DIGITALEUROPE

12 DECEMBER 2024

Strengthening healthcare cybersecurity: Focus on implementation, not new legislation

Executive summary

Europe's healthcare sector faces an escalating cybersecurity crisis, with a sharp increase in ransomware and data-related attacks targeting hospitals and healthcare providers. A recent ENISA report revealed that 54 per cent of reported cyber incidents in healthcare involved ransomware, whilst 46 per cent pertained to breaches of patient data.[1] These growing threats jeopardise patient safety, data integrity and the operational continuity of essential healthcare services.

Despite the critical importance of cybersecurity, hospitals and healthcare providers face significant challenges in addressing these risks. Limited budgets, talent shortages and complex regulatory requirements hinder their ability to implement holistic, risk-based cybersecurity measures. Additionally, fragmented information-sharing practices within and across Member States exacerbate vulnerabilities, leaving healthcare systems ill-prepared to respond to emerging threats.

To address these challenges, DIGITALEUROPE supports the EU Action Plan for the Cybersecurity of Hospitals and Healthcare Providers, as outlined in European Commission President Ursula von der Leyen's political guidelines.[2] This plan should strengthen public-private partnerships, particularly through information sharing and analysis centres (ISACs), and provide practical support to healthcare entities for regulatory compliance and threat management. It must focus on the effective implementation of existing regulations as opposed to new legislation.

Key recommendations include:

[1] See *ENISA threat landscape: health sector*, July 2023, available at https://www.enisa.europa.eu/sites/default/files/publications/Health%20Threat%20Landscape.pdf.

[2] https://commission.europa.eu/document/download/e6cd4328-673c-4e7a-8683-f63ffb2cf648_en?filename=Political%20Guidelines%202024-2029_EN.pdf.

DIGITALEUROPE
Rue de la Science, 37, B-1040 Brussels
T.+32 (0) 2 609 53 10 / www.digitaleurope.org / @DIGITALEUROPE
EU Transparency Register: 64270747023-20

- **Strengthen supply chain cyber resilience**: Address vulnerabilities in outdated medical devices and legacy systems by conducting regular security assessments, upgrading critical systems and transitioning to secure, scalable cloud-based solutions that leverage advanced technologies like AI.
- **Enhance cybersecurity in procurement**: Update procurement guidelines to require suppliers to meet stringent cybersecurity standards.
- **Invest in funding and skills development**: Allocate national and EU-level funding for cybersecurity upgrades, training programmes and research initiatives, with specific budget thresholds for healthcare institutions. Promote cybersecurity careers through education, certifications and partnerships with academia and industry.
- **Strengthen ISACs**: Expand ISACs' role by increasing awareness, engaging ENISA, empowering ISACs to lead coordinated responses and integrating them into EU frameworks for critical infrastructure protection.
- **Establish rapid-response cybersecurity units**: Require Member States to mandate rapid-response teams within healthcare systems to ensure service continuity and conduct annual cybersecurity exercises to enhance preparedness.
- **Clarify and streamline NIS2 implementation**: Publish harmonised guidelines aligning NIS2 with other regulations to avoid duplication.

By addressing these priorities, the action plan can unify Member States in creating a resilient healthcare cybersecurity framework, ensuring the safety and sustainability of Europe's healthcare systems.

Table of contents

- Executive summary 1
- Table of contents 2
- Embedding cyber resilience in healthcare supply chains 4

Mitigating legacy risks and transitioning to modern solutions 4

Creating a 'ring of steel' around critical assets 4

Strengthening cybersecurity in procurement 5

Promoting secure-by-design principles ..... Error! Bookmark not defined.

Developing digital resilience action plans **5**

- **Dedicated funding and skills development** **5**

Building a robust funding framework **6**

National funding initiatives 6
EU-level financial support 6
Budget thresholds for healthcare institutions 7
Incentives for cybersecurity investments 7
Investment in cybersecurity research 7

Skills development: strengthening the cybersecurity workforce **7**

Promoting cybersecurity careers 7
EU-wide certification 7
Partnerships for career opportunities 8
Enhancing cybersecurity education 8
Tailored training for healthcare ecosystems 8

- **Strengthening ISACs and leveraging EU response mechanisms** **8**
- **Guidelines for NIS2 Directive implementation in healthcare** .. **10**
- **Annex I: examples of successful cooperation through ISACs** **13**

Embedding cyber resilience in healthcare supply chains

In acute care environments, the challenge of maintaining cybersecurity is heightened by the catastrophic consequences of system downtime. Many hospitals and healthcare providers continue to rely on outdated medical devices and software, which lack the advanced security features needed to withstand modern cyberattacks. Legacy solutions, whilst often indispensable for healthcare operations, become significant vulnerabilities when they are no longer supported or maintained, exposing critical infrastructure to escalating risks.

