ESCAPE:

Preparing healthcare professionals for cyberattacks

Material for learners

Cybersecurity and critical care staff: A mixed methods study

ESCAPE: Preparing healthcare professionals for cyberattacks	
Cybersecurity and critical care staff: A mixed methods study	
Language	*English*

Co-funded by the European Union

The project "ESCAPE: preparing healthcare professionals for cyberattacks" is co-funded by the European Union. The opinions and viewpoints expressed in this minute meeting solely commit to their author(s) (ESCAPE consortium) and do not necessarily reflect those of the European Union or the Servicio Español para la Internacionalización de la Educación (SEPIE). Neither the European Union nor the National Agency SEPIE can be held responsible for them.

ESCAPE: Preparing healthcare professionals for cyberattacks	
Cybersecurity and critical care staff: A mixed methods study	
Language	*English*

Table of contents

Co-funded by the European Union

The project "ESCAPE: preparing healthcare professionals for cyberattacks" is co-funded by the European Union. The opinions and viewpoints expressed in this minute meeting solely commit to their author(s) (ESCAPE consortium) and do not necessarily reflect those of the European Union or the Servicio Español para la Internacionalización de la Educación (SEPIE). Neither the European Union nor the National Agency SEPIE can be held responsible for them.

ESCAPE: Preparing healthcare professionals for cyberattacks	
Cybersecurity and critical care staff: A mixed methods study	
Language	*English*

1. Name of the material and description

This research investigates cybersecurity awareness, knowledge, and behaviors among critical care (ICU) personnel across multiple hospital sites. Using the validated HAIS-Q tool, scenario-based questions, and free-text responses, it assesses the gap between self-perceived cybersecurity awareness and actual practices. The study reveals that, despite high awareness, confidence and accurate behaviors—especially in breach recognition and reporting—are lacking. Critical factors like limited training, fatigue, and infrastructure constraints impede effective cybersecurity behavior.

2. Classification

Category	Mark if applies
Sector	☑ Healthcare (*all materials focusing specifically on the healthcare sector)*
	☐ General public *(materials targeting citizens but that are considered useful and relevant for working with the students and for the professionals, these tend to be more generic materials not targeting a specific sector)*
	☐ Other *(other materials considered relevant event though targeting a specific sector, for instance a company, but that are considered relevant for learning about cybersecurity and data protection)*
Topics covered	☑ Cybersecurity
	☐ Data protection
Situation type	☑ Prevention
	☐ Impact (i.e. when it is occurring or has occurred) on patient care. *(e.g. direct treatments, medicine distribution, etc.)*

Co-funded by the European Union

The project "ESCAPE: preparing healthcare professionals for cyberattacks" is co-funded by the European Union. The opinions and viewpoints expressed in this minute meeting solely commit to their author(s) (ESCAPE consortium) and do not necessarily reflect those of the European Union or the Servicio Español para la Internacionalización de la Educación (SEPIE). Neither the European Union nor the National Agency SEPIE can be held responsible for them.

ESCAPE: Preparing healthcare professionals for cyberattacks	
Cybersecurity and critical care staff: A mixed methods study	
Language	*English*

	☐ Impact on all other activities not involving direct patient care. *(e.g. recording data, lab tests, etc.)*
Language of the original materials	☐ Dutch
	☑ English
	☐ German
	☐ Italian
	☐ Spanish
Type of the material	☐ Guidelines or manuals
	☐ Case or examples
	☐ Training courses
	☑ Others

3. Description

This is an empirical mixed-methods study assessing critical care staff's cybersecurity awareness, confidence, and behaviors, identifying real-world barriers in high-stakes healthcare environments.

3.1. Origin

- ***Authors:*** *Kevin Hore, Mong Hoi Tan, Anne Kehoe, Aidan Beegan, Sabina Mason, Nader Al Mane, Deirdre Hughes, Caroline Kelly, John Wells, and Claire Magner.*

- ***Published in:*** *International Journal of Medical Informatics (2024), Article 105412.*

3.2. Why is it relevant/important for ESCAPE

- Focused on **frontline healthcare staff** in critical care—a group with unique pressures and consequences from cybersecurity failures.

Co-funded by the European Union

The project "ESCAPE: preparing healthcare professionals for cyberattacks" is co-funded by the European Union. The opinions and viewpoints expressed in this minute meeting solely commit to their author(s) (ESCAPE consortium) and do not necessarily reflect those of the European Union or the Servicio Español para la Internacionalización de la Educación (SEPIE). Neither the European Union nor the National Agency SEPIE can be held responsible for them.

- Highlights the **discrepancy between awareness and practice**, emphasizing the need for practical, scenario-driven training rather than theoretical modules.
- Identifies systemic and human barriers—education gaps, workload, infrastructure—that undermine cybersecurity, giving ESCAPE a grounded human-factor perspective.

3.3. Lessons learned

Study findings and implications:

- ***Awareness vs. Practice:*** *While HAIS-Q scores suggest high awareness (raw median scores between 12–15), staff lacked confidence recognizing or reporting cybersecurity incidents. Scenario-based responses revealed behavioral gaps.*
- ***Identified Barriers:***
  - *Inadequate training and education*
  - *Excessive workloads and staff fatigue*
  - *Lack of IT support and poor infrastructure*
- ***Solutions proposed:***
  - *Implement **targeted, practical training** focused on breach recognition and incident reporting.*
  - *Reduce workload-related pressures and enhance IT support accessibility.*
  - *Improve critical care infrastructure to enable safe cybersecurity practices.*

4. Direct link to the material

Available via *International Journal of Medical Informatics*, 2024, Article 105412. DOI: 10.1016/j.ijmedinf.2024.105412

Co-funded by the European Union

The project "ESCAPE: preparing healthcare professionals for cyberattacks" is co-funded by the European Union. The opinions and viewpoints expressed in this minute meeting solely commit to their author(s) (ESCAPE consortium) and do not necessarily reflect those of the European Union or the Servicio Español para la Internacionalización de la Educación (SEPIE). Neither the European Union nor the National Agency SEPIE can be held responsible for them.

ESCAPE: Preparing healthcare professionals for cyberattacks	
Cybersecurity and critical care staff: A mixed methods study	
Language	*English*

https://www.sciencedirect.com/science/article/pii/S1386505624000753?pes=vor&utm_source=scopus&getft_integrator=scopus

5. Other resources (optional)

- ***System-level responses:*** *The Irish health system's resilience in response to cyberattacks highlights staff dedication and systemic deficiencies that align with these findings.*

- ***Broader healthcare contexts:*** *Evaluations of the ECHO cybersecurity framework demonstrate persistent education and capacity challenges in healthcare organizations.*

Co-funded by the European Union

The project "ESCAPE: preparing healthcare professionals for cyberattacks" is co-funded by the European Union. The opinions and viewpoints expressed in this minute meeting solely commit to their author(s) (ESCAPE consortium) and do not necessarily reflect those of the European Union or the Servicio Español para la Internacionalización de la Educación (SEPIE). Neither the European Union nor the National Agency SEPIE can be held responsible for them.