Introduction to Cybersecurity Trends in Healthcare

METIS Lecture Series

UiA

Today's topics

- Why cybersecurity matters in healthcare
  - Real-world impacts on care and patients
- What makes healthcare a target for cybersecurity attacks
  - Why do attacks succeed
- What should healthcare organizations do
- How clinicians contribute to cybersecurity in their daily work

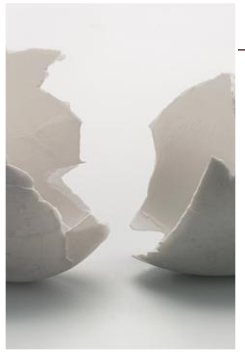
Learning goals:

- Explain how increasing digitalisation in healthcare can lead to disruptions in care when systems fail.
- Describe why cybersecurity is a patient safety issue — not just an IT concern.
- Recognise the clinician's role in supporting cybersecurity in everyday clinical practice.

The Real-Life Impact of a Cybersecurity Incident

- In 2023, University Hospital Frankfurt was hit by a cyber attack.
- A trauma and orthopedic surgeon, Simon Meier, described how it affected everyday clinical work:
  - The attack severely disrupted communication between digital systems.
  - Accessing lab results or data from mobile X-ray machines became extremely difficult, as the systems could no longer send information to the hospital database.
  - Clinicians had to reschedule appointments just to access patient files, and planned surgeries had to be postponed.
- It took considerable to until the hospitals systems returned to “normal”. (Politico, 2025)

Some Vocabulary



Cyber attack:

When someone uses digital tools or the internet to break into systems, steal data, cause damage, or disrupt normal operations.

Think of it as a digital break-in — instead of picking a lock on a door, the attacker uses software tricks to enter a digital system.

Cybersecurity incident:

Any event that affects the normal functioning, security, or availability of digital devices, data, or networks — whether it causes harm or creates disruption.

It does not have to be an attack; it can also be accidental or unexpected.

Think of it as any event — intentional or accidental — that impacts digital systems in a negative or unusual way.

Cybersecurity:

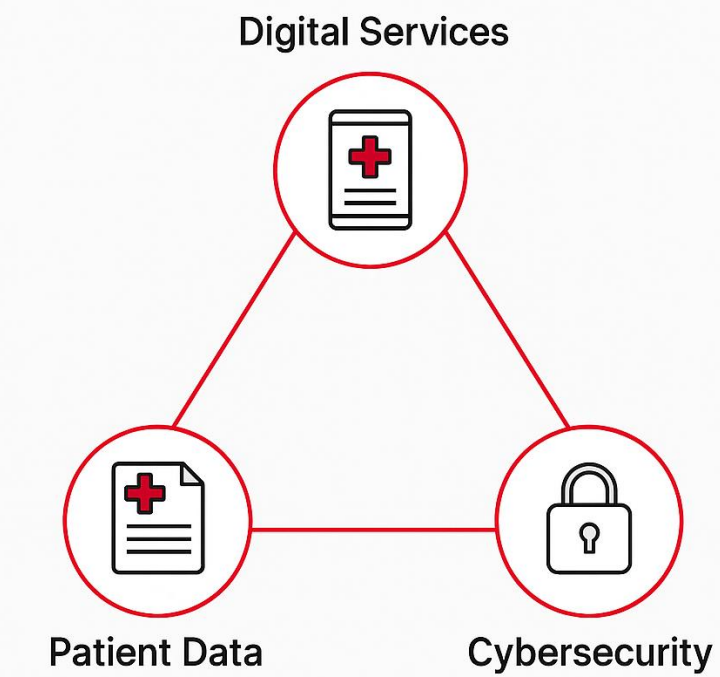
The practice of protecting data, digital devices, and networks from cybersecurity incidents.

Includes technical tools, organizational policies, and human behaviour.

Why Cybersecurity Matters in Healthcare?

Cybersecurity is a necessary foundation for responsible digitalisation in healthcare. Without secure systems, digital tools cannot be trusted to support clinical care safely.

Why Cybersecurity Matters in Healthcare?



