Hacking Heathcare - Weekly Blog

Hacking Healthcare	TLP:WHITE	Alert Id: e6748eb0	2025-03-14 12:43:09

This week, Health-ISAC®'s Hacking Healthcare® examines a new report from the European Union Agency for Cybersecurity (ENISA) to assess what it says about the cybersecurity maturity and criticality of various sectors in the EU. We break down how the health sector measures up to other sectors and where ENISA thinks there is room for improvement.

Welcome back to Hacking Healthcare®.

ENISA Launches NIS360 Report – Health Sector in the "Risk Zone" Despite Improvements

What is the NIS360 Report?

The NIS360 2024 report was published on March 5, and it "assesses the maturity and criticality of sectors of high criticality under the NIS2 Directive, providing both a comparative overview and a more in-depth analysis of each sector."[i] The intent of NIS360 is to aid EU and member state-level entities in identifying areas for improvement and prioritization, and to facilitate the tracking of sector progress over time.

Methodology

The report is based on a variety of EU-level inputs (e.g. Eurostat) and survey participation from over 1300 EU entities across 22 (sub)sectors, including 150 healthcare entities and 22 sector-specific or sector-agnostic national authorities with some relation to healthcare. It uses a refined version of the original NIS360 methodology which plots along dimensions of maturity and criticality.

This method was first piloted in 2023 and an explanation of the revised version used in this report can be found in Annex A, but at a high-level, NIS360 assesses a sector's maturity and criticality.

Maturity was measured along dimensions of:[ii]

- **Operational Preparedness:** Including the "level of preparedness of the sector to handle large-scale incidents and crises"
- **Collaboration and Information Sharing:** Including the level of sharing within and between authorities and sector entities at the national and EU level.
- **Policy Framework and Guidance:** Including an evaluation of policy and legislative frameworks that "drive" cybersecurity objectives.
- **Risk Management and Good Practices:** Including to "the level of understanding of cyber risks and steps taken towards their mitigation by sector entities, national authorities, and at the EU level"

Criticality was measured along dimensions of:[iii]

- **Socio-Economic Impact of Significant Incidents:** Including the “potential socioeconomic impact in the event of a significant incident.”

- **Dependency on ICT:** Including how reliant sector entities are on ICT systems for their core functions and operations.

- **Time Criticality:** Including “how quickly the impact of a significant incident affecting the sector would be felt in society and the economy and/or impact to other sectors, taking into account the existence of alternatives and the time sensitivity of the sector’s operations.”

Non-Healthcare Key Findings

Before we get to the health sector specifically, it's worthwhile to examine some of the key findings of other critical sectors that the health sector relies upon.[iv]

- Electricity, telecommunications, and banking were all rated as being significantly mature, befitting their criticality and the amount of “regulatory oversight, global investments, political focus, and robust public-private partnerships” they have been subject to.

- Digital infrastructure (e.g. internet services, cloud services, data centers, etc...) also rate highly in maturity, but have “challenges to navigate due to their inherent heterogeneity, cross-border nature, and the inclusion of previously unregulated entities within their scope.”

Health Sector Assessment

The health sector finds itself roughly in the center of the 22 sectors assessed along both axes. Due to the health sector being one of six sector’s judged to have a higher “criticality” score than “maturity” score, it has been placed in the “risk zone”. The report calls for these sectors to receive “extra attention to ensure their maturity gaps are addressed in a way that enables them to effectively deal with the added challenges posed by their respective criticality levels.”[v]

In terms of maturity, the health sector is placed well above sectors like public administration, oil, and drinking water, but well behind leaders like electricity, banking, and telecommunications. Maturity challenges include wide variations in how NIS is implemented across EU member states, numerous national authorities providing only basic support in terms of guidance and supervision, limited guidance on how to manage cyber risk, no comprehensive understanding of sector-wide risks at the EU-level, and a mixed level of operational preparedness.

