ECSO
EUROPEAN CYBER SECURITY ORGANISATION

Cybersecurity in Healthcare: Insights from Security Professionals

January 2025

For Discussion

Agenda

- Setting the Stage
- First-Hand Insights from Security Professionals
- Challenges and Suggested Solutions
- Final Considerations

Setting the Stage

ECSO

Von der Leyen's Action Plan

In her inception speech and political manifesto,
Ursula von der Leyen made a specific reference to **cybersecurity in healthcare**

Political Guidelines for the Next European Commission 2024-2029 (18 July 2024)

We must also do more to protect the security of our health systems, which are increasingly the target of cyber and ransomware attacks.

To improve threat detection, preparedness and crisis response, I will propose a European ***action plan on the cybersecurity of hospitals and healthcare providers*** *in the first 100 days of the mandate.*

In response, ECSO decided to collect inputs regarding challenges and potential solutions from ECSO Members and the ECSO CISO Community

How to Enhance Cybersecurity in Healthcare?

The Starting Point

Healthcare is a **critical sector** by any standard or criterion.

Providers and hospitals often face **challenging budgetary situations**.

Decision-makers must allocate financial and personnel resources to **competing yet essential priorities,** such as securing digital infrastructure and security aware staff to provide the needed level of privacy and data protection.

The challenges are not new, yet the **increasing number of breaches** make them more evident than ever.

The Suggested Approach

Public administrations must team up with healthcare security and business professionals to boost resources through shared tools, crowdsourced solutions, scalable initiatives, and optimized workflows

In Brief...

Policy Initiatives Covering Healthcare

!

The healthcare sector has certainly **not been overlooked** by any policymakers and cybersecurity professional stakeholders.

It is considered a **critical sector by all measures**.
It has been addressed from multiple perspectives, including organisations, products, and data.

Relevant policies worth mentioning

Illustrative

- NIS2 Directive
- Cyber Resilience Act (CRA)
- General Data Protection Regulation (GDPR)
- Commission Recommendation on a European Electronic Health Record Exchange Format
- Communication on Enabling the Digital Transformation of Health and Care in the Digital Single Market
- Council Conclusions on Health in the Digital Society
- Regulation 2017/745 and /746 on medical devices and in vitro diagnostic medical devices
- Guidance on Cybersecurity for medical devices (MDCG 2019-16 Rev.1)
- eHealth Network

ECSO

Types of Healthcare Organisations

The Healthcare sector encompass a wide range of actors, with their own nuances and specificities

Healthcare providers*

Laboratories

Medicinal products research and development entities

Pharmaceutical products entities

Medical devices manufacturers

* As per Directive 2011/24/EU of 9 March 2011 on the application of patients' rights in cross-border healthcare,
'healthcare provider' means any natural or legal person or any other entity legally providing healthcare on the territory of a Member State;

ECSO

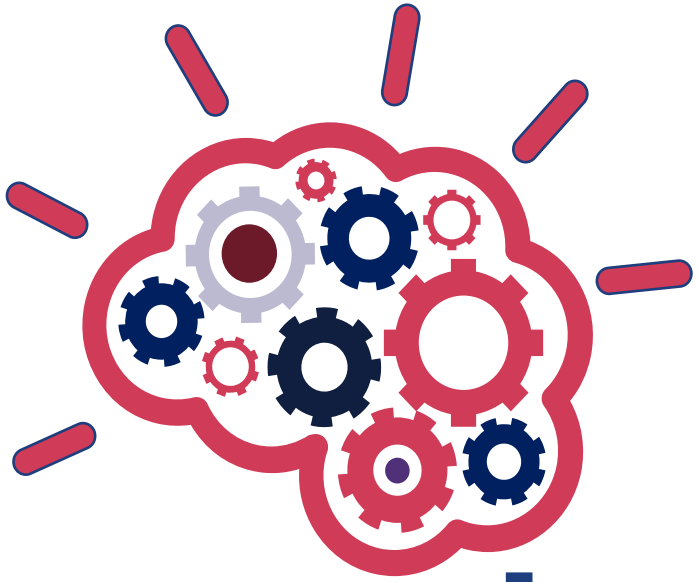
State of Play

Several measures were put in place
to improve cybersecurity in the healthcare sector
in Europe over the last few years.

