DIGITAL HEALTH
Volume 9: 1–15
© The Author(s) 2023
Article reuse guidelines:
sagepub.com/journals-permissions
DOI: 10.1177/20552076231191095
journals.sagepub.com/home/dhj

# CYBER-AIDD: A novel approach to implementing improved cyber security resilience for large Australian healthcare providers using a Unified Modelling Language ontology

Martin Dart and Mohiuddin Ahmed

## Abstract

**Purpose:** This paper proposes a novel cyber security risk governance framework and ontology for large Australian healthcare providers, using the structure and simplicity of the Unified Modelling Language (UML). This framework is intended to mitigate impacts from the risk areas of: (1) cyber-attacks, (2) incidents, (3) data breaches, and (4) data disclosures.

**Methods:** Using a mixed-methods approach comprised of empirical evidence discovery and phenomenological review, existing literature is sourced to confirm baseline ontological definitions. These are supplemented with Australian government reports, professional standards publications and legislation covering cyber security, data breach reporting and healthcare governance. Historical examples of healthcare cyber security incidents are reviewed, and a cyber risk governance UML presented to manage the defined problem areas via a single, simplified ontological diagram.

**Results:** A clear definition of 'cyber security' is generated, along with the 'CYBER-AIDD' risk model. Specific examples of cyber security incidents impacting Australian healthcare are confirmed as N = 929 over 5 years, with human factors the largest contributor. The CYBER-AIDD UML model presents a workflow across four defined classes, providing a clear approach to implementing the controls required to mitigate risks against verified threats.

**Conclusions:** The governance of cyber security in healthcare is complex, in part due to a lack of clarity around key terms and risks, and this is contributing to consistently poor operational outcomes. A focus on the most essential avenues of risk, using a simple UML model, is beneficial in describing these risks and designing governance controls around them.

## Keywords

Cyber security, risk management, healthcare, Australia, UML

Submission date: 17 January 2023; Acceptance date: 13 July 2023

## Introduction

The healthcare industry has been a significant consumer of information and communications technology (ICT) innovation since the introduction of digital networks and databases in the 1960s. As this usage has grown, it has presented an emergent challenge for healthcare providers, who have sought to exploit the benefits of this

School of Science, Edith Cowan University, Joondalup, WA, Australia

**Corresponding author:**
Martin Dart, School of Science, Edith Cowan University, Joondalup, WA 6027, Australia.
Email: m.dart@ecu.edu.au

rapidly emerging digital industry, while avoiding the inevitable vulnerabilities such complex new technology also delivers.

The growth in both human populations and the sophistication of medical services has placed increasing importance on these digitally enabled services, such as those multiple hospital systems delivered via Australia's state and territory governments or private healthcare businesses. This is a risk most recently recognised by the Commonwealth government of Australia with amendments to the Security of Critical Infrastructure Act 2018 (Cth),[1] which classifies any health provider operating an intensive care unit as an asset of critical national infrastructure requiring mandatory risk protection governance. It is these types of services that are the focus of this paper and are referred to throughout as large Australian healthcare providers, or 'LAHPs'.

Part of this challenge has been how to effectively implement the emergent security risk control frameworks which have also evolved, and which define prescriptive and systemic management processes. These large frameworks require the structured discovery and recording of assets (physical and data), the identification and prioritisation of risks to those assets, and the identification of controls to apply to each component. This is a complex and expensive undertaking which general ICT support teams, and clinically trained or business-focussed risk managers, have struggled to implement effectively in many LAHPs. With unique legal, technical and social structures influencing Australian healthcare delivery, this paper seeks to clarify and define these risks to LAHP data and technology systems, and propose an alternative (but complimentary) simpler approach to establish.

In the literature, a theme emerges around a lack of research investigating how healthcare providers can prioritise cyber security risk management, especially with staff members who lack expertise in the area. This is evidenced via the comprehensive bibliographic analysis of healthcare and cyber security conducted by Jalali et al.,[2] where the authors identified the majority of their 472 verified sources originating from technically focussed science fields, which led them to conclude:

> This focus on the technological aspects of cyber security suggests that nontechnological variables (human–based and organisational aspects, strategy, and management) may be understudied.

This theme was also prefaced some 13 years earlier by Williams,[3] who summarised:

> Research into the protection of sensitive medical data is often technically focused and does not address information systems and behavioural aspects integral to effective information security implementation.

Finally, Warren and Leitch[4] also identified that healthcare requires more than improved technical solutions, highlighting instead the need for:

> (an) information systems security design method that effectively models and evaluates both the technical and social aspects of information security.

## Methods

This paper utilises aspects of empirically based evidence discovery and phenomenological review, in a mixed-methods approach to achieve an ultimately improved and novel ontological model. The methodology to achieve this was undertaken across three phases, being:

1. Literature review: identifying the phenomena contributing to the underlying cyber security healthcare problem and ascertaining the key baseline definitions. Discovering and building on the work of multiple authors to define key aspects of cyber security and cyber resilience, particularly Schatz et al.[5] to concisely define 'cyber security' based on their semantic analysis of 28 definitive sources.
2. Analysing multiple quantitative data sources: confirming the problem scope in an Australian context by reviewing published evidence from the Australian Cyber Security Centre (ACSC), Office of the Australian Information Commissioner (OAIC), and Australian Digital Healthcare Agency (ADHA), and linking the cyber security and resilience definitions from stage 1 to those known risks most likely to impact them.
3. Completing a novel ontological design using UML modelling, to create a simple governance framework that LAHPs could realistically adopt. The construction of this bespoke ontological model, using the clarity offered by UML modelling, provides a simplified single-view of the required high-level governance processes required to achieve improved cyber resilience.

This combined approach is undertaken in order to integrate aspects of two highly complex domains: cyber security and large healthcare environments.

In seeking to reduce ontological ambiguity in support of improved LAHP cyber resilience, this paper recognises the importance of considering the influence of people and human psychology in ensuring effective cyber resilience.[2–4] This leads to the adoption of distinct Soft Systems Methodology (SSM) concepts, such as that articulated by Checkland,[6] in his approach of using SSM to seek 'practical and achievable' outcomes within complex systems. A further justification for this SSM approach, as opposed to a purely scientific-positivist methodology, is to overcome the problem concisely defined by Avorn,[7] who wrote:

> In reality, we [clinicians and patients] are all influenced by seemingly irrational preferences in making choices about reward, risk, time, and trade-offs that are quite different from what would be predicted by bloodless, if precise, quantitative calculations.

## Literature review

To precisely define and scope the cyber security risk and governance themes and criteria relevant to this study, this section explores the existing literature in order to discover what material already exists and is applicable, or where gaps or anomalies might exist in either the specific data or the methods used to obtain it.[8] Papers were sourced via an initial Google Scholar search for articles with the phrase 'medical cyber risk governance', and using the 'related articles' option where relevant papers were identified from reading their abstracts.

