CYBER RESILIENCE

Co-funded by the European Union

ESCAPE. *Preparing healthcare professionals for cyberattacks*
Project No.2023-1-ES01-KA220-VET-000151536

Partners

ISTITUTO DEI SORDI
DI TORINO

Firda

PRAMMER

eolas

BBS Weser

ESCAPE. Preparing healthcare professionals for cyberattacks
Project No.2023-1-ES01-KA220-VET-000151536

Co-funded by
the European Union

This project has been co-funded with support from the European Commission. This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Table of Contents

Co-funded by the European Union

FACTSHEET – CYBER RESILIENCE

1. Definition

It is an organisation's ability to prepare for, respond to, and recover from cyber threats while maintaining patient care and operational continuity. It focuses on minimising disruptions caused by cyberattacks and ensuring the security of sensitive data1.

This concept combines business continuity, information systems security, and organisational resilience. It describes the ability to continue delivering intended outcomes despite experiencing challenging cyber events2.

2. General importance

Cyber resilience is relevant across all sectors because of digital dependence. Nowadays, governments, businesses and individuals rely on digital systems for operations, communication, and data storage. This dependence on technology has had numerous benefits, such as fast access to information, improved care coordination, and resource optimisation, among others. However, it has also increased cyber threats and attacks in scale and sophistication, making cybersecurity prevention a high-priority matter.

Another factor that makes cyber resilience an important matter that should be treated globally is its understanding that breaches are inevitable and it focus on how to adapt, recover, and thrive after incidents, not just prevent them3.

Here are some of the benefits of cyber resilience3:

- Business Continuity: Ensures critical business operations can persist during active cyber incidents, significantly reducing operational disruptions even when conventional defences are compromised.
- Reduced Downtime: Reduces the amount of time and resources that would be lost during prolonged outages by allowing organisations to quickly recover from attacks and incidents.
- Financial Protection: Reduces costs associated with system failures, data breaches, and potential legal consequences, which typically follow significant security incidents.
- Reputation management: It builds and maintains stakeholder trust by demonstrating the organisation's dependability and capability to handle unanticipated security challenges.
- Regulatory compliance: Guarantees that organisational practices adhere to the most stringent laws. Cyber Resilience, which was just launched, emphasises the increased regulatory attention being paid to this topic.
- Advantage in the marketplace: By demonstrating strong security procedures that set the company apart from less prepared rivals, it draws in security-conscious clients and partners. unprepared competitors.

3. Importance in health and care, and impact in quality of care

Modern healthcare relies on tightly linked systems. Due to the vast amount of sensitive patient data it holds and the criticality of its operations, the healthcare industry has become the prime target for cybercriminals4.

Resilience is crucial to preventing extensive service disruption because if one component fails, the effects could spread throughout the entire care infrastructure. Lives may be directly endangered if vital healthcare systems, such as electronic medical records or medical devices, are disrupted. In order to protect patient security and privacy, cyber resilience makes sure that patient care continues even in the face of attacks.

Furthermore, preserving the trust of partners, patients, and the general public depends on cyber resilience. Because patient data contains extremely sensitive information, disruptions or compromises to it can harm healthcare organisations' reputations.

4. What can I do as a healthcare professional?

- Keep a good cyber hygiene. With measures such as using strong passwords, enabling two-factor authentication, and keeping software constantly updated.
- Protect patient data. By promptly reporting any suspicious activity and carefully managing information in day-to-day tasks.
- Take part in cyber-training. By enrolling in classes that cover data breach prevention, detection, and response techniques.

5. More information

5.1 Learning Materials

- Cybersecurity for your sector (JGT-1)
- Sequential videos for general topics about cybersecurity (JGT-2)
- Web seminars about key aspects of cibersecurity (JGT-3)
- Awareness kit about cibersecurity in enterprises (JGT-4)
- Online workshop on how to set-up our device. (JGT-5)
- Cybersecurity for SMEs & self-employed (JGT-6)
- Cibersecurity guide for healthcare sector (EU scope) (JGT-7)
- Cibersecurity training from National Cryptographic Centre of Spain. Requires National login (JGT-8)
- General training (71 infopacks) about cibersecurity descriptions. Provided by cryptographic National centre. (JGT-10)
- An article exploring the current state of cybersecurity in healthcare. (IST-36)
- An article on security strategies applicable to electronic patient records (IST-37)

