EU support could prevent WannaCry's £92 million loss and Synnovis's delays.[131] Uniform enforcement (Article 41) by October 2024 avoids Vastaamo's gaps.[132] Training (Article 20(2)) eases WannaCry's resource

[119] Directive (EU) 2022/2555, Article 20(2); UK National Audit Office, "WannaCry."
[120] Directive (EU) 2022/2555, Article 1(1).
[121] Directive (EU) 2022/2555, Article 23, Article 20; UK National Audit Office, "WannaCry"; Finnish Data Protection Ombudsman, "Vastaamo."
[122] European Commission, "Cybersecurity Strategy", available at https://digital-strategy.ec.europa.eu/en/policies/cybersecurity#:~:text=The%20EU%20Cybersecurity%20Strategy&text=The%20strategy%20has%20three%20areas,advance%20global%20and%20open%20cyberspace, last acces- sed 01.02.2025.
[123] Directive (EU) 2022/2555, Article 41.
[124] UK National Audit Office, "WannaCry"; Finnish Data Protection Ombudsman, "Vastaamo."
[125] European Commission, "Assessment of the EU Member States' Rules on Cybersecurity", with information available at https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies, last revised 02.03.2025.
[126] UK National Audit Office, "WannaCry"; NHS England, "Synnovis."
[127] ENISA, "ENISA Threat Landscape 2023."
[128] Directive (EU) 2022/2555, Recital 15.
[129] Directive (EU) 2022/2555, Article 1(1).
[130] Directive (EU) 2022/2555, Article 16(1); Finnish Data Protection Ombudsman, "Vastaamo."
[131] Directive (EU) 2022/2555, Article 21; UK National Audit Office, "WannaCry."
[132] Directive (EU) 2022/2555, Article 41.

strain.[133] These enhance NIS2's efficacy.[134]

NIS2's reporting (Article 23) and accountability (Article 20) are robust, but coordination, legacy issues, transposition, and resources challenge its preparedness, as seen in WannaCry, Vastaamo, and Synnovis.[135] Reforms could ensure resilience, guiding EU policy and advancing cybersecurity law.[136]

## Bibliography


1. Abbou, Benyamine, Boris Kessel, Merav Ben Natan, Rinat Gabbay-Benziv, Dikla Dahan Shriki, Anna Ophir, Nimrod Goldschmid et al., (2024). "When all computers shut down: the clinical impact of a major cyber-attack on a general hospital", *Frontiers in Digital Health*, 6. Accessible at https:// doi.org/10.3389/fdgth.2024.1321485, last revised 01.03.2025.
2. Carrapiço, Helena and André Barrinha, 2017. "The EU as a coherent (cyber) security actor?", *Journal of Common Market Studies* (6), 55:1254-1272. https://doi.org/10.1111/jcms.12575.
3. Ciekanowski, Zbigniew, Marek Gruchelski, Julia Nowicka, Sławomir Żurawski and Yury Pauliuchuk, 2023. "Cyberspace as a source of new threats to the security of the European Union", *European Research Studies Journal* (Issue 3), XXVI:782-797. https://doi.org/10.35808/ersj/3249.
4. Directive (EU) 2016/1148. "Concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union." July 6, 2016. https://eur-lex.europa.eu/eli/dir/2016/1148/oj.
5. Directive (EU) 2022/2555. "On Measures for a High Common Level of Cybersecurity Across the Union." November 14, 2022. https://eur-lex.europa.eu/eli/dir/2022/2555/oj.
6. Ehrenfeld, Jesse M., 2017. "Wannacry, cybersecurity and health information technology: a time to act", *Journal of Medical Systems* 41, 104, https://doi.org/10.1007/s10916-017-0752-1.
7. European Commission. 2019. "Assessment of the EU Member States' Rules on Cybersecurity." July 10, 2019. https://digital-strategy.ec.europa.eu/en/library/assessment-eu-member-states-rules-cybersecurity.
8. European Commission. 2020. "Cybersecurity Strategy for the Digital Decade." December 16, 2020. https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0.
9. European Union Agency for Cybersecurity (ENISA). 2023. "Checking-up on Health: Ransomware Accounts for 54% of Cybersecurity Threats." July 4, 2023. https://www.enisa.europa.eu/news/checking-up-on-health-ransomware-accounts-for-54-of-cybersecurity-threats.
10. European Union Agency for Cybersecurity (ENISA). 2023. "ENISA Threat