Other studies into healthcare cyber security risk have been undertaken, although, the lack of practical procedural guidance included in these, or their specialist skills requirements, restricts their general applicability to LAHP cyber risk governance. This includes the work of:

- Webb and Dayal,[9] who reviewed overall cyber security risk profiles in medical devices, but did not provide a bespoke framework for implementing remediations, focussing instead on existing standards from NIST, ISO and the therapeutic good administration (TGA).
- Schwartz et al.[10] reviewed the lifecycle of medical devices, commenting on the need for a standards-based approach and detailing the approaches used by regulators and governments, but not including guidance for healthcare end consumers.
- Thomasian and Adashi[11] provided a more detailed risk review, including a 'taxonomy of harm' that included impacts on the confidentiality, integrity and availability of medical devices. Their ultimate framework for managing risk was to apply the NIST CSF standards-based approach.
- Falco et al.[12] created a guide, the 'Cyber Crossroads', which identified many relevant cyber risk issues, and also confirmed that the high cost and complexity of undertaking the standards-based approach was limiting for healthcare providers. The report identifies a simplified and bespoke high-level governance process but does not detail the specifics of addressing targeted cyber risks.

### Cyber definitions

In considering the growing threat landscape LAHPs face a significant challenge in operationalising justified and costed actions, founded on clear semantic meaning that supports agreement between vendors, technologists and clinical staff. 'Cyber security', 'cyber risk', 'cyber governance', 'cyber space', 'risk management' and 'information security' are just some of the closely related terms that may be used interchangeably to describe risks or activities. Even more fundamentally, adding the prefix 'cyber' to myriad other words to create new phrases may deliver no obvious semantic meaning at all. Terms such as 'cyber threat', 'cyber operations', 'cyber-attack', or 'cyber warfare' may introduce ambiguity or confusion for audiences – especially interdisciplinary ones – regarding what is being described.[13] These problematic aspects of semantic and pedagogical definitions and interpretation are indicative of the understudied yet important aspect of *people* – and the phenomenological cultures they create and work within, of which LAHPs are a prime example.

A starting point should therefore be that cyber-*anything* denotes those aspects of the LAHP processes-of-interest which intersect with digital information management or communications systems. These elements can cover any one of the five areas of: (1) physical infrastructure, (2) communication networks, (3) information processing systems, (4) devices or (5) virtual environments. In any combination, these elements can be referred to as 'cyber space'.[14]

To avoid an abstract and incomplete series of definitions based purely on a technical-positivist approach, it is vital to note the important roles that people play within the LAHP context of seeking to understand cyber space. It is people who assign value to data, and a myriad of conflicting personality traits and cognitive processes are present in them as the users, designers and maintainers of LAHP systems – and effective cyber security cannot be achieved without consideration of them.[15] Security within a LAHP comprising of 130,000 clinical users (such as in the New South Wales state healthcare system) is not therefore a zero-sum approach of establishing a single secure configuration to defeat all attacks and possible risks. Instead, an accommodation of hundreds of distinct social, language, political and cultural backgrounds needs to feed into a security culture that users will accept, understand and regularly apply to their everyday work.[3,16,17]

### Cyber security versus information security

Against this large and complex organisational context, cyber security and cyber risk management should be seen as a subset of the overarching process of information security,[18,19] which provides common policy and reporting requirements to both the cyber and physical domains. Nesting cyber security within information security in this manner recognises that there are requirements for information security management which remain purely physical and are managed outside of cyber space.[20] An illustration of a typical LAHP information security ecosystem, and the distinct zone that cyber space occupies, is included in Figure 1. The area within the shaded central 'cyber space' zone includes non-exhaustive examples of the scope of cyber security risks that could be managed via the model proposed in this paper.

As 'cyber security' is a key term used throughout this paper, it is important to highlight the thorough work on defining it undertaken by Schatz et al.,[5] who processed 28 academic, government and industry source definitions of 'cyber security' via a semantic similarity analysis. Their final output was the creation of the most representative definition of cyber security yet seen, which this paper supplements with the underlined text below (based on the definitions for common vectors of cyber security failure, which will be detailed later in this paper):

> (Cyber security is…) the approach and actions associated with security risk management processes followed by organisations…to protect the confidentiality, integrity and availability of data and assets used in cyber space from attacks, incidents, data breaches, and data disclosures.

## Cyber security or cyber resilience?

A final aspect to define is the concept of 'security' itself. Too often, this is presented a binary choice of a system or process either being secure – or not. In reality, the concept is a sliding scale, where a system's security status is dependent upon multiple interacting elements that might include timeliness, group knowledge, legislative requirements, or other service-specific aspects. Together, this creates a dynamic web of *trustworthiness* – built on evidence that a system can operate within its design parameters, and perform dependably and reliably in the face of passive failures or active threats.[21]

'Cyber resilience' is the term given to a system's capacity to maintain its status of… *reliability and dependability in the face of persistent threats*.[22] The December 2022 edition of the Australian Government's Information Security Manual (ISM)[23] defines it similarly as, '*the ability to adapt to disruptions caused by cyber security incidents while maintaining continuous business operations*'.

Pursuing resilience as opposed to seeking *formal proof* of absolute security[24] is therefore a practical approach given the dynamic challenges persistent throughout LAHP systems, stemming from their complexity, heterogeneity and rapid rate of change. As such, it is called out as a key concept in the 2022–2025 Cyber Security Strategy for the Australian Digital Health Agency (the national governments' peak health organisation), which states that its three-year vision is to achieve, '*Cyber security that enables the next frontier of digital health by supporting a resilient healthcare ecosystem*'.[25]

The Australian Cyber Security Centre's (ACSC) Annual Cyber Threat Report for 2022 also focuses on resilience, where it is mentioned 21 times and forms a foundation for the ACSC's planned 10-year strategic response to the current threat environment, known as REDSPICE (Resilience, Effects, Defence, Space, Intelligence, Cyber, Enablers).[26]

Adopting an approach towards increased resilience also helps manage the time and budget limitations that a purely standards-based approach of executing deep and bespoke risk assessments can bring. This is a particular problem for LAHPs where disparate technical and management capabilities make the six steps of risk management (shown in Table 1, as published by the US National Institute for Standards and Technology[27] and the Australian Cyber Security Centre)[23] impractical, leading to the persistence of many preventable risks.

Pursuing a more flexible approach towards cyber resilience in LAHPs, based on the practical knowledge of just how LAHPs actually suffer from cyber risks, can enable multiple aspects of these risk reduction and recovery options to apply in the right measure at the right time, without the gridlock that can otherwise ensue from getting stuck at stages 1 or 2 in the risk management process.

Resilience also accepts that bad things will happen to systems on occasion despite all best efforts, and the important outcome is being able to accommodate such incidents and recover from them with as little impact as possible. This does not necessarily equate to such systems being *insecure*, but in being *secure enough*.

