ESCAPE:

Preparing healthcare professionals for cyberattacks

Material for learners

A Critical Review on Cybersecurity Awareness Frameworks and Training Models

ESCAPE: Preparing healthcare professionals for cyberattacks	
A Critical Review on Cybersecurity Awareness Frameworks and Training Models	
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	
A Critical Review on Cybersecurity Awareness Frameworks and Training Models	
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	
A Critical Review on Cybersecurity Awareness Frameworks and Training Models	
Language	*English*

1. Name of the material and description

This open-access, quantitative review evaluates multiple approaches to cybersecurity awareness and training—framing them as strategic initiatives that reduce security incidents and organizational costs while improving resilience and overall cybersecurity posture. The analysis emphasizes real-world evidence of the effectiveness of structured awareness and training programs.

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.)*
	☐ Impact on all other activities not involving direct patient care. *(e.g. recording data, lab tests, 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	
A Critical Review on Cybersecurity Awareness Frameworks and Training Models	
Language	*English*

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 evidence-based literature review that applies quantitative methods to assess cybersecurity awareness frameworks and training models against cost reduction, incident prevention, and resilience enhancement outcomes.

3.1. Origin

- ***Author:*** *Hamed Taherdoost.*
- ***Publication:*** *Procedia Computer Science, Volume 235, April 2024, Pages 1649–1663. Open access under a Creative Commons license.*

3.2. Why is it relevant/important for ESCAPE

- **Quantitative evaluation**: Offers stakeholders a grounded, data-driven understanding of what training and awareness methods truly impact organizational resilience.
- **Strategic insights**: Highlights that structured awareness initiatives not only cut costs and incidents but also act as accelerators for cyber resilience—a clear value-add for organizations designing training interventions.

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.

3.3. Lessons learned

Review insights:

- ***Introduction:*** *Emphasizes how structured cybersecurity awareness frameworks and training can produce measurable improvements in security posture and cost-efficiency.*

- ***Target audience:*** *Ideal for organizational leaders, training developers, and policymakers keen on investing in effective, evidence-based cybersecurity education.*

- ***Risks addressed:*** *Inefficiencies in training, rising security incidents, and lack of demonstrable ROI on awareness programs.*

- ***Solutions proposed:*** *Evaluate training approaches quantitatively, focusing investment on methods that demonstrably reduce risk and costs.*

- ***Tips for implementation:***

    - *Use metrics to assess training effectiveness (e.g., incident rate changes, cost benefits).*

    - *Incorporate quantifiable goals into awareness initiatives to justify resource allocation and demonstrate value.*

4. Direct link to the material

Accessible via *Procedia Computer Science*, Volume 235 (2024), Pages 1649–1663. DOI: 10.1016/j.procs.2024.04.156
https://www.sciencedirect.com/science/article/pii/S1877050924008329?via%3Dihub

5. Other resources (optional)

Related frameworks & evaluations

- *Taherdoost's broader review of cybersecurity frameworks and standards (2022).*
- *Analytical comparisons of cybersecurity training capabilities and models across sectors.*

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.

Supporting theories and interdisciplinary approaches

- *Human-centric cybersecurity models grounded in behavioral, social, and organizational dimensions.*

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.

7