

Capacity Building Activities under the Health Action Plan

Ioanna Kalogeropoulou
ENISA

EU action plan for the cybersecurity of hospitals and healthcare providers



HEALTH
ACTION
PLAN

- Published on 15.1.2025

- Objective 

Enhance cybersecurity resilience in hospitals and healthcare providers across the EU

- Strategic Pillars

 Prevent incidents	Training, preparedness
 Detect threats	Early warning system, detection tools
 Respond and recover	Incident response teams, EU reserve
 Deter malicious actors	Legal tools & cyber diplomacy



Brussels, 15.1.2025
COM(2025) 10 final

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN
PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL
COMMITTEE AND THE COMMITTEE OF THE REGIONS

European action plan on the cybersecurity of hospitals and healthcare providers

Empowering Communities

The most feasible option to **scale up** the impact.



The Power of Community

Collective Impact: The community acts as a **force multiplier**, shifting efforts from isolated efforts to a unified European front.

Capacity Building Activities



AWARENESS RAISING

Strategic campaigns designed to raise awareness on cybersecurity risks in healthcare



EXERCISES

Cybersecurity exercises in hot-line mode supporting planning, execution and evaluation phases



TRAININGS

Integration of health cybersecurity training modules in online platforms

A horizontal bar with a blue-to-white gradient, positioned above the title.

Awareness Raising: What's in motion?

The 1st Awareness Raising campaign is ready



HEALTH
ACTION
PLAN

A campaign dedicated to promoting **Cyber Hygiene** among health professionals.

Build your cyber defences

Good cyber habits build your cyber immunity

1 Use Strong and Unique Passwords
Avoid personal information like birthdays or pet names, and never reuse passwords. Use passphrases of at least three unrelated words.

2 Add an Extra Layer of Protection
Enable multi-factor authentication wherever available. Combining two verification methods builds your immunity shield.

3 Always Lock Your Screen
Lock your screen every time you step away from your workstation, even for a moment. Keep devices in secure, supervised areas.

4 Only Use Approved Tools
Only use devices and applications approved by your organisation for work-related tasks. Avoid public Wi-Fi for accessing work systems or patient information.

enisa HEALTH ACTION PLAN #BuildYourCyberImmunity

Keep patients cyber safe

Protecting patient's data means protecting a patient.

1 Keep Patient Data on Safe Channels
Only share patient information through approved communication channels. Personal messaging apps, unauthorized platforms, or unencrypted emails are not safe for health data.

2 Before You Send, Check Twice
A single misdirected email can expose sensitive patient information. Before sending, take a moment to verify the recipient, review the content, and confirm it's the right person.