## Cyber security failures in healthcare

There are many media and industry reports claiming that healthcare is the most breached, attacked, or vulnerable industry in Australia.[28–30] While such headlines may cause concern for those working in the industry, they rarely provide enough analysis to create a meaningful 'lessons learned' for LAHPs to apply and reduce their own operational risks. Precisely identifying the key vectors of these reported failures in LAHP systems is important, as there are varying risk impacts and treatments depending on whether a LAHP is seeking to manage 'vulnerabilities' as opposed to 'cyber-attacks' or 'data breaches'.

Porcedda[31] examined aspects of this problem with a review of various European data protection legislation and identified a need to describe more than just 'breaches'. The author defined breaches as being comprised of 'events', leading to …*destruction*, *loss*, or *disclosure* of data. However, while Porcedda helped focus these data breach definitions, they did not include a focus on the contributory causes of targeted and malicious cyber-attacks. To achieve a separation and full definition of the high-level cyber failures that could impact on a LAHPs ability to achieve cyber

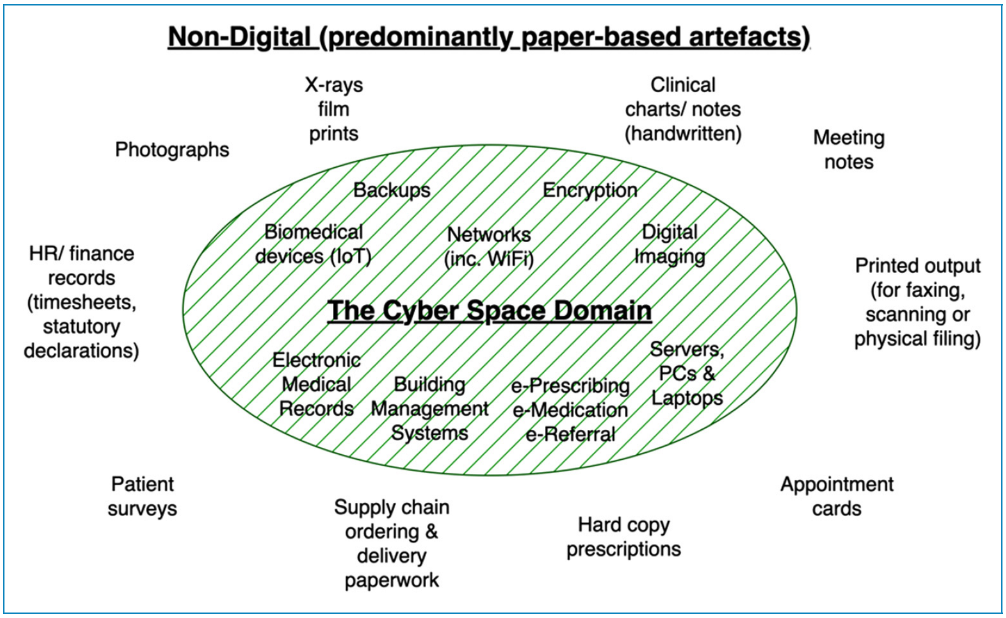
Non-Digital (predominantly paper-based artefacts)
X-rays film prints
Clinical charts/ notes (handwritten)
Photographs
Meeting notes
Backups
Encryption
Biomedical devices (IoT)
Networks (inc. WiFi)
Digital Imaging
HR/ finance records (timesheets, statutory declarations)
Printed output (for faxing, scanning or physical filing)
The Cyber Space Domain
Electronic Medical Records
Building Management Systems
e-Prescribing e-Medication e-Referral
Servers, PCs & Laptops
Patient surveys
Supply chain ordering & delivery paperwork
Hard copy prescriptions
Appointment cards

Figure 1. The information security (physical) and cyber space domains in healthcare.

Table 1. ACSC and NIST risk management stages.

| Stage | Risk management process |
|---|---|
| 1 | Define and categorise the system: using risks based on likelihood, threats, vulnerabilities and potential for loss of life |
| 2 | Select controls: and tailor controls to reduce risk to an acceptable level |
| 3 | Implement controls: and describe how they are employed with the environment |
| 4 | Assess controls: to determine if they are producing the desired outcomes |
| 5 | Authorise the system: based on its operational risk and controls baseline |
| 6 | Monitor the system: by reviewing the approved controls and documenting changes |

resilience, this paper expands Porcedda's classification work and combines it with the empirical findings of the ACSC's 2022 Annual Cyber Threat Report,[26] the OAIC's Notifiable Data Breach (NDB) scheme, and the ADHA's 2022–2025 Cyber Security Strategy.[25]

In their 2022 Annual Cyber threat Report, the ACSC details 76,000 cyber-related crimes or incidents (up 13% from the previous year) and 25,226 new publicly reported software vulnerabilities (up 25%) and concluded that '*ransomware attacks represent the most destructive cybercrime threat*'.[26] In summarising their findings relating to cyber defence and resilience, the ACSC concludes that the blurring of home and work life, coupled with increasing device interconnectivity, presents many more opportunities for malicious actors to conduct targeted or opportunistic attacks.

In considering the existing literature alongside the ACSC and OAIC data and the ADHA's stated strategy, this paper focuses on four priority cyber security areas. These consolidated categories, which represent the prioritised opportunities to manage both inbound threats and data exfiltration risks to which LAHPs are particularly vulnerable, are: (1) attacks, (2) incidents, (3) data breaches and (4) data disclosures. These can be summarised using the 'CYBER-AIDD' acronym and are illustrated in Figure 2, which shows that the central role people occupy in facilitating the encroachment of attack and incident-based risks into the protected perimeter, despite the presence of multiple control processes that may be comprehensive in content. Of importance in this diagram are the four green paths of escalation, which represent the controllable interfaces that LAHPs should better manage to intercept or divert these risks, to avoid the ultimate realisation of data breaches or data disclosures from occurring.