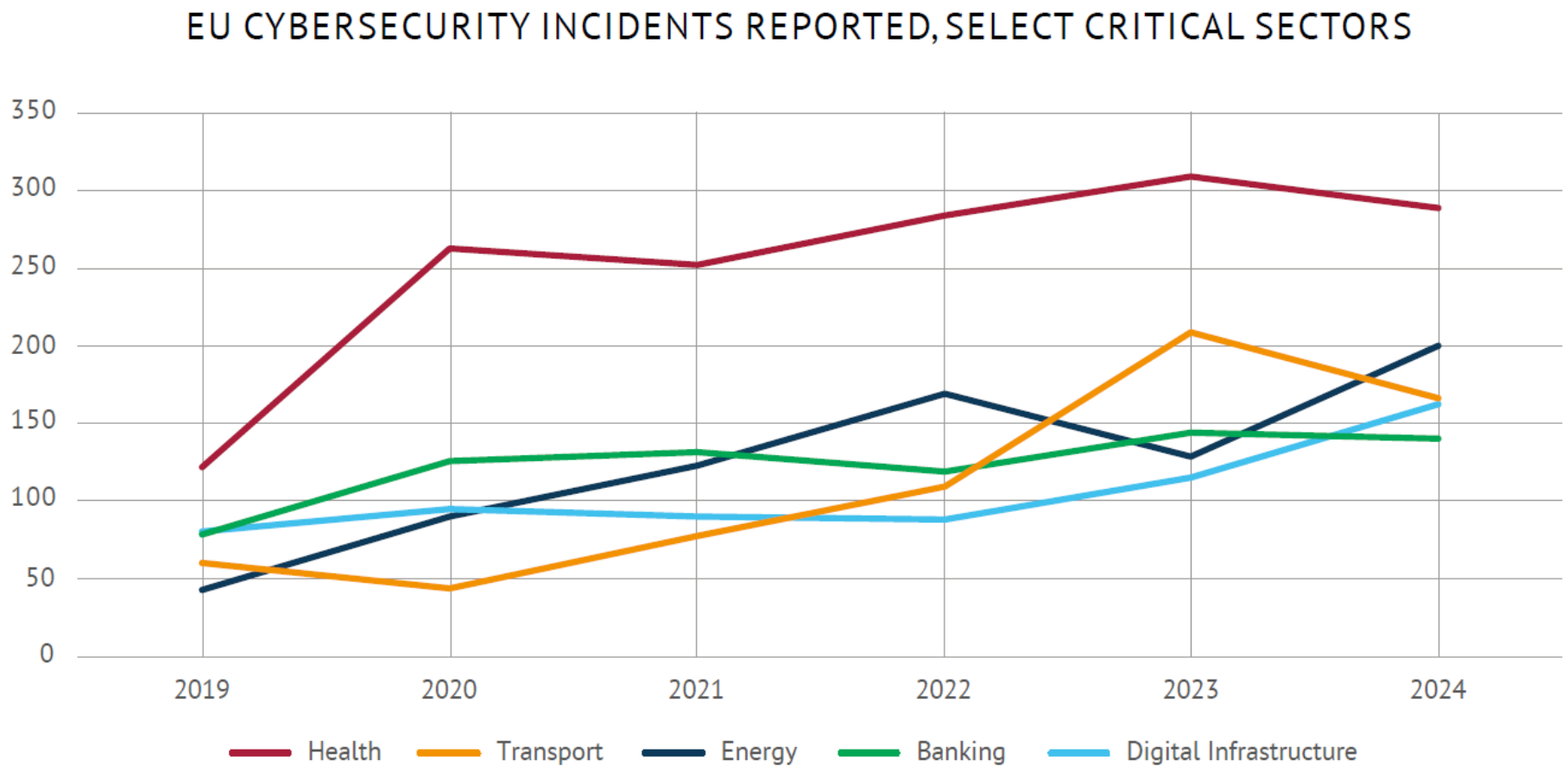
As healthcare becomes more digital, our responsibility grows. The more we rely on digital services, the more we must protect:

- the data used within these services, and
- the services themselves, which are essential for, e.g., diagnosis, treatment, and communication.

Why Cybersecurity Matters in Healthcare?