What is the current situation?

Are these measures working?

Why not?



Concerning Challenges and Risks

Based on ECSO Members' and CISOs' firsthand experiences, including cybersecurity products and intelligence vendors, the state of play is still very concerning.

Cyber threat intelligence and incident response reports show that the Healthcare sector is heavily targeted and to a certain extent not mature enough, given its systemic criticality.

See next slides for more intelligence and insights from ECSO Members

Lazarus Group Cyberattack and HL7Magic:
Protecting Healthcare from Nation-State Threats and Securing Medical Devices

The cyber attack by the Lazarus Group underscores the urgency of enhancing cybersecurity in the medical sector.

Open-source tools like HL7Magic are crucial for identifying and mitigating vulnerabilities in medical devices.

Improved cooperation between government agencies, and private sector entities is essential for effective threat detection and response.

No Pineapple! –DPRK Targeting of Medical Research and Technology Sector | WithSecure™ Labs

- WithSecure™ detected and responded to a sophisticated cyber attack attributed to the Lazarus Group. This attack targeted both public and private sector research organizations, specifically within the medical research and energy sectors, as well as their supply chains. The attribution to Lazarus Group was made with high confidence due to overlapping techniques, tactics, and procedures, along with an operational security mistake by the attackers. The primary motivation behind this campaign is assessed to be intelligence gathering.

HL7Magic: A tool for testing medical devices using the HL7 protocol | WithSecure™ Labs

- HL7Magic is a tool developed to assist security testers in identifying vulnerabilities in medical devices that use the HL7 protocol. HL7 is the most commonly used protocol in the healthcare industry, but it poses significant security challenges due to its complexity and difficulty in testing. HL7Magic addresses these challenges by providing a more straightforward method for testing and securing devices that communicate using HL7, making it easier to identify and mitigate potential security issues.

ECSO Member

BITSIGHT

Cybersecurity Risks in Healthcare

Hospital Data Breaches, TLS/SSL Vulnerabilities, and Patching Challenges

!

Hospitals have historically lower cybersecurity ratings, which are linked to a higher risk of data breaches.

76% of healthcare organizations are at increased ransomware risk due to poor TLS/SSL management.

Poor patching practices in healthcare organizations significantly increase the likelihood of ransomware attacks.

In 2020, healthcare IT security breaches rose by 55%, affecting over 26 million individuals.

- The relationship between cybersecurity ratings and the risk of hospital data breaches
  - Hospitals have lower cybersecurity ratings than Fortune 1000 firms but have improved recently. Low-rated hospitals face a 14% to 33% annual breach risk. Policymakers should encourage hospitals to invest in security controls
- TLS/SSL Management Issues Increase Healthcare Ransomware Risk (Oct 2023)
  - 76% of healthcare organizations are at higher ransomware risk due to poor TLS/SSL management. Many lack a unified framework for managing TLS/SSL certificates, leading to system security incidents. Improving TLS/SSL security is a critical improvement measure.
- Poor Patching Cadence Correlated To Healthcare Ransomware Risk
  - Bitsight research indicates that healthcare organizations with poor patching practices are up to 7 times more likely to experience ransomware attacks.
- Healthcare IT Security: 3 Best Practices for Protecting the Expanding Attack Surface
  - In 2020, healthcare IT security breaches rose by 55%, affecting over 26 million individuals. Best practices include understanding the attack surface, continuous cyber risk monitoring, and reducing third-party supply chain risks.

ECSO

First-Hand Insights from Security Professionals

ECSO

Competing Priorities and Sectoral Culture

Insights from Security Professionals

In hospitals anyone is welcome (criminal or not) to be taken care.