## Attacks

There is an increasingly sophisticated and capable global risk from organised crime, citizen activists, government intelligence agencies and other government-funded or issue-motivated groups to target networks for deliberate attack (including LAHP networks). These are the so-called

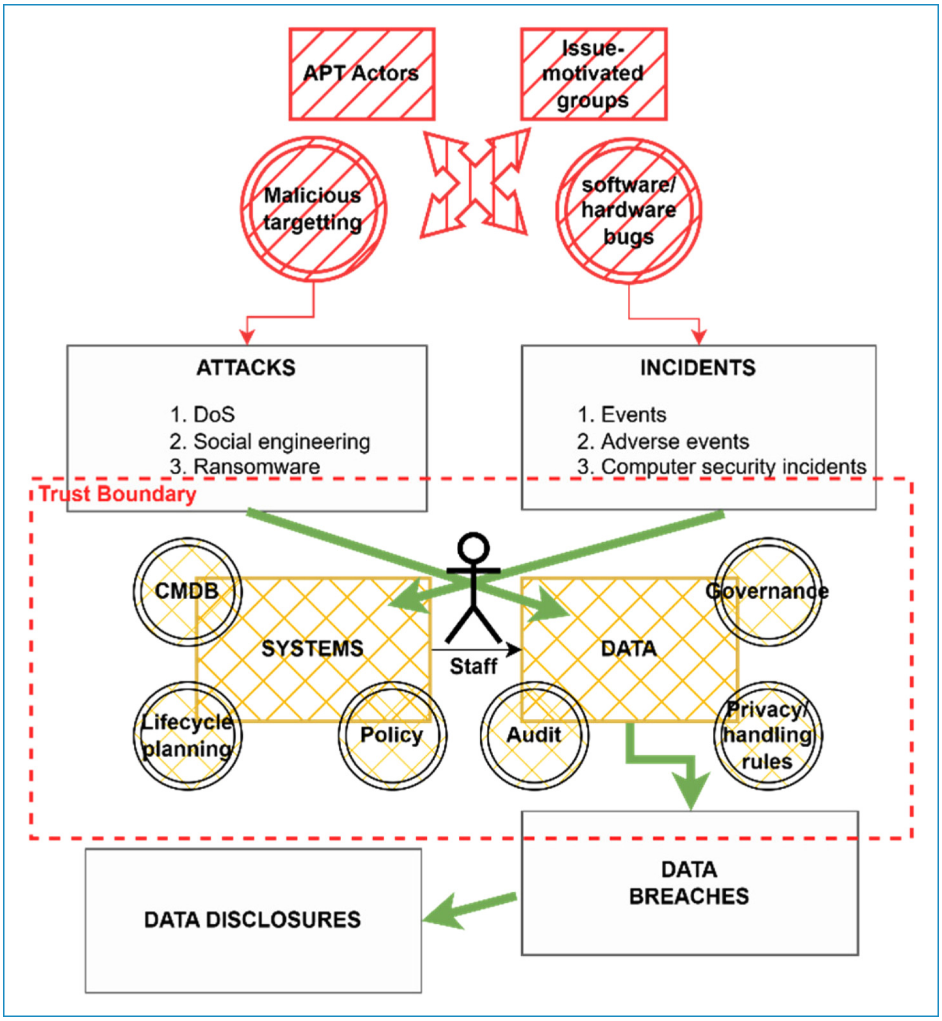

**Figure 2.** CYBER-AIDD risks and their logical infringement across LAHP trust boundaries.

Advanced Persistent Threat (APT) groups and their motivations can range from political pressure, all-domain warfare, or financially-motivated outcomes, and they can deploy coercive military-grade cyber weapons and techniques with a very high likelihood of success.[32–34] These attacks can range from ransomware, systems performance degradation (denial of service (DoS) attacks), website defacement, or destructive malware. Such attacks can be executed via human-based vectors ('social engineering'), exploitation of known and unpatched software vulnerabilities, the manipulation of badly configured systems, or the discovery and deployment of previously unknown vulnerabilities ('Zero-Day' exploits).

The consequences of such attacks can be any combination and severity of security incidents, data breaches, or data disclosures. In an attack on the Singapore Health system in 2018, the attacker spent 10 months inside the network discovering the most valuable data and exploiting multiple avenues of back-door access, before eventually exfiltrating 1.5 million patient records.[35]

LAHPs are attractive targets for these attacks as healthcare systems tend to be very complex and therefore very likely to host known vulnerabilities that can be exploited. While this may seem obvious when considering legacy systems with expired vendor support, it can also be the case for cutting-edge solutions being used in new configurations. Researchers have, for example, undertaken penetration tests demonstrating successful compromises of Bluetooth-enabled insulin pumps,[36] pacemakers,[37] medical alert pager networks,[38] deep brain implants[39] and even AI-supported cancer diagnostic software.[40]

The implication for LAHPs is that sophisticated attacks against them may be underway at any time, via many novel vectors, and the absence of obvious symptoms may not represent the absence of a determined or possibly already successful attack.

## Incidents

Several well-developed international standards are available that identify what any organisation *should* do to manage security incidents, including ISO/IEC 27035 'Information Security Incident Management';[41] the National Institute of Standards and Technology (NIST) 'Special Publication 800-61 - Computer Security Incident Handling Guide';[42] The European Union Agency for Cyber Security (ENISA) 'Good practice guide for incident management');[43] and the SysAdmin, Audit, Network and Security (SANS) 'Incident Handlers Handbook'.[44] Despite these mature standards being available, adoption resistance can be high for a LAHP, who may try to embrace too many aspects of that ideal standard and may become mired in 'paralysis by analysis'[45] as they seek to assess too many systems, and implement too many risk mitigations. This can ultimately lead to ineffective outcomes when decisions in an emergency situation are made in haste, and with incomplete awareness or knowledge of the true nature of the incident taking place.[46,47]

To seek a simplified approach, there are two high-level definitions that should first be recognised – that of 'events' versus 'incidents':[48]

- Security events – an occurrence in a system, service, or network state indicating a possible breach of safeguards.
- Security incidents – an unwanted, unexpected security event, or series of events that have a significant probability of compromising business operations.

The NIST Special Publication (SP) 800-61 introduces one further aspect to these definitions, sub-dividing 'events' in a way that is useful for recognising that many events are in fact 'noise' that need to be filtered out during incident response. This results in an optimum definition comprised of: (1) *events*, (2) *adverse events* and (3) *computer security incidents*.[42]

For a LAHP, being able to adopt and implement at least some rudimentary incident controls based off these three definitions is a core requirement that can deliver a powerful prevention and remediation capability, and a foundation for effective cyber resilience.

## Breaches

Much has been written in academia and the media on the subject of data breaches, fuelled by the drivers of: (1) the rapid expansion of digital systems into increasingly sensitive areas of public services and citizens' private lives, (2) the seeming ease and regularity of those digital systems being compromised, (3) the rising business cost of recovering from data breaches and (4) government privacy legislation establishing mandatory reporting frameworks, which has led to greater exposure of such incidents.[49] Throughout the literature, definitions for the term can vary depending on the specific data of concern, the professional or governance body writing policies, or the social expectations of the government creating new laws.[50]

It should also be noted, when seeking to clearly identify and resolve the problem of data breaches, that the word 'breach' lends itself differently to specific aspects of the cyber security resilience problem, given the main definitions of the word from the Cambridge Dictionary:[51]

1. *Noun*: Broken promise/rule – an act of breaking a law, promise, agreement, or relationship.
2. *Noun*: Opening – a hole that is made in a wall or in another structure being used for protection during an attack.

