A Systematic Literature Review of Cybersecurity Approaches to Healthcare Worldwide

Azadeh Khodadadi

Department of Computing Technologies, Swinburne University of Technology, Australia, akhodadadi@swin.edu.au, az.khodadadi27@gmail.com

Armita Zarnegar

Department of Computing Technologies, Swinburne University of Technology, Australia, azarnegar@swin.edu.au

Wendy Burke

Federation University Australia, Ballarat, Australia, w.burke@federation.edu.au

Abstract

With the increase in cyberattacks and online threats, health information has become more vulnerable due to its sensitive nature. It is crucial to assess the security and vulnerabilities of these systems to safeguard them against potential breaches. Focusing on the health sector, this systematic review examines cybersecurity and self-assessment frameworks used throughout the world. Following the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) methodology, 43 relevant publications were selected from an initial pool of 1,366 records. Firstly, frameworks were assessed based on the region (Australia, US, UK, and other countries). Secondly, their specificity to the healthcare domain, effectiveness in prevention or defence, scalability to different organisational sizes, and responsiveness to emerging technologies were reviewed. The findings reveal a critical shortfall in self-assessment tools that are explicitly designed for the healthcare context, particularly in Australia. This gap highlights the need for more targeted, evidence-based self-assessment frameworks to enhance cybersecurity preparedness in healthcare organisations.

Background

The integration of digital technologies in healthcare has undeniably transformed patient care and administrative processes, offering improved efficiency, accessibility, and personalised care. However, this digital transformation has also introduced substantial cybersecurity risks.

To reduce the risk of cyberattacks, healthcare organisations can either respond reactively during an attack or proactively assess their cybersecurity posture using self-assessment frameworks. In the first approach or the reactive response, early identification of cyber threats can significantly improve the chances of successful mitigation. This requires a number of steps, including recognising the type of attack, selecting the appropriate defence measures, as well as keeping technologies up-to-date. The proactive response, which concentrates on cybersecurity self-assessment, is the primary focus of this review.

Cybersecurity self-assessment frameworks (sometimes termed Cybersecurity Indexes) are a structured set of questions designed to evaluate an organisation's readiness across all critical areas of cybersecurity. By answering these questions, organisations can assess their preparedness and resilience against potential security threats. These tools also provide healthcare organisations with the ability to gauge their maturity and prioritise areas for improvement. This study undertakes a systematic review of existing cybersecurity and self-evaluation frameworks relevant to the healthcare sector.

Methodology

This review adheres to the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines, which offer a structured and evidence-based framework for conducting and reporting systematic reviews. The PRISMA methodology ensures transparency and reproducibility by providing a detailed checklist and flow diagram to document each stage of the review process, from study identification to final inclusion.

A systematic search was conducted across three major electronic databases: Google Scholar, Scopus, and IEEE Xplore. The search targeted literature published between January 2019 and December 2024. The following Boolean keyword combination was used to identify relevant studies:

("cybersecurity" OR "cyber security") AND ("framework" OR "self-assessment framework") AND ("healthcare" OR "health care").

This search strategy was designed to capture a broad range of cybersecurity frameworks applicable to the healthcare sector, including both academic research and industry or government-developed frameworks. To ensure the quality and relevance of the studies included in this review, clearly defined inclusion and exclusion criteria were applied. Studies were considered eligible for inclusion if they were published in English, appeared between January 2019 and December 2024, and focused on cybersecurity or self-assessment frameworks specifically within healthcare contexts. Eligible sources included peer-reviewed journal articles, conference proceedings, and credible government or industry reports that addressed the development, implementation, or evaluation of cybersecurity strategies relevant to healthcare systems. Articles that focused solely on general IT or cybersecurity without a healthcare application, or those lacking methodological rigour, were omitted.

A total of 1,366 research articles (including duplicates) were identified in the initial search process. These consisted of 630 articles from IEEE Xplore, 636 from Scopus, and 100 from Google Scholar, alongside 15 organisational frameworks, as illustrated in Figure 1. After duplicate removal and title/abstract screening, 1090 articles were shortlisted for detailed assessment. Based on a full-text review and the inclusion/exclusion criteria, a total of 38 papers were selected, including 4 from IEEE Xplore, 18 from Scopus, as well as five organisational reports, resulting in a total of 43 articles.

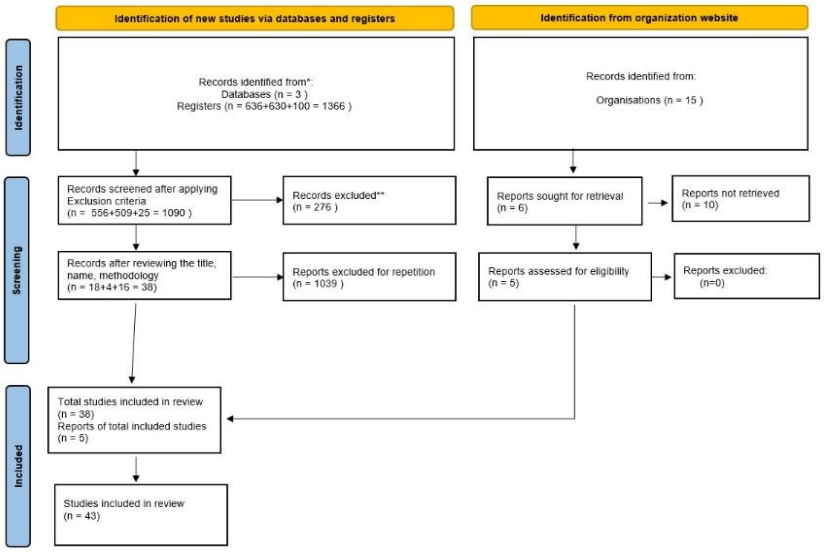

Figure 1: The PRISMA guidelines

Contribution

This literature review examined 43 cybersecurity frameworks used in the healthcare sector across countries like the US, UK, and Australia, focusing on their domain specificity, scalability, and responsiveness to emerging technologies. It found a wide range of frameworks—derived from sources like NIST, ISO/IEC, and Zero Trust—serving various purposes such as compliance, resilience, and medical device safety. Notable contributions include Australia's Essential Eight and ADHCF.

A key finding is that no single framework fits all healthcare organisations, particularly smaller or resource-limited ones. Many frameworks are either too complex or too generic for practical use in such contexts. The review argues for a flexible, self-assessment cybersecurity framework tailored to healthcare, allowing organisations to benchmark and improve their security posture based on size, risk, and technology readiness. Future research should explore designing such a tool, especially in local contexts like Victoria, to ensure it aligns with evolving threats and emerging technologies.