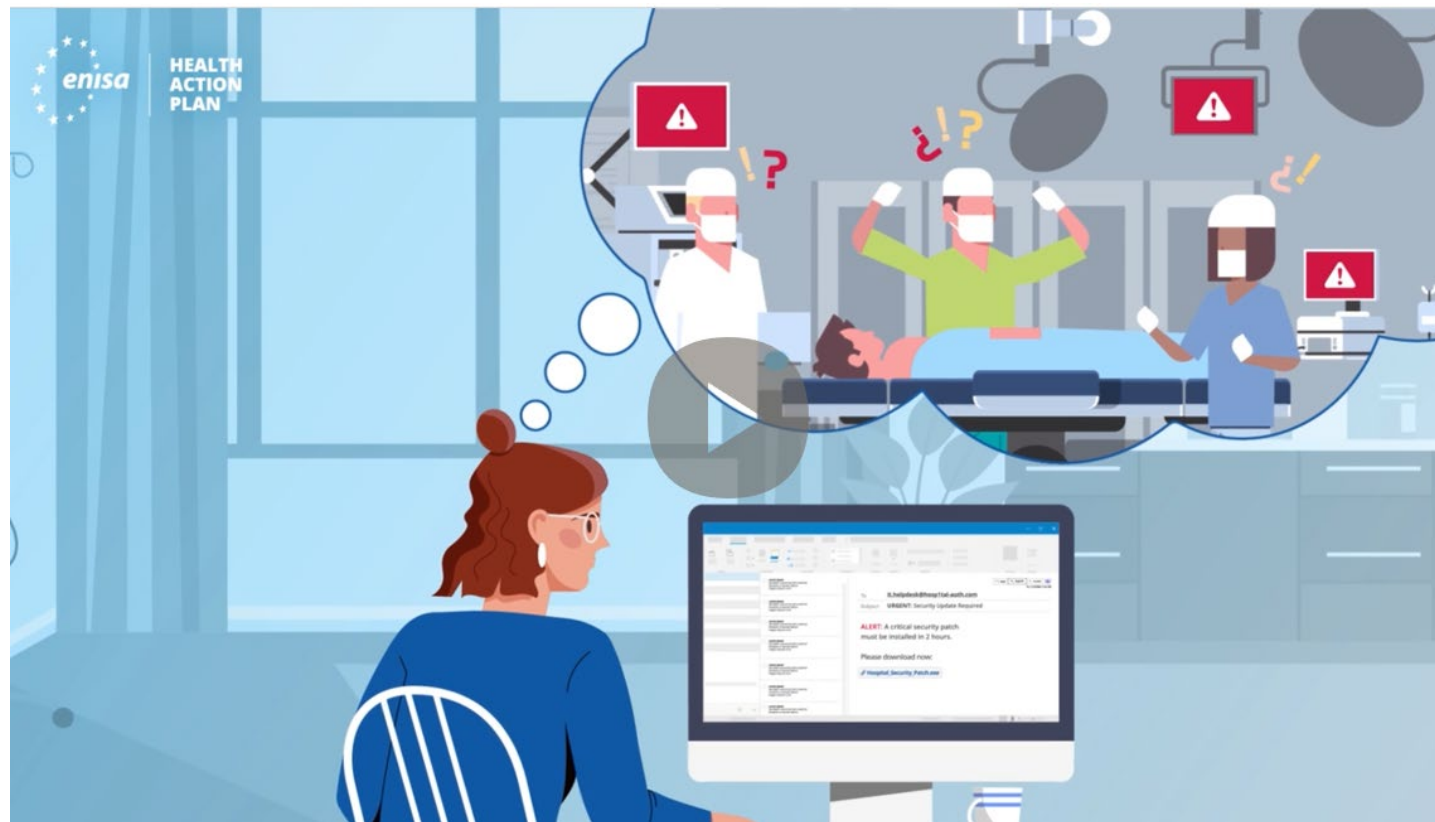
3 Share Only What's Needed
When sharing patient information, limit it to the minimum required for the task. Not every request needs a full record.