The first definition applies to the failure of explicit or implied legal contracts or protections that apply when patients or third-party stakeholders provide sensitive personal, business, or research data to LAHPs for processing or storage. When attacks on systems or incidents result in data being disclosed, the LAHP can be said to be *in breach* of their agreement with the provider or subject of that data. The second definition applies to the practicalities of how attacks or incidents are actually successful. In this context, a malicious or incidental action reveals a gap (*breach*) in one or more of the protections in place to maintain the confidentiality, integrity, or availability of sensitive data.

Taking elements of these definitions into consideration when examining data breaches, Khan et al.[52] define a data breach as, '*a security incident in which sensitive, protected, or confidential data are copied, transmitted, viewed, stolen, or used by an unauthorised individual*'. A similar definition is arrived at by Hendee,[53] '*a confirmed incident in which sensitive, confidential or otherwise protected data has been accessed and/or disclosed in an unauthorised fashion*'.

While these definitions focus on the ultimate threshold of a data breach being linked the *authorised* status of the user, they do not adequately cover the subtleties that may be present in the early stages of a LAHP breach where user access is fully 'authorised'. In these cases, the user managing data or systems may only subtly or inadvertently be at odds with policy or best practice, but the foundations for a future significant data breach are sown when minor breaches of contracts, policy, or security controls go unnoticed or unactioned. This is why the previous sections defining *attacks* and *incidents* as precursors for this separate process of a data breach are important – they show that data breaches do not occur in isolation but are in fact the product of other security failures.[54] It is also why the prevention of attacks and the early identification and strategic learnings from security incidents are essential, as these are

Table 2. Select Australian healthcare cyber security incidents 2018–2022.

| Provider | Incident | Cause | Year |
|---|---|---|---|
| **HealthEngine** | 59,600 items of 'patient feedback' accessed[57] | Website misconfiguration | 2018 |
| **Cabrini Hospital Melbourne Heart Group** | 15,000 patient records encrypted by malware. Attempts to pay the ransom failed to recover the data[58] | Unpatched systems and malware | 2019 |
| **Victoria Health** | Multiple sites attacked, and numerous systems impacted over several weeks. Multiple surgeries cancelled[59] | Emotet malware | 2019 |
| **Ambulance Tasmania** | Unencrypted radio transmissions intercepted and posted online[60] | Legacy communications | 2021 |
| **Eastern Health** | Elective surgeries cancelled across four Melbourne hospitals[61] | Ransomware | 2021 |
| **Medibank** | A 200 GB database containing approximately 9.7 million customer records stolen[62] | Phishing attack (stolen privileged credentials) | 2022 |

opportunities to avoid the subsequent realisation of a data breach from ever occurring.

In reviewing the Australian legislative response to data breaches, Daly[50] defines a data breach as, '*security breaches, which lead to the disclosure, access or acquisition of information*'. This definition is more helpful in removing the 'authorised user' threshold, but still falls short of identifying the important variation between 'access or acquisition of information' (which may in fact be inconsequential), versus confirmation of that information actually being disclosed in a manner that is harmful to individuals or stakeholders. This is a key point as in many cases stolen or exfiltrated ('breached') data is not immediately disclosed, as doing so would undermine its value to the attacker. In a ransomware attack, stolen data is usually kept private by the attacker for long periods, and it is the *threat* of disclosure that is exploited in order to extract payment from the victim. This is why the subsequent inclusion of the *disclosure* threat to cyber security resilience, detailed in the next section, is needed.

Further to this same point is the fact that if controls are effectively planned, data breaches do not have to result in disclosure at all. If a data resource is strongly encrypted when it is stolen, it may still be publicly released during a breach event yet remains unreadable to any third party, and its integrity and confidentiality remain assured.

## The data breach problem

The regularity and severity of data breaches impacting both commercial and government data networks worldwide have been extensively covered in the literature.[55] Collins et al.[56] detailed 6 years of breaches impacting the healthcare and education sectors in the US and identified 2219 events in total, while Hendee,[53] having identified 9600 worldwide breaches over 14 years, came to define the data breach as a modern 'epidemic'. As well as the volume of data breaches, the speed at which a data breach can impact users and systems can be very rapid. Hendee[53] outlines two examples of data breach evaluations undertaken by the US Federal Trade Commission's Office of Technology Research Investigation, who observed attempts to exploit breached data commencing after 90 and 90 min, respectively.

This trend of data breaches and data disclosures has impacted healthcare globally and in Australia significantly, with a selection of examples shown in Table 2.

## Disclosures

Unauthorised data disclosure is the ultimate adverse consequence in the cyber security risk and resilience journey – the end state that every LAHP is seeking to avoid. The previous stages of: (1) attacks, (2) incidents and (3) breaches may all be realised, yet even then disclosure of data does not always result from those events. The threat of disclosure is so pervasive and effective that it has been used in attacks and scams for several years. Keshavarzi and Ghaffary[63] undertook a taxonomy review of extortion/disclosure-themed attacks, and detailed contemporary mutations including fake software installers, 'leakware' and six sub-variants of ransomware.

For LAHP patients, given the wide-ranging sensitivity their health data holds, the potential for serious consequences from this targeting and disclosure is ever-present, and has been a disturbing feature of many previous healthcare disclosure incidents. One of the more serious examples of this was the breach of data from a mental health counselling clinic in Scandinavia, and subsequent attempts to bribe individual patients with the threat of their clinical records being disclosed to friends or family unless a ransom was paid.[64]

While the word 'disclosure' has several similar meanings, within the domain of cyber resilience, the definition that is most relevant is, '*something that was not previously known, or the act of giving such information to the public*'.[50] This provides an explanation that resonates at this final stage of the AIDD focus. The eventual revelation of sensitive information resulting from a data breach is damaging to a LAHP (and the patient), both for the specific nature of that data (as the 'thing that was not previously known' could be very personal medical data), and the fact that the system which should have protected it failed (this 'act of giving' the data to the public – albeit via a data breach – is one that can cause the public to lose trust in the LAHP).

McLeod and Dolezel[65] highlight this same concern in their paper modelling healthcare data breaches, with the inclusion of the 'disclosure' definition from the US Health Insurance Portability and Accountability Act (HIPAA), which states, '*a breach is, generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information*'.

## Recognising healthcare cyber security concerns

As the situation above outlines, healthcare has increasingly been identified as an industry of concern regarding its cyber risk management and cyber resilience capabilities. Williams[66] identified the lack of a coordinated national approach to the protection of Australian healthcare as a growing risk, along with the poor understanding of risk by clinical end-users. Langer[67] captured the scope of threat actors interested in healthcare through his classification of 'thieves, vandals and assassins' all seeking to exploit healthcare, and reiterated Williams' finding that naive users opening emails or visiting malicious websites makes success likely for potential attackers, without them even having to compromise user credentials.