[133] Directive (EU) 2022/2555, Article 20(2); UK National Audit Office, "WannaCry."
[134] Directive (EU) 2022/2555, Article 1(1).
[135] Directive (EU) 2022/2555, Article 23, Article 20; UK National Audit Office, "WannaCry"; Finnish Data Protection Ombudsman, "Vastaamo."
[136] European Commission, "Cybersecurity Strategy." Available at https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy, last revised 02.03.2025.

Landscape 2023." October 31, 2023. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023.

11. Finnish Data Protection Ombudsman. 2020. "Decision on Vastaamo Data Breach." October 29, 2020. https://tietosuoja.fi/en/-/decision-on-vastaamo-data-breach.
12. Ghafur, Saira, Søren Rud Kristensen, Kate Honeyford, Guy Martin, Ara Darzi, and Paul Aylin, 2019. "A retrospective impact analysis of the wannacry cyberattack on the nhs", *NPJ Digital Medicine*, 2, 98, https://doi.org/10.1038/s 41746-019-0161-6.
13. Ghanbari, Hadi and Kari Koskinen, 2024. "When data breach hits a psychotherapy clinic: The Vastaamo Case", *Journal of Information Technology Teaching Cases* 0(0). https://doi.org/10.11 77/20438869241258235.
14. Kessel, Robin van, Madeleine Haig and Elías Mossialos, 2023. "Strengthening cybersecurity for patient data protection in Europe", *Journal of Medical Internet Research*, 25:e48824. https://doi. org/10.2196/48824.
15. King's College Hospital NHS Foundation Trust. 2024. "Update on Synnovis Cyber Attack." June 21, 2024. https://www.kch.nhs.uk/news/update-on-synnovis-cyber-attack/.
16. Kioskli, Kitty, Theofanis Fotis, Sokratis Nifakos and Haralambos Mouratidis (2023). „The importance of conceptualising the human-centric approach in maintaining and promoting cybersecurity-hygiene in healthcare 4.0". *Applied Sciences*, 13(6), 3410. https://doi.org/10.3390/ app13063410.
17. Mikac, Robert, 2023. "Protection of the EU's Critical Infrastructures: Results and Challenges", *Applied Cybersecurity & Internet Governance* (1), 2:1-5. https://doi.org/10.60097/acig/162868.
18. Odermatt, Jed, *The European Union as a Cybersecurity Actor* (March 20, 2018). in Blockmans Steven & Panos Koutrakos (eds.), *Research Handbook on EU Common Foreign and Security Policy*. Cheltenham/Northhampton: Edward Elgar Publishing, Forthcoming, University of Copenhagen, Faculty of Law Research Paper No. 2018-52, Available at SSRN: https://ssrn.com/abstract=314 4257 or http://dx.doi.org/10.2139/ssrn.3144257.
19. Rajamäki, Jyri, Dominik Jarzemski, Jiri Kucera, Ville Nyman, Ilmari Pura, Jarno Virtanen, Minna Herlevi et al., 2024. "Implications of GDPR and NIS2 for cyber threat intelligence exchange in hospitals", *Wseas Transactions on Computers*, 23:1-11. Available at: https://doi.org/10.37394/232 05.2024.23.1.
20. Seh, Adil Hussain, Mohammad Zarour, Mamdouh Alenezi, Amal Krishna Sarkar, Alka Agrawal, Rajeev Kumar and Raees Ahmad Khan, 2020. "Healthcare data breaches: insights and implications", *Healthcare* (2), 8:133. https://doi.org/10.3390/healthcare8020133.
21. Tsohou, Aggeliki, Vasiliki Diamantopoulou, Stefanos Gritzalis and Costas Lambrinoudakis, 2023. "Cyber insurance: state of the art, trends and future directions", *International Journal of Information Security* (3), 22:737-748. https://doi.org/10.1007/s10207-023-00660-8.