“We trust Facebook, we trust mobile apps, but we don’t trust our own healthcare system like MyHealthRecord”: Preparing users for healthcare cybersecurity attacks.

Wendy Burke[1], A/Prof Andrew Stranieri[1], Dr Taiwo Oseni[1], Prof. Iqbal Gondal[2] & Dr Charlynn Miller[3]

[1] Federation University, Ballarat, Victoria
[2] RMIT University, Melbourne, Victoria
[3] DeakinCo, Melbourne, Victoria

2022 Australian Computer Science Week

Scenario: FeelBetter Health Service

Location: Regional Victoria

Attributes: Approx. 4000 staff, 4 campuses, 800 beds, treats 60,000 inpatients and 80,000 emergency attendances. Integrated EMR, EDIS, Roster-On, iPIMS, patient flow portal, CERNER, IIMIS, patient transport portal, HETI eLearning etc.

Current Environment: Increased number of attempted IT security breaches causing disruption across the Service. Cybersecurity is extreme on the risk register.

Push for cloud-based clinical software.

Ad hoc ability to assess cybersecurity mitigation techniques, cyber-response readiness, and capabilities.

ISSUE: How does the organisation measure its preparedness to prevent and manage cybersecurity attacks?

Research Objectives

- Identify tools that enable the healthcare sector to gauge their preparedness for cybersecurity and cyber-resilience.
- Identify essential components required in a healthcare sector cybersecurity index by evaluating currently available generic indexes.
- Develop a cybersecurity index for the Australian healthcare sector.

What do we know so far?

- There is a lack of tools that allow the healthcare sector to evaluate its cybersecurity vulnerabilities.
- Cybersecurity frameworks, tabletop exercises and cybersecurity tools exist but these are best used once a robust defence system is in place.

Cybersecurity Indexes

What are they? An index is made up of a series of questions, often broken into categories. These categories target areas such as law, technical responses, organisational threats, capacity building, and social context. Some indexes provide ranking capabilities against other countries, while others directly evaluate what it means to be cyber-ready.

Problem? Indexes allow insight into potential vulnerabilities within an organisation or country, but they are often generic. The healthcare sector has unique features requiring a customised solution.

Unlike cybersecurity frameworks, cybersecurity indexes are often written in isolation by organisations and universities.

Healthcare Cybersecurity Index

- Designed for the whole Australian healthcare sector – Government, Healthcare Associations, Healthcare Organisations and Healthcare Consumers.
- Users are presented with a series of questions that relate to areas such as:
  - Cybersecurity policy and strategy
  - Cybersecurity mindset and awareness
- After answering the questions, a report is generated with advice to assist in strengthening that area.
- Everyone has a role to play.

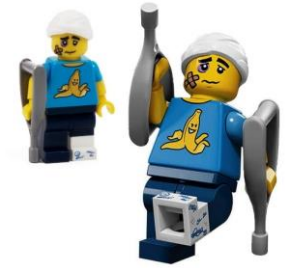
Example

Question for Healthcare Organisations (e.g. FeelBetter Health Service):

1. Has your organisation created a way to identify healthcare cybersecurity incidents?
2. Is there a national-level process for identifying healthcare cybersecurity incidents?
3. Is there regular sharing of healthcare cybersecurity threats and vulnerability information and operational good practices between the government and the organisation?
4. Do associations promote internal mechanisms for identifying healthcare cybersecurity incidents to your organisation?

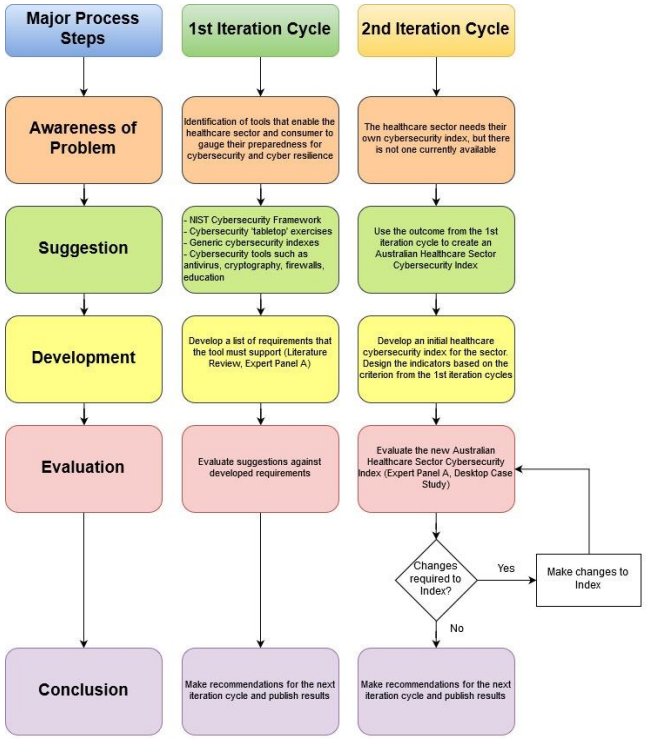
Advice to Healthcare Organisations:

- Advocate the need for a national-level healthcare cybersecurity incident reporting mechanism.
- Create internal procedures to report healthcare cybersecurity incidents.
- Consider undertaking an awareness program so that employees can identify healthcare cybersecurity incidents.



Design Science Research (DSR)

- DSR is concerned with reducing the gap between theory and practice. It is not overly concerned with understanding the problem, but with the potential solutions.
- There are five distinct process steps of DSR; awareness of the problem, suggestions, development, evaluation and conclusion.



How you can help!

As a representative of the Government, healthcare sector, or as a computer security expert we are interested in inviting you to participate in this research. If you agree to participate, we will ask you to share your insights about healthcare and cybersecurity by reading and providing feedback on a draft healthcare cybersecurity index. You will receive a list of questions to guide you in reviewing the index.

If you have any questions, or you would like further information regarding the project titled **A review of a new healthcare cybersecurity index for Australia** please contact the Principal Researcher, Associate Professor Andrew Stranieri of the School of Engineering, Information Technology and Physical Sciences.

EMAIL: a.stranieri@federation.edu.au

PH: +61 3 5327 9283

The ethical aspects of this research project have been approved by the Human Research Ethics Committee of Federation University Project Number B21-148