Jalili and Kaiser[68] further detail the unique problems healthcare experiences from endpoint complexity, multiple stakeholder alignment, and the financial value attackers can reap from exploiting medical records. Those authors also identified the attractiveness of healthcare attacks to politically or terrorist motivated cyber attackers, with one of their interview subjects identifying that such actors would target healthcare because, '*…it makes the news faster. If you have to turn patients away from your emergency room because you can't get your IT up, that's scary*'.

Wherever protective approaches have been applied historically, they have been focussed on better managing the critical elements of the 'CIA triad' – the *confidentiality*, *integrity* and *availability* elements that form the core of cyber security for any digital system.[18,69–71] While these are important attributes to protect for a range of systems, they take on especial importance when dealing with the life-and-death diagnostics, vulnerable citizen records and pandemic-scale containment processes provided by LAHPs. For such systems there is a virtual inevitability of some form of attack, incident, or breach occurring due to system complexity. This view is supported by Goel et al.[72] who also surmise that given the resource constraints most organisation face and the continual risk trade-offs needed, there needs to be a re-think of purely compliance-based strategies based on rigidly following monolithic security frameworks.

## Statistical analysis

The main relevant statistics for this paper are those describing the frequency and cause of data breaches impacting LAHPs – the risk that the CYBER-AIDD model is seeking to reduce. The examples shown in Table 2 (primarily sourced from media or industry reports) tend towards reporting on volumetric measures such as the number of records lost in each breach, the cost to organisations of recovery, or the volume of data transferred to the attackers. This selective focus on data breach consequences also applies via other Australian data, with the most recent (October 2022) Australian National University *Public Exposure and Responses to Data Breaches*[73] poll reporting that '32.1% of the Australian population has been the victim of a data breach in the previous 12 months'.

As the ANU data does not deal specifically with healthcare, when seeking to focus on LAHP figures the peak Australian data comes via the Commonwealth Privacy Act's Notifiable Data Breach (NDB) scheme, which is overseen by the Office of the Australian Information Commissioner (OAIC). This has been in place since 2018 and a summary of the first five years of eligible data breaches (which total $N = 929$) are illustrated in Figure 3. This also shows the vectors by which those breaches were realised, including an annualised population mean ($\mu$) for each cause. While this shows for each year that healthcare has reported significant breach volumes (and that human error is consistently the main cause at 462/929 (49.9%) of all breaches), it should also be noted these figures are likely to be significantly under-reported for the following reasons:

1. Not all LAHPs have a mandatory reporting requirement under this Commonwealth legislation (such as state-run public health services), and so several very large LAHPs are excluded from these figures.
2. The Commonwealth Government's Australian Digital Health Agency (ADHA) reports separately on data breaches or incidents impacting the national My Health Record system, and those figures are also excluded here.

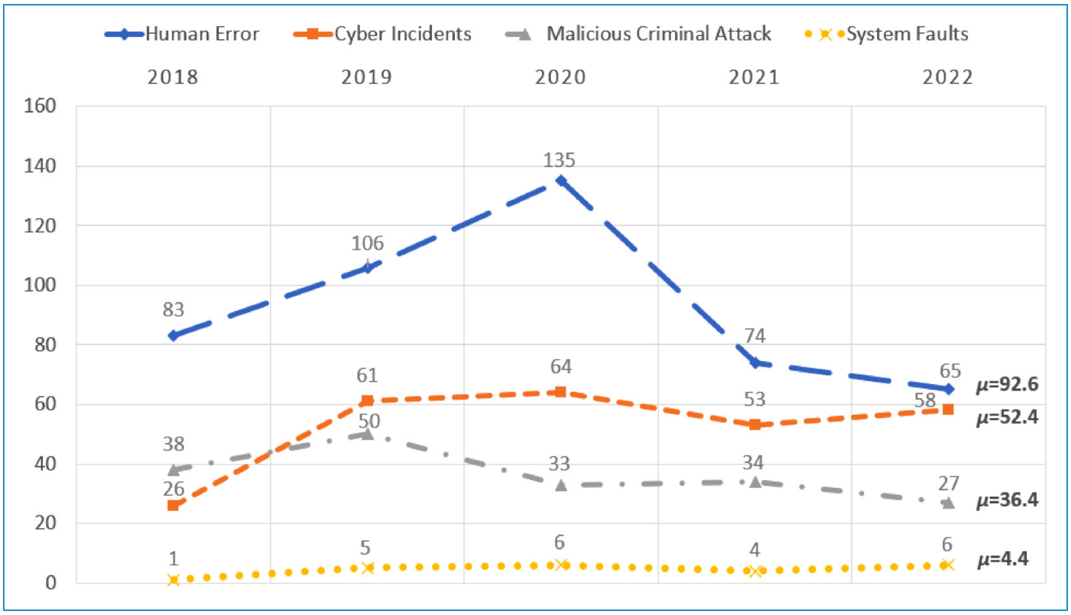

**Figure 3.** Australian healthcare data breaches 2018–2022 ($N = 929$).[74]

3. For LAHPs that are covered under these Privacy Act reporting requirements, not all data breaches are considered 'eligible' for inclusion into these periodic reports, and are also excluded here.

## Results

This paper has shown that achieving cyber resilience begins with clearly defining the scope and goals of cyber risk concerns for LAHPs. The figures presented show that of the 929 total healthcare data breaches reported in Australia over a five-year period, human error ($\mu = 92.6$) is the most prevalent. Supplementing this trend with analysis from the ACSC and AHDA, a prioritised four-stage risk model is defined, recommending that LAHPs focus on: (1) attacks, (2) incidents, (3) data breaches and (4) data disclosures (the 'AIDD' approach).

In order to present these results in an easily consumable form, the final definitions, relationships and implementation order of these findings are incorporated into the ontological diagram shown in Figure 4, using the Unified Modelling Language (UML) to present a 'specified conceptualisation'.[75]

### *Model construction*

In this model, the 'classes' referred to are the four prioritised aspects within the expanded definition for 'cyber security', and reproduced here with the classes bolded for clarity, each of which is shown via the UML model as a 'set of objects with common features':[76]

> (Cyber security is…) the approach and actions associated with security **risk management processes** [**1**] followed by organisations…**to protect the confidentiality, integrity and availability** [**3**] of **data and assets used in cyber space** [**2**] from **attacks, incidents, data breaches, and data disclosures** [**4**].

For each of the classes, three stacked boxes are presented which respectively describe the *name* of the class, its *attributes*, and any logical or practical *operations* that apply to it. The model commences with class #1, 'risk management'; shown as the initiating action of cyber security resilience (of which there must be at least one, but possibly many versions) with a protected (#) attribute of 'controls' and a public operating attribute (+) of 'governance'. Protected attributes of the risk management class include operations '()' for maintaining a risk register, a recognised risk appetite, a formal risk committee, and an incident management process, along with publicly available (+) policies. This class of attributes are then applied to class #2 'cyber space', and the process continues in sequence with the ultimate goal, at class #4, of minimising cyber risks through reduced attacks, incidents, data breaches and data disclosures.