Hospitals, healthcare providers and entities handling health data must regularly assess the security status of their software and hardware, identifying vulnerabilities and obsolete systems. These evaluations should form the basis for implementing mitigation measures, such as upgrading systems or transitioning away from unsupported technologies. To support this process, the Commission, Member States and national authorities must provide harmonised guidelines, ensuring consistent assessment practices across healthcare systems.

Mitigating legacy risks and transitioning to modern solutions

Hospitals should prioritise addressing unsupported legacy technologies, focusing on upgrading systems where feasible or phasing them out of critical networks. Dedicated funding, drawn from national and EU sources, must be made available to facilitate these upgrades. Beyond immediate replacements, healthcare providers should embrace a strategic transition to innovative, secure and scalable cloud-based solutions. Cloud infrastructure offers enhanced security, resilience and adaptability, helping mitigate cybersecurity concerns whilst improving patient care and operational efficiency. For example:

- Transitioning high-risk legacy systems to cloud-based platforms can protect sensitive data, streamline healthcare workflows and address chronic staffing shortages by automating and optimising processes.
- Advanced technologies like artificial intelligence (AI) can be integrated into security workflows to enhance risk mitigation and adapt to evolving threats.

Creating a ‘ring of steel’ around critical assets

Healthcare organisations must establish a ‘ring of steel’ to protect critical assets, such as medical devices, electronic health records (EHRs) and

essential legacy systems. Although it may be impractical to fortify every asset to the highest degree, critical systems warrant enhanced protection due to their potential impact on patient safety and overall system integrity. Security measures should be tailored to safeguard these assets whilst ensuring the seamless operation of healthcare workflows and system interoperability.

In alignment with the Resilience of Critical Entities Directive, Member States should actively support healthcare organisations by developing guidance materials, conducting resilience exercises and offering training programmes. These measures will ensure that critical entities are prepared to respond effectively to threats, whether they arise from cyberattacks or other sources.

Strengthening cybersecurity in procurement

To embed cybersecurity into healthcare systems, procurement processes must be aligned with security standards. The Commission should issue updated guidelines requiring suppliers to demonstrate compliance with cybersecurity benchmarks as a prerequisite for participation in procurement tenders. This step would ensure that newly acquired technologies meet robust security criteria, reducing risks from the outset.

Developing digital resilience action plans

Building on best practices from sectors like financial services, European governments should encourage hospitals and healthcare providers to adopt comprehensive digital resilience action plans. These plans should encompass:

- ICT risk-management measures: Strategies to identify, assess and mitigate risks across IT systems.
- Resilience testing: Regular evaluations of system robustness against potential disruptions, including cyberattacks and IT outages.
- Third-party risk management: Measures to secure supply chains and vendor relationships, addressing vulnerabilities that extend beyond the organisation.

Dedicated funding and skills development

Tight budgets, acute workforce shortages and a lack of specialised skills remain significant barriers preventing European hospitals and healthcare providers from adequately addressing cybersecurity threats.

These constraints hinder the recruitment and retention of skilled cybersecurity personnel, as hospitals are often unable to offer competitive remuneration due to financial limitations. Compliance with EU legislation, staff training and

system updates require substantial investments, placing further strain on already stretched resources.

Addressing these challenges necessitates a targeted approach that prioritises funding and skills development to fortify the sector's cyber resilience.

Building a robust funding framework

Ensuring adequate funding is a cornerstone of improving healthcare cybersecurity. There must be dedicated financial support at both national and EU levels to bolster the cybersecurity readiness of hospitals and healthcare providers.

National funding initiatives

Member States must allocate funding at the national level to enhance the cybersecurity and resilience of healthcare systems. France's €750 million programme launched in December 2023 serves as an exemplary model, demonstrating how strategic financial commitments can drive systemic improvements.[3] Similar programmes across Member States could provide the necessary resources for cybersecurity advancements.