enisa HEALTH ACTION PLAN #BuildYourCyberImmunity

#BuildYourCyberImmunity

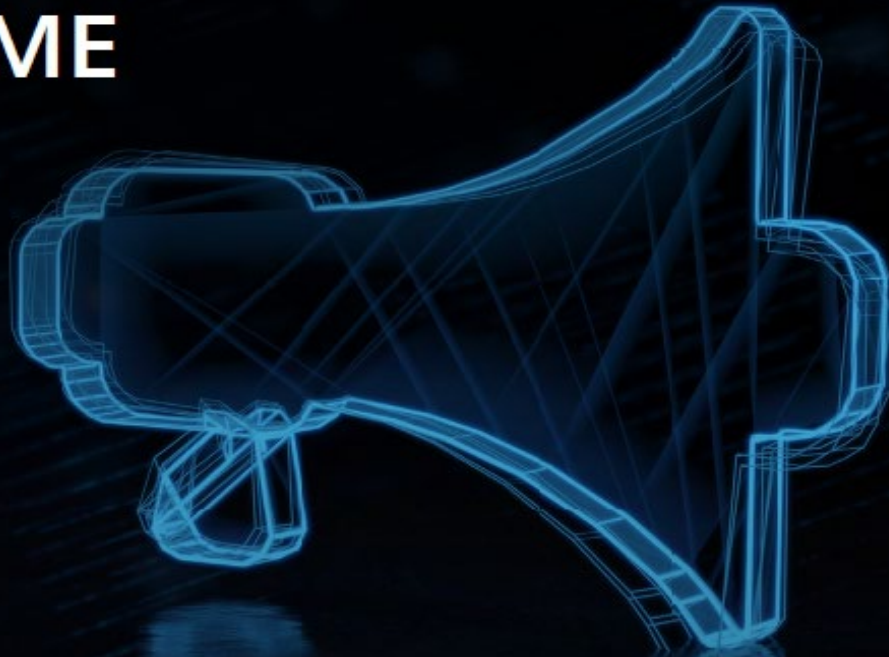


HEALTH ACTION PLAN





YOUR GUIDE TO DESIGNING A CYBER-AWARENESS PROGRAMME



The ENISA-Do-It-Yourself Toolbox

how to **design** and **implement** your own effective cybersecurity awareness program

Aim

- Teaches **how to mitigate the impact of cyber threats.**
- Incorporates activities, materials and training to promote a **culture of cyber security.**

Target audience

organizations seeking to **enhance cybersecurity awareness** among internal and external stakeholders – from SMEs to large enterprises.

What's inside the box?



<https://www.enisa.europa.eu/topics/awareness-and-cyber-hygiene/ar-in-a-box>

The AR-in-a-Box Game: reimagined for **health**



Can you find the attacker?

A horizontal bar with a blue-to-white gradient, positioned above the title.

Cybersecurity exercises: Setting the groundwork

Cybersecurity exercises

What does the Action Plan foresee?

- A large roll out of national cybersecurity exercises, in hot-line mode, to test the playbooks and strengthen incident response protocols.

How will we put this into practice?

- A dedicated team of experts, trained on the scenario, will be set up to support Member States in conducting health exercises according to their needs.





Cybersecurity exercises

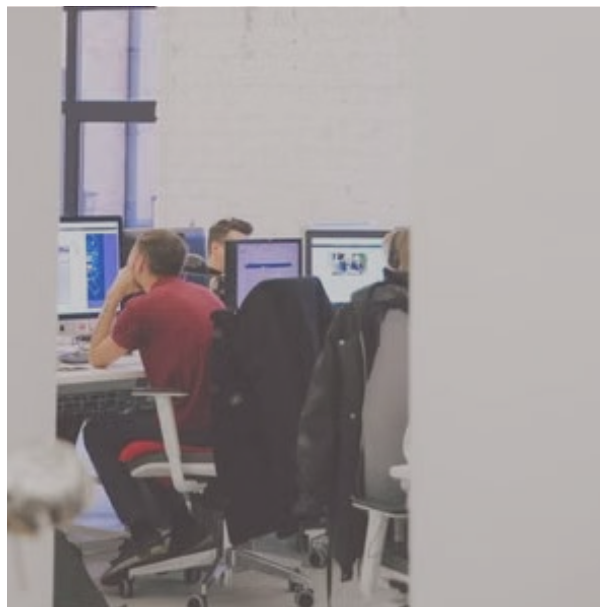
Support Member States during the exercise lifecycle.