This paper has adopted the use of UML class diagrams for the illustration of this ontology in recognition of their following attributes:

1. UML class diagrams are consistent with the object-centred outcomes traditional ontologies seek to represent, across various domains of interest.[77]

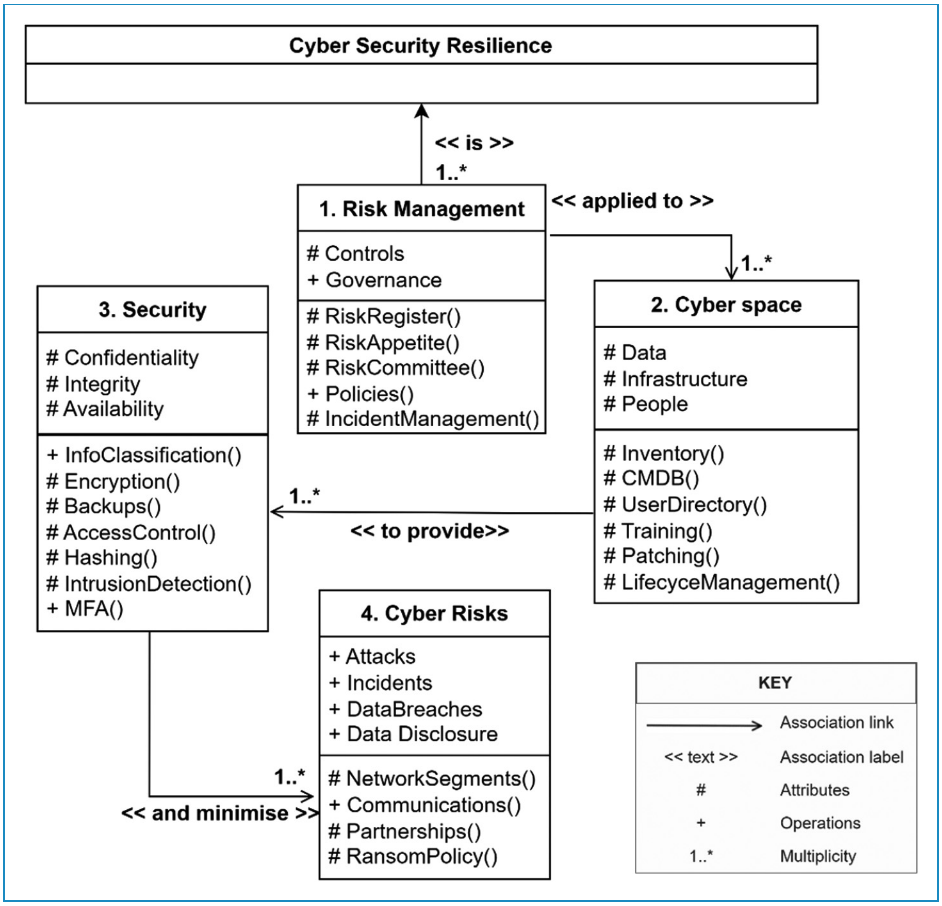

**Figure 4.** UML depiction of the cyber security ontology.

2. In this use-case, UML is effective in achieving the ontological outcome of ‘explicit specification of a conceptualisation’ or *declarative formalism*.[78]
3. Through the use of class diagrams, UML can be used to describe both the arrangement and semantics required to understand relationships, via the use of labels.[79]

## Discussion

This paper has provided a simplified model which can be used by LAHP organisations to commence a transformation towards better cyber resilience. LAHPs who are struggling to understand or begin such a journey – to find a ‘way in’ to this complex cyber space – will find these definitions and the final model useful in establishing the necessary risk and governance frameworks and supporting processes. What the literature review has shown is that there are currently many widely disparate definitions for cyber risk terms, but with a more precise application, ‘cyber security’ can be defined to focus on the risks most relevant to LAHPs, being attacks, incidents, data breaches and data disclosures (the CYBER-AIDD model).

Of central relevance to this investigation has been the difficulty that LAHPs experience implementing exhaustive cyber risk frameworks such as NIST, ISO/IEC 27001 or the ACSC’s Information Security Manual – evidenced by the ongoing trend of data breaches which those standards are intended to reduce. These do remain vital resources for any LAHP to ultimately adopt, and the attributes and operations identified in this paper’s CYBER-AIDD approach are consistent with the controls those standards support and should be seen as a bridge between the two methodologies.

The presentation of the single-page CYBER-AIDD model is useful for a variety of practical uses, such as scoping new projects, procurement shortlisting, or populating an initial risk register. This brevity is intended to be the models’ primary attribute, much like the ACSC publishes an *Essential Eight Maturity Model*[80] version of its larger 37 *Strategies to Mitigate Cyber Security Incidents*,[81] which is itself condensed from the 850 controls of the full Australian *Information Security Manual*.[23]

While Australian legislation that applies to LAHPs in the management of cyber resilience and the reporting of data breaches is still evolving, it is apparent there is an increasing intent from the government to develop this area further, and at some pace, after the large data breaches in Australia of Optus and Medibank in 2022.[82] Further major developments in this area also emerge for LAHPs from the 2021 and 2022 amendments to the Commonwealth's Security of Critical Infrastructure Act, 2018 (Cth), which for the first time creates a nationwide set of risk management and incident response criteria that includes all LAHPs across Australia (including all states, territories and private sectors).[83] This should be considered a further driver for LAHPs to enhance their understanding of the basic cyber security concepts which underpin these and future legislative changes.

A foundational aspect of this model is also that there is more to the LAHP cyber risk problem that just the 'data breach' headlines. This concept that data breaches are in reality a symptom of a wider security deficiency that is rooted in other precursory areas (namely the prevalence of attacks and incidents) does not emerge readily from the formality of contemporary industry standards. Neither does the possibility readily emerge from those standards that, even in an ideal environment, full implementation of the standards may still not guarantee cyber security or resilience for very long, and a more agile model is needed to deliver practical outcomes.