EU-level financial support

Leveraging EU mechanisms such as the Digital Europe Programme, EU4Health and European Structural and Investment Funds is critical to ensuring comprehensive support across Member States. These funds should focus on:

- Increasing capacity, capability, expertise and awareness in cybersecurity amongst healthcare authorities, hospitals and providers;
- Implementing skills development and upskilling initiatives to address workforce shortages;
- Launching awareness campaigns to educate stakeholders on the NIS2 Directive and the requirements for essential entities;[4]
- Supporting public-private partnerships like ISACs; and

[3] The French CaRE action plan aims to strengthen cybersecurity in healthcare, with €250 million allocated until 2025 and a total goal of €750 million by 2027. Initial funding of €60 million is supporting hospitals in implementing remediation plans to address vulnerabilities and mitigate risks. More information is available (in French) at https://esante.gouv.fr/espace-presse/presentation-du-programme-care.

[4] Directive (EU) 2022/2555.

- Establishing specialised cybersecurity programmes tailored to procurement teams and other relevant stakeholders.

Budget thresholds for healthcare institutions

A proportional allocation of budgets for cybersecurity, based on each institution's level of digital transformation, should be recommended. For instance, a minimum of 10 per cent of the IT or digital transformation budget should be designated for cybersecurity, independent of clinical resources.

Incentives for cybersecurity investments

To encourage healthcare organisations to prioritise cybersecurity, Member States should explore financial incentives. These could include grants, tax benefits or subsidies that recognise the difficult spending trade-offs healthcare providers face.

Investment in cybersecurity research

Collaboration with academia and industry is essential to foster dedicated research into healthcare cybersecurity. Establishing and funding research partnerships would contribute to innovative solutions and advanced defences against evolving threats.

Skills development: strengthening the cybersecurity workforce

A robust and skilled workforce is critical to defending healthcare systems against cyber threats. The acute shortage of cybersecurity professionals in the healthcare sector requires immediate action to attract talent, foster expertise and create sustainable career paths.

Promoting cybersecurity careers

Public campaigns and educational initiatives should focus on breaking down stereotypes about cybersecurity careers, particularly in healthcare. Emphasising the diversity of roles and the sector's vital societal impact can position cybersecurity as a compelling career choice.

EU-wide certification

A unified training certification framework is needed to enhance the visibility and coherence of cybersecurity education. High-quality labels for training programmes would ensure that courses meet established standards and are up to date. Certification levels should align with the varying responsibilities within healthcare organisations, from frontline IT personnel to strategic decision-makers.

Partnerships for career opportunities

Collaboration between private companies, academia and government institutions can create opportunities for cybersecurity professionals at all career stages. These partnerships could support internships, apprenticeships and other work-based learning programmes tailored to the healthcare sector.

Enhancing cybersecurity education

Cybersecurity must be integrated into academic curricula to build a pipeline of highly skilled graduates. Accredited, continuous learning opportunities, such as certifications, technical boot camps and secondments, should also be available for professionals seeking to enhance their skills. A structured framework for consistent cybersecurity education and workforce development is essential, encompassing healthcare delivery organisations, vendors and service providers.

Tailored training for healthcare ecosystems

Training programmes should address the unique cybersecurity needs of healthcare systems, focusing on practical applications and sector-specific challenges. For instance, procurement teams could benefit from specialised programmes on assessing cybersecurity risks in vendor contracts, whilst clinical staff might require training on mitigating risks from medical devices.

Strengthening ISACs and leveraging EU response mechanisms

Effective information sharing and collaboration are critical for building collective capacity and preparedness to counter cyber threats. ISACs play a key role in this effort, enabling public-private partnerships to enhance cybersecurity. Their contributions align with the goals of key EU frameworks, including the NIS2 Directive, the Cybersecurity Act and the Cyber Solidarity Act,[5] which emphasise the importance of collaboration and information exchange across sectors.

Whilst the NIS2 Directive does not explicitly mandate the establishment of ISACs, it encourages their use to foster improved communication and cooperation. As non-profit, membership-based organisations, ISACs provide a centralised resource for gathering and sharing information on cyber threats, incidents and best practices. This two-way exchange between private entities and public institutions has proven invaluable in mitigating cyber risks and enabling effective responses to incidents across the EU.

[5] Directive (EU) 2022/2555, Regulation (EU) 2019/881 and COM(2023) 209 final.

Currently, two ISACs are active in the field of health.[6] The membership fee structure enables organisations with more resources to subsidise those with less.

Despite the added value provided by ISACs, these organisations face several challenges that can hamper active participation. For example, smaller organisations or those with lower levels of maturity may feel that they lack the expertise to contribute to an ISAC's the work. Furthermore, certain organisations may feel reluctant to share information during incidents, for instance, due to reputational concerns. Finally, a lack of awareness of ISACs' role, their way of working and how they can be best leveraged is a major barrier that prevents exploiting their full potential.