Planning



Execution



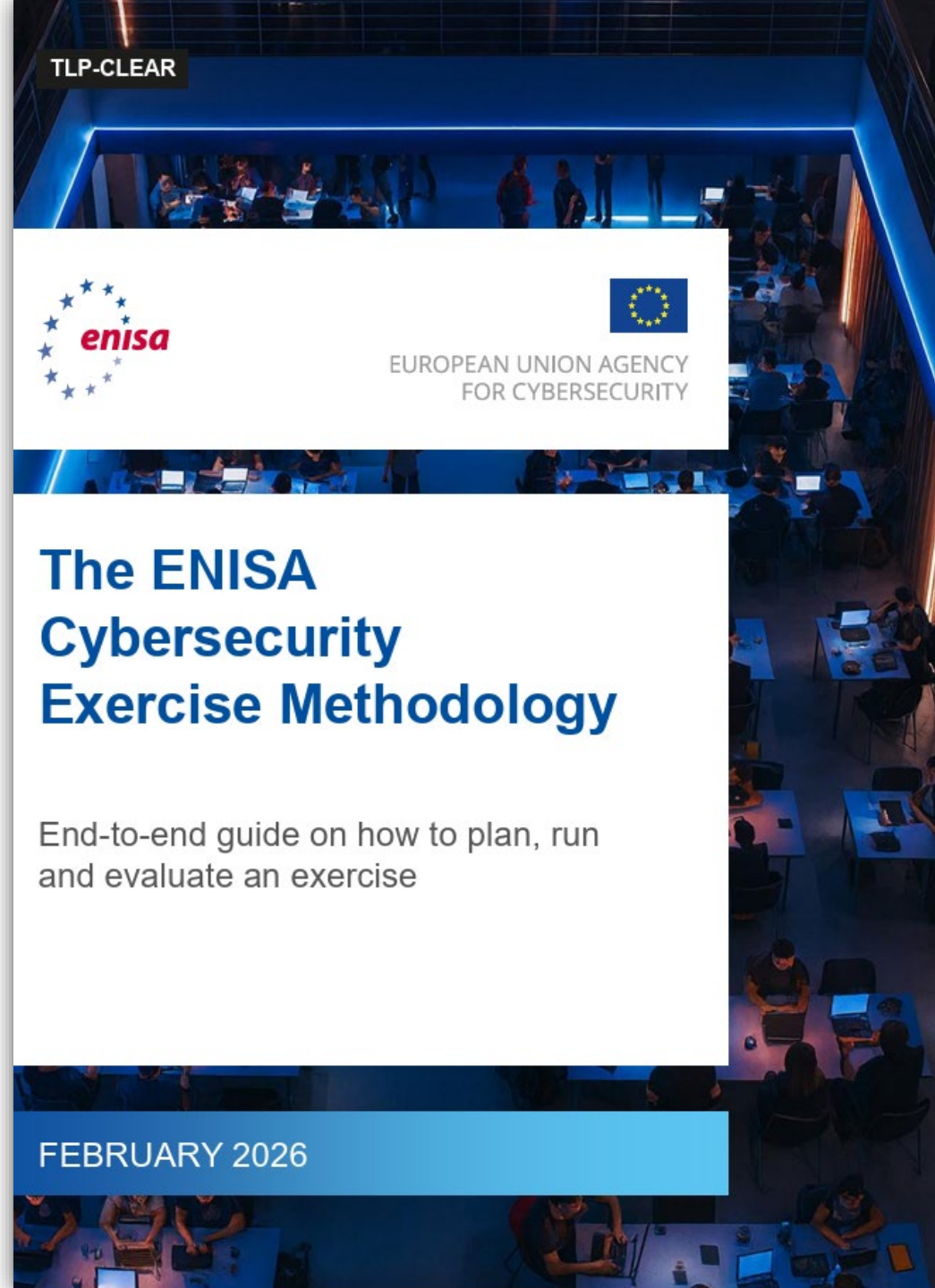
Evaluation



Methodology

An **end-to-end** framework for planning, running and evaluating cybersecurity exercises.

Highly adaptable to the exercise, country, maturity level and specific objectives.