- As digital devices and artificial intelligence (AI) reshape healthcare, cyberattacks and cybersecurity incidents are becoming more frequent, including:
  - Phishing
  - Ransomware
  - Distributed Denial-of-Service (DDoS) attacks
  - Data breaches
  - Medical device vulnerabilities
  - Disinformation campaigns
- Healthcare organizations often struggle to keep up with the growing number and complexity of attacks and incidents.

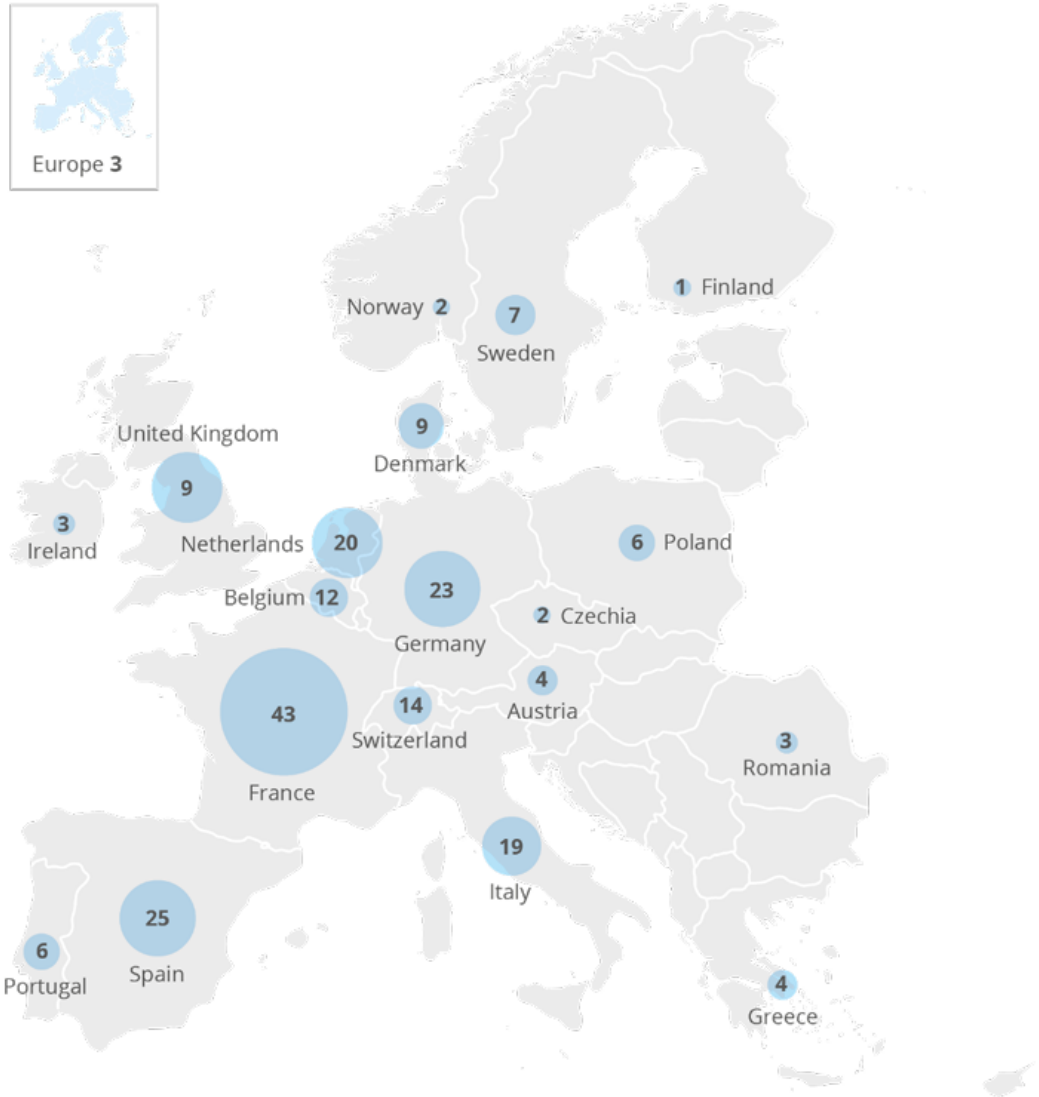
Figure 1



Source: European Commission, Annual Report NIS Directive Incidents, 2019-2024.[8] Authors' own elaboration.