*IT was **not** seen for a longtime as **core business** of hospitals but only non-essential support.*

***Cybersecurity by design is still a dream**.*

Alexandru Pelin, CISO, Cliniques Universitaires Saint-Luc

Note: The opinions expressed in the survey do not represent ECSO official position

Analysis

- Any organisation's core mission shapes other lines of work and priorities. Hospitals exist to provide medical care and support to anyone. **There is competition for resource allocation due to their limited availability.**
- Given the severity of incidents impacting the healthcare sector, **IT and cybersecurity have become foundational to delivering care in a digital age.**

Regulations Compliance Workload and Benefits

Insights from Security Professionals

New requirements help *organizations to raise* ***awareness*** *but also* ***increase workload*** *on the current organization.*

Head of Information Security and Risk Management, Pharmaceutical Company

Note: The opinions expressed in the survey do not represent ECSO official position

Analysis

- Security professionals frequently encounter a **dilemma** with new policies.
- On one hand, these regulations often add to their already heavy **workload**.
- On the other hand, they also provide an opportunity to **escalate the issue to upper management**, raising awareness and above all advocating for additional resources due to the mandatory nature of legal requirements.

Medical Products Development Lifecycle

Insights from Security Professionals

Medical device suppliers have not yet fully integrated cybersecurity into the lifecycle of their products.

Javier Zapata Victori, CISO, Quironsalud

Note: The opinions expressed in the survey do not represent ECSO official position

Analysis

- **Medical device manufacturers** still treat **cybersecurity as an add-on**, rather than a foundational aspect of the product development lifecycle.
- As a result, devices present vulnerabilities once they are on the market and in production, with greater risks and costs.
- Regulations are already in place to require **cybersecurity to be embedded in product development from the outset**, but the practice differs.

First-Hand Insights from Security Professionals

Sector-Tailored Frameworks

Insights from Security Professionals

*There is **no dedicated toolkit** for healthcare or pharma to identify our own risk posture and control statements that are **customized for the sector.***

Anonymous

Note: The opinions expressed in the survey do not represent ECSO official position

Analysis

- The establishment of general, widely adopted **frameworks** has vastly **simplified governance and compliance**.
- Sector-specific nuances however require **frameworks** to be **adjusted to their needs**, ensuring risks prioritization and optimal resources allocation.
- To this end, other sectors have developed **tailored versions** (see NIST Profiles).

First-Hand Insights from Security Professionals

Legacy Systems and Practices

Insights from Security Professionals

*Instead of building a **solid foundation** and consolidating it, many services are **layers of decisions** piled on top of each other*

Stéphan Rimbert, Head of IT Infrastructure, Hôpitaux Iris-Sud

Note: The opinions expressed in the survey do not represent ECSO official position

Analysis

- **Legacy systems are a challenge in any organisation**: harder to maintain due to lack of historical knowledge and staff skills, not updated anymore, and harder to integrate with new solutions.
- The lack of long-term plans and investments does not allow to fix the problem at its root. As a result, a patchwork of digital components makes the system even more **difficult**, **inefficient**, and above all **vulnerable**.

Supply Chain Management

Insights from Security Professionals

*One of our biggest challenges is getting a proper grip over this **supply chain** and ensuring they are all following the same level of cybersecurity resilience and maturity.*

Healthcare CISO

Note: The opinions expressed in the survey do not represent ECSO official position

Analysis

- Supply chain is one of the hardest challenges for any organisation, in any sector, anywhere in the world today. The healthcare sector is not an exception.
- A hospital can have 1,000s of suppliers, with a wide range of differences, each with different security postures, and without complete information visibility.
- The often **distributed**, **fragmented**, and **open nature** of hospitals makes this domain **even more difficult**.

First-Hand Insights from Security Professionals

Attracting and Retaining Talent

Insights from Security Professionals

*The current **staff funding level** for a suitably qualified and experienced Senior Information Security engineer would be around 60% of the private market rate, with no additional tangible comparative benefits (e.g., bonus reward structure, stocks, additional incentive allowance, defined promotion path)*

Senior Information Technology Manager

Note: The opinions expressed in the survey do not represent ECSO official position

Analysis

- The challenge of attracting and retaining skilled cybersecurity professionals faced by the public sector is not new. This issue is even more emphasised in a sector with competing priorities, where IT and security are considered non-essential support functions.
- The **mismatch in compensation and benefits** with other sectors leads to serious constraints in the ability to improve security overall.