However, on the positive side, the report does note the expectation for national authorities to grow their capacity, general approval of cyber risk management controls within health entities leadership, and a fairly well-established collaboration and information sharing environment.

In terms of criticality, the health sector was assessed as roughly equal to space, gas, and railways, and behind core internet, telecommunications, and ICT service management. Socioeconomic impacts were judged to be moderate as incidents tended to be relatively confined to member states and with the health sector. Time criticality was assessed to be moderate due to the "relatively high tolerance before an outage escalates into a crisis."[vi] The report also noted the likelihood of the criticality score increasing over time as ICT dependencies continue to grow.

Key Health Sector Challenges & Areas for Improvement

The key challenges identified by the report include:

- The "pressing" need to address the "disparity in understanding among sector entities of cyber risks facing them", especially between large and small entities;
- The health sector's "reliance on complex supply chains as well as its dependence on legacy systems and inadequately secured medical devices";
- Inconsistent and inadequate levels of operational preparedness.

The report also outlined some key areas for improvement, including:

- A need to clarify the "interplay and synergies" between the various regulations and policy efforts that affect the health sector (NIS2, Medical Device Regulation (MDR), AI Act, Cyber Resilience Act (CRA), Cyber Solidarity Act (CSA), etc...);
- A need for the sector to engage in EU and member state level exercises to improve response capabilities; and
- A need to expand participation in information sharing and collaboration initiatives.

The health sector portion of the report is not particularly long, and we encourage members to review it for full details.

Action & Analysis

Available with Health-ISAC Membership

Reference(s): Europa Analytics
Report Source(s): Health-ISAC
Sources:

[i] https://www.enisa.europa.eu/sites/default/files/2025-03/ENISA%20-%20NIS360%20-%202024_0.pdf
[ii] https://www.enisa.europa.eu/sites/default/files/2025-03/ENISA%20-%20NIS360%20-%202024_0.pdf
[iii] https://www.enisa.europa.eu/sites/default/files/2025-03/ENISA%20-%20NIS360%20-%202024_0.pdf
[iv] https://www.enisa.europa.eu/sites/default/files/2025-03/ENISA%20-%20NIS360%20-%202024_0.pdf
[v] https://www.enisa.europa.eu/sites/default/files/2025-03/ENISA%20-%20NIS360%20-%202024_0.pdf
[vi] https://www.enisa.europa.eu/sites/default/files/2025-03/ENISA%20-%20NIS360%20-%202024_0.pdf
[vii] https://www.enisa.europa.eu/sites/default/files/2025-03/ENISA%20-%20NIS360%20-%202024_0.pdf

Release Date: Mar 15, 2025 (UTC)

Tags: NIS2, Hacking Healthcare, ENISA, European Union
TLP:WHITE: Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.
Conferences, Webinars, and Summits:
https://h-isac.org/events/
Hacking Healthcare:
Hacking Healthcare is co-written by John Banghart and Tim McGiff.

John Banghart has served as a primary advisor on cybersecurity incidents and preparedness and led the National Security Councils efforts to address significant cybersecurity incidents, including those at OPM and the White House. John is currently the Senior Director of Cybersecurity Services at Venable. His background includes serving as the National Security Councils Director for Federal Cybersecurity, as Senior Cybersecurity Advisor for the Centers for Medicare and Medicaid Services, as a cybersecurity researcher and policy expert at the National Institute of Standards and Technology (NIST), and in the Office of the Undersecretary of Commerce for Standards and Technology.

Tim McGiff is currently a Cybersecurity Services Program Manager at Venable, where he coordinates the Health-ISACs annual Hobby Exercise and provides legal and regulatory updates for the Health-ISACs monthly Threat Briefing.

- John can be reached at jbanghart@h-isac.org and jfbanghart@venable.com.
- Tim can be reached at tmcgiff@venable.com.

Access the Health-ISAC Threat Intelligence Portal:
Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Health-ISAC Threat Intelligence Portal (HTIP).
For Questions or Comments:
Please email us at toc@h-isac.org