Source: Goodger & Kuiper, 2025, p. 1

Figure 2: Map of incidents observed (January 2021 to March 2023)



Note: the size of the circle refers to the sum of observed incidents in the country during the reporting period. Incidents labelled as 'Europe' refer to entities that have activity in Europe and not only one country.

Source: Enisa threat landscape: Health sector, 2023, p. 8

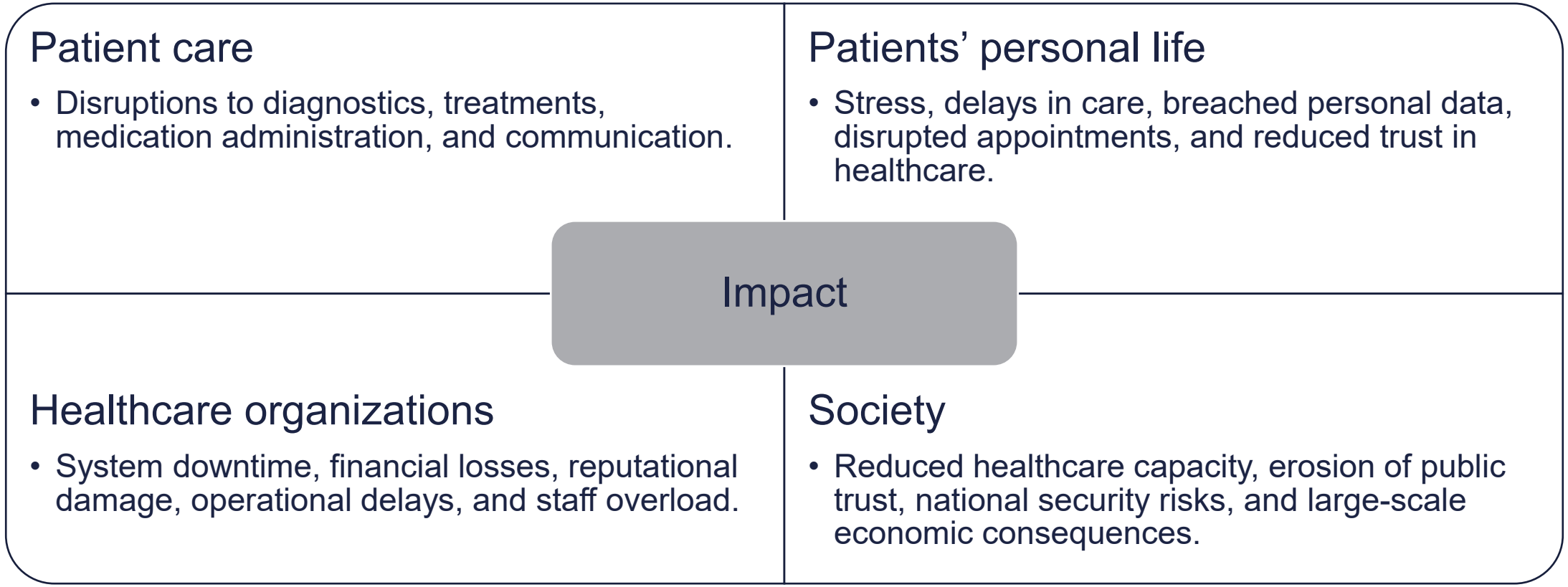
Real-World Impact on Hospitals

The impact of a cyberattack on a hospital can be wide-ranging, for example:

- Confidential patient data may be breached.
- Appointment systems can go offline, leading to delays and cancellations.
- Employees may lose access to electronic health records, making it difficult to deliver safe care.
- Ambulances may need to redirected because of system outages.
- Emergency departments may have to divert patients to other facilities.
- Laboratory services may stop functioning, delaying test results.
- Medical imaging systems may be unavailable, affecting diagnostics.
- Internet access may be disrupted, impacting communication and workflows.
- Devices used in care may malfunction or become unusable (e.g., PCs, tablets, phones, and connected “smart” medical devices)

Real-World Impact on Various Stakeholders of Healthcare

The impact of cyberattacks is far-reaching and affects many stakeholders:



Real-World Impact on Various Stakeholders of Healthcare

"*Ransomware and other cyberattacks on hospitals and other health facilities are not just issues of security and confidentiality,* ***they can be issues of life and death***" (Tedros Adhanom Ghebreyesus, WHO Director-General)

What Makes Healthcare a Target for Cybersecurity Attacks?