First-Hand Insights from Security Professionals

Budget Constraints

Insights from Security Professionals

Financial challenges have always been there and will always be there.

Head of Information Security and Risk Management, Pharmaceutical Company

Note: The opinions expressed in the survey do not represent ECSO official position

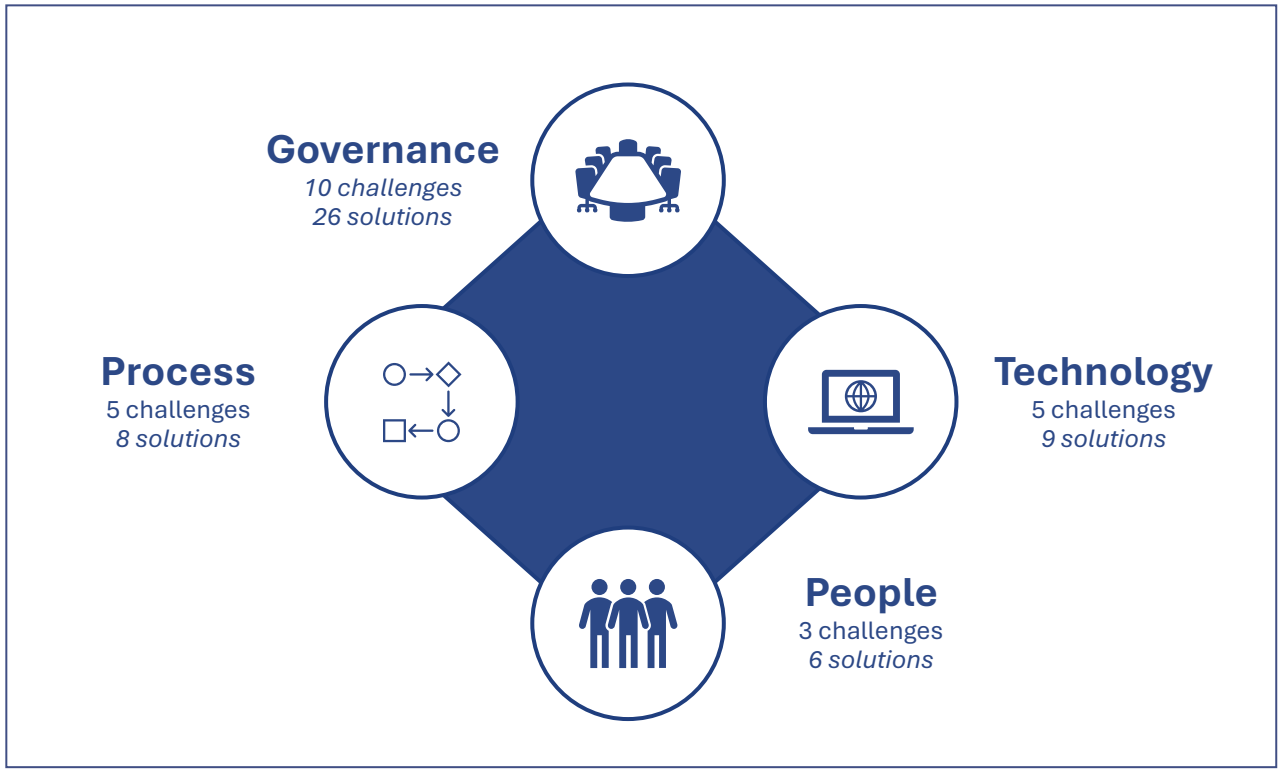
Analysis

- Notwithstanding the trade-off between business drivers and security, the **financial constraints** that IT and security teams have been facing **do not match their risk profile.**
- From the perspective of individual organizations, there is no evidence to expect this trend to change, despite the urgent need for long-term investments.
- A different approach is warranted to address this challenge.

