ESCAPE:

Preparing healthcare professionals for cyberattacks

Material for learners

From Dis-empowerment to empowerment: Crafting a healthcare cybersecurity self-assessment

ESCAPE: Preparing healthcare professionals for cyberattacks	
From Dis-empowerment to empowerment: Crafting a healthcare cybersecurity self-assessment	
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	
From Dis-empowerment to empowerment: Crafting a healthcare cybersecurity self-assessment	
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	
From Dis-empowerment to empowerment: Crafting a healthcare cybersecurity self-assessment	
Language	*English*

1. Name of the material and description

*The academic article **"From Dis-empowerment to Empowerment: Crafting a Healthcare Cybersecurity Self-Assessment"** presents the development and evaluation of a healthcare-specific cybersecurity self-assessment tool tailored for the Australian healthcare sector. Unlike traditional frameworks, this tool integrates both technical and psychological empowerment aspects to improve individual and institutional cybersecurity awareness and preparedness. Using Design Science Research (DSR) methodology, the authors designed the tool to help government agencies, healthcare providers, associations, and consumers identify cybersecurity gaps and receive actionable, role-specific recommendations. The study emphasizes that empowering users—not just training them—enhances security behavior and fosters a proactive cybersecurity culture.*

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

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	
From Dis-empowerment to empowerment: Crafting a healthcare cybersecurity self-assessment	
Language	*English*

	□ Impact (i.e. when it is occurring or has occurred) on patient care. *(e.g. direct treatments, medicine distribution, etc.)*
	□ 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

3.1. Origin

This academic article was developed by researchers from ***Federation University Australia****—specifically the Global Professional School and the Institute of Innovation, Science and Sustainability. It was published in Computers & Security, a peer-reviewed scientific journal by Elsevier focused on cybersecurity research. The authors represent a collaboration between academic experts in cybersecurity, healthcare systems, and user-centered research methodologies.*

3.2. Why is it relevant/important for ESCAPE

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.

This material is highly relevant to the ESCAPE project, aiming to raise cybersecurity awareness among healthcare employees. It presents a healthcare-specific, self-administered cybersecurity assessment tool that combines technical and psychological empowerment elements, helping healthcare workers and institutions identify their cyber vulnerabilities and build confidence to take preventive action. It supports ESCAPE's objectives by:

- *Promoting shared responsibility and user engagement*
- *Offering sector-specific recommendations*
- *Encouraging proactive cybersecurity behavior in both technical and non-technical healthcare staff*

3.3. Lessons learned

Lessons learned

Guidelines or Manuals

The Objective of the material is to present the development and validation of a self-assessment cybersecurity index tailored for the Australian healthcare sector. Its purpose is to help healthcare professionals, organizations, government agencies, and even consumers evaluate their cybersecurity posture and enhance both technical preparedness and psychological empowerment.

The target group is Healthcare providers (hospitals, clinics, professionals); Government agencies and associations; Healthcare consumers (patients and the public)

Risks addressed:

- *Phishing, ransomware, data breaches, and insider threats*
- *Low cybersecurity awareness among non-IT staff*
- *Disempowerment and lack of ownership in following cybersecurity protocols*
- *Delays in patient care and damage to public trust from breaches (e.g., Medibank and MediSecure incidents)*

Solutions and contingency measures proposed:

- *A tailored self-assessment index covering four domains:*
    1. *Understanding incidents*

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.

6

2. *Strategy*
3. *Culture*
4. *Training*

- *Generation of customised, actionable feedback for each user group*
- *Emphasis on psychological empowerment: building confidence, responsibility, and engagement with cybersecurity practices*
- *Design accessible, plain-language tools suited to different stakeholder literacy levels*

Tips & tricks for implementation

- *Make the tool available anonymously online to encourage honest participation*
- *Use clear, jargon-free language and adjust questions to the user's role*
- *Avoid rigid scoring systems; instead, offer qualitative feedback and improvement plans*
- *Encourage users to self-reflect and follow up with linked educational resources*
- *Promote collaboration across stakeholders by sharing aggregated findings and best practices*

4. Direct link to the material

Insert direct URL to the materials

https://www.sciencedirect.com/science/article/pii/S016740482400453X?pes=vor&utm_source=scopus&getft_integrator=scopus

5. Other resources (optional)

No other resource.

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.