To overcome these challenges, the action plan should implement targeted measures to strengthen ISACs' role and impact:

- **Raise awareness**: Conduct comprehensive awareness campaigns at the EU and national levels to highlight the value and role of health ISACs. These campaigns should target hospitals, healthcare providers and smaller businesses, emphasising the practical benefits of membership. Collaboration with stakeholder organisations, such as hospital associations, would amplify outreach efforts.

- **Enhance ENISA's engagement**: ENISA should take a more active role in supporting ISACs by disseminating their guidelines, best practices and reports across the healthcare sector. Recognising ISACs as primary partners for activities related to critical infrastructure would further institutionalise their importance.

- **Strengthen institutional partnerships**: ISACs should be positioned as trusted partners for policymakers, national cybersecurity organisations and other institutional stakeholders. Their insights can shape cybersecurity policies, aid the implementation of relevant legislation and foster the development of knowledge-sharing networks amongst healthcare providers.

- **Empower health ISACs for coordinated responses**: Health ISACs should be empowered to lead coordinated responses to ransomware and other cyberattacks affecting critical sector entities. Examples in the Annex illustrate how health ISACs have played pivotal roles in addressing major cyber threats, underlining their capacity to act as coordinators in crisis scenarios.

- **Integrate ISACs into EU frameworks**: In alignment with the Cyber Solidarity Act, ISACs should serve as partners for collaboration

[6] EU Health ISAC (see https://www.isacs.eu/) and Health-ISAC (see https://h-isac.org).

with cluster security operation centres (SOCs) and potential contributors to cybersecurity reserves. Their expertise would enhance these initiatives' efficacy and reach.

- **Incentivise collaboration**: Larger companies and cybersecurity organisations should be encouraged to educate and support smaller entities, which often lack resources to address known threats and vulnerabilities. Incentives could include grants, recognition programmes or tax benefits.

- **Facilitate joint playbooks and real-time intelligence sharing**: Develop joint operating playbooks for healthcare organisations to standardise incident responses. Broader sharing of real-time indicators of compromise, including lessons from other sectors such as finance, would strengthen preparedness and resilience across the board.

- **Rapid-response cybersecurity units**: To further enhance healthcare resilience, Member States should require the establishment of dedicated, rapid-response cybersecurity units within healthcare systems. These units would ensure continuity of critical services during cyber incidents and support long-term recovery efforts:

    - Proactive measures for critical entities: In line with the Directive on the Resilience of Critical Entities,[7] Member States and critical entities should adopt proactive measures to ensure security and continuity in response to threats, both natural and man-made.

    - Cybersecurity exercises: Annual cybersecurity exercises should be conducted to test and improve healthcare systems' defences. For example: ENISA-facilitated purple teaming exercises could identify vulnerabilities and refine defence mechanisms; and tabletop simulation exercises with National Cybersecurity Centres (NCSCs) would enhance practical crisis response and decision-making capabilities.

Guidelines for NIS2 Directive implementation in healthcare

[7] Directive (EU) 2022/2557.

As of October 2024, the NIS2 Directive has officially become applicable, requiring hospitals, healthcare providers, medical device manufacturers and pharmaceutical companies to adopt robust cybersecurity measures.[8]

So far, only six Member States have fully or partially enacted the directive into national law. Its implementation poses significant challenges, particularly for the healthcare sector, due to overlaps with existing regulations such as the Medical Device Regulations, the European Health Data Space (EHDS) and the Cyber Resilience Act (CRA). [9]

The action plan should seek to clarify and foster harmonised implementation of NIS2 in the healthcare context. It is crucial for all stakeholders involved in the health sector that overlapping requirements across regulations are streamlined and clarified to facilitate compliance and simplify implementation.

To this end, the Commission should:

- Publish clear guidelines on NIS2 Directive implementation in healthcare, aligning its requirements with the other legal frameworks. Tailored cybersecurity guidelines should define the shared responsibilities of healthcare providers, medical device manufacturers, pharmaceutical companies and other entities, ensuring streamlined compliance. These guidelines should specify applicable state-of-the-art standards, such as ISO 27001, to simplify adherence across the healthcare ecosystem. Organisations should not be required to duplicate compliance efforts if existing European or international standards already address the relevant requirements.