Challenges and Suggested Solutions

Challenges and Suggested Solutions

Challenges



Suggested Solutions

Rated across two dimensions

- **Complexity**
- **Criticality**

Note: Qualitative assessment based on expert judgement. See the Annex for further information about the analytical framework

Challenges and Suggested Solutions

Governance (1/4)

For Discussion

Challenge	Solution	Complexity	Criticality
Budget constraints	• Offer direct funding and/or fiscal incentives to support healthcare organisations, ensuring no competition with funding for critical patient care	●●●	●●●
	• Establish centralised IT infrastructure for critical healthcare organisations (cloud and secure DCs/distributed infrastructure, dedicated network communications/infrastructure of sensitive data)	●●●	●●●
	• Identify critical IT infrastructure and security projects where public-private partnerships and communities can be leveraged to crowdsource resources	●●○	●●●
	• Provide incident response support at European level (e.g., European Healthcare CSIRT; Cyber Reserves)	●●●	●●●
Lack of prioritisation of IT/cyber	• Raise the importance with dedicated political initiatives and targeted awareness campaigns	●○○	●○○
	• Establish working groups with C-suite representatives from healthcare organisations, through MSs or ISACs, for awareness and accountability	●●○	●●○

Critical

Note: Qualitative assessment based on expert judgement. See the Annex for further information about the analytical framework

ECSO

Challenges and Suggested Solutions

Governance (2/4)

For Discussion

Challenge	Solution	Complexity	Criticality
Lack of mgmt. involvement in risk management (and risk acceptance)	• Explicitly call on upper management to ensure proper risk management processes, with risk acceptance	●●○	●●○
	• Establish clear accountability mechanisms for risk acceptance	●●●	●●○
Lack of harmonised standard	• Harmonise and streamline operational security standards	●●○	●●○
	• Identify a single information security controls framework for the sector to use (e.g., ISO27x1)	●○○	●●○
	• Develop a Healthcare Profile based on the identified security framework, customizing controls to address unique needs of the healthcare sector	●○○	●●○
No *tailored* risk mgmt. frameworks for the healthcare sector	• Identify a single risk management framework for the healthcare sector to use (e.g., ISO 27x5)	●●○	●●○
	• Developed tailored guidance for risk mgmt. in healthcare	●○○	●○○
	• Establish targeted awareness campaigns to adopt the identified framework	●○○	●○○
	• Develop a unified European cybersecurity risk assessment to identify systemic risks and prioritise resources allocation coordination	●○○	●●○

Note: Qualitative assessment based on expert judgement. See the Annex for further information about the analytical framework

ECSO

Challenges and Suggested Solutions

Governance (3/4)

Challenge	Solution	Complexity	Criticality
Lack of security mindset in hospitals	• Raise the importance with dedicated political initiatives	●○○	●●○
	• Establish targeted awareness campaigns for health professionals	●○○	●○○
Misalignment b/ business and security objectives	• Raise the importance with dedicated political initiatives	●○○	●●○
	• Establish targeted awareness campaigns for executives	●○○	●○○
No sector-specific CTI	• Set up CTI products tailored for the healthcare sector via ENISA and ISACs	●●○	●●○
	• Set up a dedicated feed for healthcare orgs (with IoC sharing)	●●○	●●○
	• Establish a vulnerability watch and communication channels targeted and adapted to European systems	●●○	●●○

Note: Qualitative assessment based on expert judgement. See the Annex for further information about the analytical framework

ECSO

Challenges and Suggested Solutions

Governance (4/4)

For Discussion

Challenge	Solution	Complexity	Criticality
Complex environments and geographical distribution	• Facilitate the adoption of a risk-based approach to complex environment, starting by securing critical assets with the highest security standards	●○○	●●○
	• Develop a unified European cybersecurity risk assessment to identify systemic risks and prioritise resources allocation coordination	●●○	●●○
Compliance workload	• Harmonise and streamline policy requirements (see ECSO other initiatives for more details on this)	●●○	●●● Critical
	• Provide dedicated sample policies, methodologies, processes and procedures, and other templates for organisations to adjust and adopt	●○○	●●○