- Healthcare data is extremely valuable on the black market.
  - It can be sold or used for identity theft, insurance fraud, or extortion.
- Healthcare organizations face strong pressure to keep services running.
  - Attackers know hospitals cannot afford long downtime and therefore expect quick ransom payments.
- Hospitals are often an “easy” target due to:
  - Highly complex systems and interconnected devices
  - Many digital devices and systems were not originally designed with security in mind
  - Increased use of smart medical equipment and mobile devices entails more ways for attackers to break in
  - Significant differences in cybersecurity maturity across Europe (Enisa, 2024)
  - Operational, organizational, and budgetary constraints that limit cybersecurity investment (Ponemon Institute, 2023)
- Healthcare is a cornerstone of any well-functioning society
  - Politically motivated attackers may aim to disrupt and limit operational healthcare capacity and thus undermine public trust in national institutions.

Why Do Attacks Succeed?

Medical services complicatedness	Health IT complicatedness	Governance complicatedness

Source: Tanriverdi et al., 2025

What Should Healthcare Organizations Do?

Prevention

- Build strong capabilities to **prevent cybersecurity incidents** before they happen.
- Improve basic security practices, system maintenance, and staff awareness.

Detection

- Enhance the ability to **identify unusual activity or cyber threats early**.
- Early detection reduces harm and helps stop incidents from spreading.

Response and Recovery

- Strengthen the capacity to **respond quickly to cybersecurity incidents**.
- Ensure hospitals can **continue critical services** and **recover systems** after an attack.
- Aim to **minimise disruption to patient care**.

Deterrence

- Explore ways to **discourage cyber threat actors** from targeting healthcare systems.
- This includes better security standards, collaboration with national authorities, and clearer consequences for attackers.

Source: European Commission (2025): Action plan on the cybersecurity of hospitals and healthcare providers

What Should Healthcare Organizations Do?

- Build digital resilience and require it from technology suppliers:
- According to Boh et al. (2023), digital resilience refers to:
  - "*the capabilities developed through the use of digital technologies to absorb major shocks, adapt to disruptions caused by the shocks, and transform to a new stable state, where entities are more prepared to deal with major shocks*"

In practice:

- Cybersecurity must be built in — not added later
  - Cybersecurity should be integrated into health technologies from the start, rather than treated as an after thought.
  - This includes secure software design, regular updates, safe connectivity, and responsible data handling.
- Cybersecurity must be embedded throughout the patient journey (Shimabukuro & Sekar, 2025)
  - Protecting every stage of care where digital tools are involved.
  - Ensuring clinicians can deliver safe care even during disruptions.
  - Designing technology with secure clinical workflows in mind.

The Clinician's Role in Cybersecurity – Everyday Good Practices

- Be cautious with emails, links, and attachments.
- Never share passwords or leave devices unlocked.
- Report anything unusual immediately (e.g., unexpected pop-ups, significantly slowed systems, suspicious emails).
- Follow hospital policies for data handling and digital device use.
- Ask for regular training.
  - For example, training on how to recognize suspicious emails and unsafe digital behaviour.
- Expect usable security
  - Clinicians should expect systems that make it easy to act securely and should be included in decisions that affect clinical workflows.

Remember: **Cybersecurity is a shared responsibility** — every action helps protect patients.

Key Takeaways

- Healthcare relies heavily on digital systems and devices, which means that patient data, clinical workflows, and devices and systems must be protected.
  - Cyberattacks can disrupt hospital operations, delay diagnoses and treatments, and put patient safety directly at risk.
- Cybersecurity is ultimately about protecting people, not digital devices or software.
  - It is a patient safety and patient trust issue.
- Clinicians play an essential role in cybersecurity.
  - Everyday actions — secure behaviour, careful use of digital systems, and rapid reporting — help prevent incidents and protect patients.
  - Cybersecurity in healthcare succeeds only when clinicians, IT teams, and leadership work together.

Creating
knowledge
together