TLP-CLEAR



EUROPEAN UNION AGENCY
FOR CYBERSECURITY

The ENISA Cybersecurity Exercise Methodology

End-to-end guide on how to plan, run
and evaluate an exercise

FEBRUARY 2026

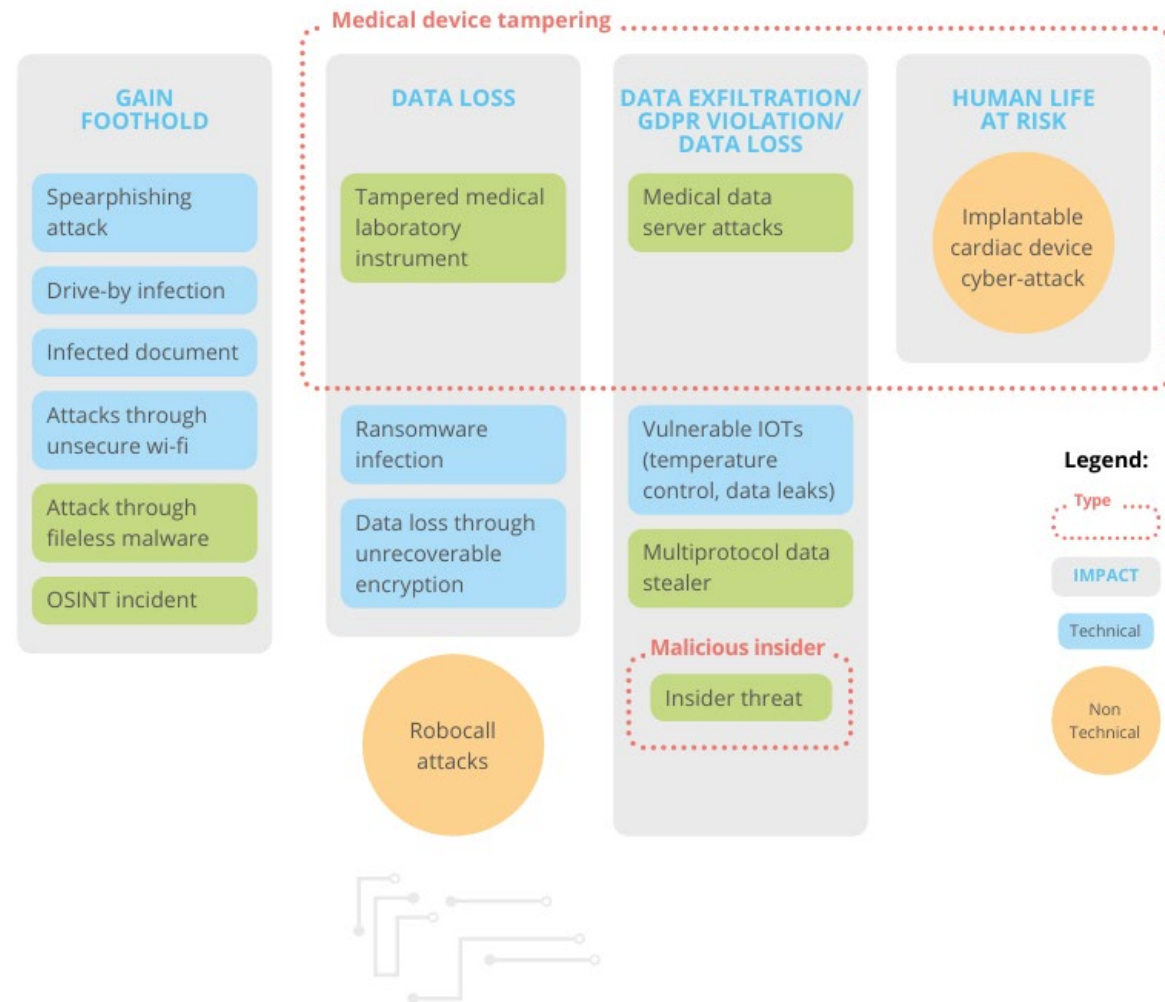
Scenario

A carefully crafted reusable scenario.

ENISA will provide a master scenario for conducting health exercises, encompassing a variety of health-related events and incidents. The scenario will be:

- **Relevant:** Designed with the health threat landscape in mind and validated by health security experts and stakeholders.
- **Modular:** Allowing Member States to tailor the scenario to their specific needs – from focused exercises to a large-scale crisis.

Overview of CE22 health technical scenario



From scenarios to exercises

Finalize scenarios

Set up support



Conduct the first exercises in 2027





Thank you for your attention

ENISA

European Union Agency
for Cybersecurity

Athens Office

Agamemnonos 14
Chalandri 15231, Attiki, Greece

Brussels Office

Rue de la Loi 107
1049 Brussels, Belgium