Note: Qualitative assessment based on expert judgement. See the Annex for further information about the analytical framework

ECSO

Challenges and Suggested Solutions

Technology

For Discussion

Challenge	Solution	Complexity	Criticality
No tailored advanced technological capabilities	• Establish centralised IT infrastructure for critical healthcare organisations (cloud and secure DCs/distributed infrastructure, dedicated network communications/infrastructure of sensitive data)	●●●	●●●
Quantity and maturity of medical devices and related supply chain	• Establish comprehensive and stringent product security requirements	●●○	●●○
	• Establish joint procurement for healthcare organisations to ensure security requests are fulfilled (hospitals have no choice with providers not fulling their requirements)	●●●	●●●

Critical

Critical

Note: Qualitative assessment based on expert judgement. See the Annex for further information about the analytical framework

ECSO

Challenges and Suggested Solutions

Technology

Challenge	Solution	Complexity	Criticality
No product security	• Encourage manufacturers to prioritize security-by-design in their products and implement initiatives to phase out or upgrade existing systems	●●○	●●○
	• Establish joint procurement for healthcare organizations to ensure their needs are met, addressing challenges when providers fail to fulfil requirements	●●●	●●●
High uptime requirements	• Establish centralised IT infrastructure for critical healthcare organisations (cloud and secure DCs/distributed infrastructure, dedicated network communications/infrastructure of sensitive data)	●●●	●●●
	• Provide CM/DR models, templates, and plans tailored to healthcare organisations for them to adjust and adopt	●○○	●●●
Legacy systems	• Facilitate the adoption of a risk-based approach to complex environment, starting by securing critical legacy systems	●●○	●●○
	• Establish a vulnerability watch (with a focus on critical legacy systems) and communication channels targeted and adapted to European systems	●●○	●●○

Critical

Note: Qualitative assessment based on expert judgement. See the Annex for further information about the analytical framework

ECSO

Challenges and Suggested Solutions

People

For Discussion

Challenge	Solution	Complexity	Criticality
Lack of staff	• Identify activities where public-private partnerships and communities can be leveraged to crowdsource resources	●●○	●●● Critical
Recruitment challenges	• Establish targeted awareness campaigns for recruitment, highlighting the noble pursuit of a career in cybersecurity and healthcare	●○○	●●○
	• Establish centralised training and career development initiatives for different organisations offer to their employees	●●○	●●○
	• Establish university partnerships to boost recruitment	●○○	●●○
Cybersecurity staff seen as admin (instead of specialists)	• Establish targeted awareness campaigns for executives	●○○	●●○
Lack of staff awareness and technical training (generally and among biomedical staff)	• Establish targeted awareness campaigns for staff as well as for executives	●○○	●○○

Note: Qualitative assessment based on expert judgement. See the Annex for further information about the analytical framework

ECSO

Challenges and Suggested Solutions

Process (1/2)

For Discussion

Challenge	Solution	Complexity	Criticality
Lack of systems maintenance and patching	• Establish comprehensive and stringent product security requirements	●●●	●●●
	• Establish a vulnerability watch (with a focus on legacy systems) and communication channels targeted and adapted to European systems	●●●	●●●
Expansion of the attack surface	• Facilitate the adoption of a risk-based approach for endpoints management, starting by securing critical assets with the highest security standards	●●●	●●●
	• Set up CTI products tailored for the healthcare sector via ENISA and ISACs	●●●	●●●
	• Set up a dedicated feed for healthcare orgs (with IoC sharing)	●●●	●●●

Note: Qualitative assessment based on expert judgement. See the Annex for further information about the analytical framework

ECSO

Process (2/2)

For Discussion

Challenge	Solution	Complexity	Criticality
Lack of comprehensive assets mgmt.	• Facilitate the adoption of a risk-based approach for endpoints management, starting by securing critical assets with the highest security standards	●○○	●●○
Complex supply chain mgmt.	• Establish joint procurement for healthcare organisations to ensure security requests are fulfilled (hospitals have no choice with providers not fulling their requirements)	●●●	●●●
Suppliers dominant market position	• Establish joint procurement for healthcare organisations to ensure security requests are fulfilled (hospitals have no choice with providers not fulling their requirements)	●●●	●●●