- An infographic on security and cybersecurity devices used in different healthcare settings. (IST-38)
- An overview of cybersecurity in healthcare, focusing on the role of AI and its regulatory framework. (IST-39)
- A compendium on the processing of patient data on online platforms. (IST-40)
- Educational project on safe and responsible digital use. (IST-41)
- Regulation of cybersecurity in healthcare (BBS-23)
- Cybersecurity of hospitals and healthcare providers (BBS-24)
- Digital Identities - With Security in Mind (BBS-25)
- Research paper on Cybersecurity and critical care staff: A mixed methods study (PRAMMER-29)
- A Critical Review on Cybersecurity Awareness Frameworks and Training Models (PRAMMER-30)
- An integrated cybernetic awareness strategy to assess cybersecurity attitudes and behaviours in school context (PRAMMER-31)
- Cyber-attacks are a permanent and substantial threat to health systems: Education must reflect that (PRAMMER-32)
- Gamification and Serious Games for Cybersecurity Awareness and First Responders Training: An overview (PRAMMER-33)
- A Serious Game for Healthcare Industry: Information Security Awareness Training Program for Hospital Universiti Kebangsaan Malaysia (PRAMMER-34)
- Systematically Applying Gamification to Cyber Security Awareness Trainings: A framework and case study approach (PRAMMER-35)
- This learning material highlights the growing role of media in the healthcare and welfare sector for both professional collaboration and client care, including attention to the consequences of media use among vulnerable groups (FIRDA-11)
- Cybersecurity for entities (HIPAA), full pack including checklists (FIRDA-12)
- Video training for professionals and students (FIRDA-13)
- Video training for professionals and students (FIRDA-14)
- Digital training in cybersecurity, fun and fast questions (FIRDA-15)
- free e-learning courses on cybersecurity in healthcare (FIRDA-17)
- Free courses to improve digital skills for health care workers (FIRDA-18)
- Online game about cybersecurity, raises awareness. (FIRDA-19)
- Online lesson about cybersecurity (FIRDA-20)
- Online game about phishing (FIRDA-21)
- Online game about cybersecurity, for general use (FIRDA-22)

5.2 Relevant Videos

This video dives into the challenge of achieving cyber resilience in the healthcare system by discussing how the digital health landscape is constantly changing. It also emphasises the relevance of building strong cybersecurity defences that are capable of adapting and recovering in real time.

What Will it Take to Build True Cyber Resilience in Healthcare?
https://youtu.be/BNsD1jKZ8Es?si=wcFCbn65VHv3aLzH

The next video focuses on how to build cyber resilience in healthcare. It offers practical advice for integrating and strengthening data security across clinical systems within a rapidly evolving digital health landscape. Their proposal is to incorporate security measures into healthcare operations to ensure that systems remain resilient to constant threats.

How to Build Cyber Resilience in Healthcare | HealthSec 2025 Keynote
https://youtu.be/U7LIBdQi78k?si=aKhDfOr3aMyzQB32

5. 3 Relevant Links

This article emphasises how inaction and underinvestment in IT resilience seriously impact patient care, operational continuity, and safety in the face of the growing threat of cyberattacks and technical outages in the healthcare industry.

https://www.mckinsey.com/industries/healthcare/our-insights/tech-resilience-for-healthcare-providers-inaction-has-a-heavy-toll?utm_source=chatgpt.com

To ensure patient care continuity even in the event of cyberattacks, the article highlights the importance of healthcare organisations prioritising cyber resilience. This can be achieved by going beyond prevention to readiness through coordinated recovery planning and strong infrastructure.

https://www.rubrik.com/blog/company/25/7/cyber-resilience-in-healthcare-preparing-for-the-inevitable-attack?utm_source=chatgpt.com

In May 2021, Ireland's Health Service Executive (HSE) fell victim to a devastating Conti ransomware attack that shut down IT systems nationwide—crippling healthcare services, exposing sensitive data, and prompting a protracted recovery involving pen-and-paper fallback and a deep post-incident review."

https://en.wikipedia.org/wiki/Health_Service_Executive_ransomware_attack?utm_source=chatgpt.com

6. Bibliography

Susnjara, S., & Smalley, I. (2025, 13 agosto). Cyber Resilience. IBM. Recuperado 18 de agosto de 2025, de

https://www.ibm.com/think/topics/cyber-resilience

Tashi, K., & Beato, F. (2024, 1 febrero). Healthcare pays the highest price of any sector for cyberattacks — that's why cyber resilience is key. World Economic Forum. Recuperado 18 de agosto de 2025, de

https://www.weforum.org/stories/2024/02/healthcare-pays-the-highest-price-of-any-sector-for-cyberattacks-that-why-cyber-resilience-is-key/?utm_source=chatgpt.com

What is Cyber Resilience and Why Does it Matter? | Fortinet. (s. f.). Fortinet.

https://www.fortinet.com/resources/cyberglossary/cyber-resilience?utm_source=chatgpt.com

ESCAPE. Preparing healthcare professionals for cyberattacks
Project No.2023-1-ES01-KA220-VET-000151536

Co-funded by the European Union

This project has been co-funded with support from the European Commission. This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.