- Provide practical support on how to implement these standards effectively and improve organisations' security posture, especially to SMEs.[10]

- Collaborate with National Cyber Agencies to lead awareness campaigns and provide targeted training for healthcare organisations, focusing on critical topics such as the scope and responsibilities under NIS2, emerging threats like deep-fake attacks and best practices for strengthening cybersecurity resilience.

---

[8] These include, amongst others: risk management and security measures; incidence reporting; governance and accountability structures to support cybersecurity risk management; supply chain and third-party vendor management; business continuity and crisis management plans; and security and awareness training.

[9] Regulations (EU) 2017/745 and 2017/746, covering medical devices and in-vitro diagnostic medical devices; COM(2022) 197 final, awaiting publication in the Official Journal of the EU; and Regulation (EU) 2024/2847, respectively.

[10] See, for example, Cyber Ireland's Cybersecurity Roadmap for micro-enterprises, available at https://cyberireland.ie/cybersecurity-roadmap.html#/.

FOR MORE INFORMATION, PLEASE CONTACT:

Gianluca Violante

Senior Manager for Digital Health Policy

gianluca.violante@digitaleurope.org / +32 492 46 78 17

Alberto Di Felice

Policy and Legal Counsel

alberto.difelice@digitaleurope.org / +32 471 99 34 25

Annex I: examples of successful cooperation through ISACs

Each of these incidents highlights the Health-ISAC community's rapid, collaborative response to cyber threats, an invaluable resource for keeping healthcare organisations resilient in the face of cyberattacks.

Petya/NotPetya attack sparks global response

In June 2017, the Petya/NotPetya cyberattack hit Ukraine in a targeted strike that sent shockwaves around the world. Even organisations outside Ukraine felt the impact. As the attack unfolded, Health-ISAC's Threat Intelligence Committee sprang into action, dissecting the malware's entry points, affected sectors and key indicators of compromise. Collaboratively, member organisations developed a 'vaccine' to halt the malware's spread. After testing and confirming its efficacy, they shared the solution with the community, showcasing how Health-ISAC can rapidly unite the healthcare sector in the face of a global crisis.

Russian hacktivists target European hospitals

In January 2023, Russian hacktivists made waves by announcing on their Telegram channel plans to target European hospitals in retaliation for the EU's support for Ukraine. Health-ISAC quickly mobilised, with analysts scouring Telegram for intel to protect vulnerable organisations. As the threat intensified, Health-ISAC shared the intelligence with both members and non-members, warning them of the potential for incoming attacks. Within 24 hours, the victim list was circulating on Twitter/X, and just two days later, a wave of DDoS attacks struck. Thanks to rapid collaboration, Health-ISAC helped healthcare organisations brace for impact, shining a spotlight on the importance of cross-sector information sharing.

CrowdStrike incident disrupts global healthcare systems

In July 2023, Health-ISAC members in Australia and Asia Pacific reported an unusual issue: Microsoft Windows systems caught in a relentless reboot loop, creating major disruptions. The alert rippled across time zones, with European members logging on to a dedicated Slack channel to tackle the escalating IT outages. Within hours, over 500 members were actively discussing CrowdStrike's faulty update, sharing mitigation techniques and real-time solutions that were continuously refined through the weekend.

The impact was massive: half of Health-ISAC's global member organisations reported disruptions affecting phone systems, patient services, pharmacy orders, electronic records, billing and more. In a 25 July webinar, CrowdStrike's senior leadership engaged with nearly 900 Health-ISAC members, providing clarity, dispelling rumours and working to remediate the affected systems.

Meanwhile, cybercriminals wasted no time exploiting the situation, launching fake CrowdStrike support websites and phishing emails. Health-ISAC members quickly countered by sharing hundreds of malicious domains, showing the power of community vigilance in a sector-wide crisis.

DIGITALEUROPE

About DIGITALEUROPE

DIGITALEUROPE is the leading trade association representing digitally transforming industries in Europe. We stand for a regulatory environment that enables European businesses and citizens to prosper from digital technologies. We wish Europe to grow, attract, and sustain the world's best digital talents and technology companies. Together with our members, we shape the industry policy positions on all relevant legislative matters and contribute to the development and implementation of relevant EU policies. Our membership represents over 45,000 businesses that operate and invest in Europe. It includes 113 corporations that are global leaders in their field of activity, as well as 41 national trade associations from across Europe.

DIGITALEUROPE
Rue de la Science, 37, B-1040 Brussels
T.+32 (0) 2 609 53 10 / www.digitaleurope.org / @DIGITALEUROPE
EU Transparency Register: 64270747023-20