Critical

ECSO

Final Considerations

Final Considerations

The Three Most Critical Areas

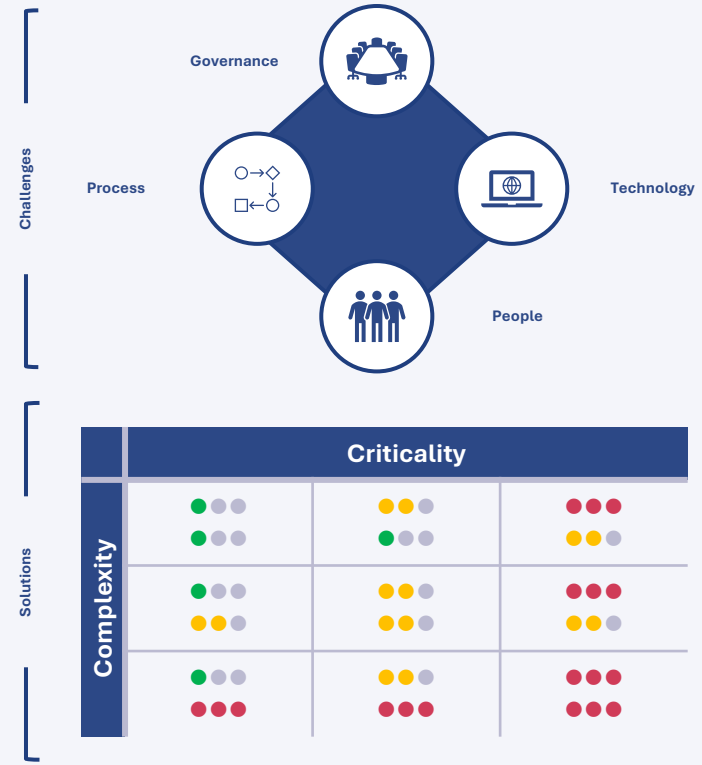
Funding and resources

Supply chain and procurement

Technological solutions and product security

Call to Action

Research and Analysis



Decision Making

Scenario A – The Ambitious Approach

Undertaking a more ambitious course of action will face significant political, financial, business, and technological constraints.

However, if successful, it will lead to substantial structural changes and benefits in the cybersecurity maturity of healthcare organizations.

Scenario B – The Gradual Approach

Opting for a gradual, advisory approach will encounter less complexity and pushback.

However, the improvements in the cybersecurity of healthcare will be incremental, rather than transformative, and potentially significantly longer.

ECSO

Open Discussion

Thank you!

Annex

Annex

Methodology

Data Collection → **Analysis** → **Dissemination**

- Collection of inputs (challenges and suggested solutions) from ECSO CISO Community and ECSO practitioners
- Collection on inputs on the threat landscape from ECSO CTI providers

- Inputs screening, identification of trends, and categorisation
- Mapping of challenges and solutions
- Aggregated and trend analysis
- Rating of challenges and solutions (dimensions and related definitions available on the next slide)

- Drafting of findings
- Sharing with policymakers
- Sharing with European cybersecurity community
- Collection of feedback
- Definition of next steps

Annex

Dimensions and Definitions

Dimension	Definition
Complexity	**The level of difficulty or challenge required to implement the suggested solution**
Technical-operational	Logistical, technical, or procedural elements, enabling or limiting the implementation of the solution
Financial	Cost implications, including upfront capital investment and ongoing expenses for operations and maintenance
Political	Resistance, stakeholder alignment or buy-in issues, or other political constraints
Criticality	**The extent to which the implementation (or lack thereof) of the solution impacts core functions or goals of healthcare**
Technical-operational	Effect on day-to-day operations, productivity, or service delivery
Financial Impact	Direct costs (e.g., investments, operational expenses) and indirect costs (e.g., opportunity costs, potential savings)
Political Impact	Impact on relationships, reputational risks, or the general public