As a practical example of using the CYBER-AIDD model, consider the challenge faced by a LAHP wanting to produce a new cyber risk management plan (RMP), as required under the newly amended Security of Critical Infrastructure Act 2018 (Cth). This act requires that LAHPs report a plan via their local board to the Commonwealth Government annually, and review and update that plan on a regular basis. Using a large (ISO or NIST CSF) standards-based approach, this would be an extensive (and expensive) undertaking. By undertaking iterations of the four-stage CYBER-AIDD process, a LAHP would be able to produce the following basic, but robust cyber resilience approach with minimal staff, time and financial commitments:

1. A corporate cyber risk appetite statement, a basic risk register, and terms of reference (ToR) plus minutes from a formally established cyber risk committee (CRC). A draft policy for cyber incident management should also be tabled and approved via this CRC.
2. The CRC should task the ICT (or a dedicated cyber) manager to establish a basic cyber awareness training programme for all users, and an inventory of key data holdings and the infrastructure used to process and store them (i.e. servers, disk arrays, or data centres – including those provided by vendors). The setup of these can be captured in a basic configuration management database (CMDB), and proposed changes to this baseline tracked via a minuted approvals process. Work instructions for managing critical patching and lifecycle management (how to dispose of old equipment, and procure effective replacements) should also be established, and reported via the CRC.
3. Definitions surrounding corporate information classifications can also be issued by the cyber manager, with confirmation of data encryption, backup and recovery requirements. These will support further assurance surrounding the confidentiality, integrity and availability of data and systems which can be reported to the CRC.
4. Finally, by establishing a ransomware policy, network segmentation approach, and partnerships with commercial cyber recovery, threat intelligence, or product partners (to seek solutions such as end point protection), the frequency and impact of attacks, incidents, data breaches and data disclosures can be monitored, managed and reduced over time.

The resulting documents and governance process would meet the needs of the Commonwealth Act, avoiding the potential imposition of legislative fines against the LAHP.

## Conclusion

In considering the long-standing semantic difficulties and trends in data breaches identified in this paper, alongside Australian Commonwealth healthcare strategies and threat intelligence data, it has been shown that a simpler ontological approach can be achieved. An important aspect of presenting this model has been the successful use of a UML class diagram to align elements of semantic meaning with a flow of interrelationships, a list of key attributes, and examples of high-level operations that would be needed to implement the model and reduce risk. Merging these techniques is aimed at supporting increased understanding by any specialist from any area within a LAHP, so that they can appreciate the basic establishment and relationships between these key concepts.

The continuing transformation of healthcare via digital and highly internetworked systems represents a major opportunity for LAHPs to significantly improve health outcomes for the Australian population. Yet those same technologies also represent an ever-present risk vector, it is essential that cyber resilience controls are in place and maintained.

In this context, effective cyber resilience for LAHPs does not result from the 'big bang' implementation of a single all-conquering product, the deployment of generic project managers, or simply commissioning a standards-based audit. LAHPs, and those who work within and supply them, need to understand the fundamentals of how and why cyber risks are being exploited by malicious actors. From such a position of knowledge, they can then rationally commit to the operational changes needed to ensure improved cyber resilience and the protection of patient data and services.

## Limitations and future research

This study has been limited due to its goal of seeking only a high-level definition of cyber risk, and a basic ontological model for any LAHP to consider using as a first step towards improved cyber governance maturity. This has necessitated a very precise and sparse use of language, to try and avoid the problem of creating yet another large and unwieldy security standard.

Further work would therefore be beneficial (expanding the UML model presented by this paper) to provide deeper detail on the four CYBER-AIDD components, and mapping those explicitly to one or more of the established cyber security risk management models (such as the NIST framework). Also an improved understanding of the range of workers in a LAHP environment, and what their current knowledge and expectations of cyber risk management are, would help contribute towards more practical training and remediation success.

**Contributorship:** MD researched the literature and created the first draft. All authors reviewed and edited the manuscript and approved the final version.

**Declaration of conflicting interests:** The author(s) declared no potential conflicts of interest with respect to the research, authorship and/or publication of this article.

**Ethical approval:** This PhD paper has received ethics approval from Edith Cowan University, Australia ref: 2020–01418 – DART.

**Funding:** The author(s) received no financial support for the research, authorship and/or publication of this article.

**Guarantor:** None declared.

**ORCID iD:** Martin Dart https://orcid.org/0000-0002-2035-8232

## References

1. Security of Critical Infrastructure Act 2018. 2022.
2. Jalali MS, Razak S, Gordon W, et al. Health care and cybersecurity: bibliometric analysis of the literature. *J Med Internet Res* 2019; 21: e12644.
3. Williams PA. Making Research Real: Is Action Research a Suitable Methodology for Medical Information Security Investigations? In: *4th Australian Information Security Management Conference* School of Computer and Information Science, Edith Cowan University, 5th December 2006.
4. Warren M and Leitch S. A participational security method for healthcare organisations. In: *e-Society 2006: Proceedings of the IADIS International Conference e-Society* 2006 2006, IADIS Press.
5. Schatz D, Bashroush R and Wall J. Towards a more representative definition of cyber security. *J Digital Forensics, Secur Law* 2017; 12: 66.
6. Checkland P. Achieving 'desirable and feasible' change: an application of soft systems methodology. *J Oper Res Soc* 1985; 36: 821–831.
7. Avorn JMD. The psychology of clinical decision making – implications for medication use. *N Engl J Med* 2018; 378: 689–691.
8. Denney AS and Tewksbury R. How to write a literature review. *J Criminal Justice Educ* 2013; 24: 218–234.
9. Webb T and Dayal S. Building the wall: addressing cybersecurity risks in medical devices in the USA and Australia. *Comput Law Secur Rev* 2017; 33: 559–563.
10. Schwartz S, Ross A, Carmody S, et al. The evolving state of medical device cybersecurity. *Biomed Instrum Technol* 2018; 52: 103–111.
11. Thomasian NM and Adashi EY. Cybersecurity in the internet of medical things. *Health Policy Technol* 2021; 10: 100549.
12. Falco G, Cornish P, Creese S, et al. Cyber Crossroads: A Global Research Collaborative on Cyber Risk Governance. *arXiv preprint arXiv:210714065* 2021.
13. Baylon C. Challenges at the intersection of cyber security and space security: country and international institution perspectives. 2014.
14. Azmi R, Kautsarina, th European Conference on Cyber W, et al. Revisiting cyber definition. *European Conference on Information Warfare and Security, ECCWS* 2019; 2019-July: 22-30.
15. Moustafa AA, Bello A and Maurushat A. The role of user behaviour in improving cyber security management. *Frontiers in Psychology* 2021; 12.
16. Box D and Pottas D. Improving information security behaviour in the healthcare context. *Proc Technol* 2013; 9: 1093–1103.
17. Leach J. Improving user security behaviour. *Comput Secur* 2003; 22: 685–692.
18. von Solms R and van Niekerk J. From information security to cyber security. *Comput Secur* 2013; 38: 97–102.
19. von Solms B and von Solms R. Cybersecurity and information security what goes where? *Inf Comput Secur* 2017; 26. doi:10.1108/ICS-09-2015-0037
20. Pipkin DL. *Information security: protecting the global enterprise*. Prentice-Hall, Inc., 2000, p.13.
21. Saydjari OS. *Engineering trustworthy systems: get cybersecurity design right the first time*. McGraw Hill Professional, 2018.
22. Linkov I, Kott A and Lonkov I (eds) *Cyber resilience of systems and networks*. Springer, 2019.
23. Australian Cyber Security Centre (ACSC). Information Security Manual (December 2022). 2022.
24. Mulligan DK and Schneider FB. Doctrine for cybersecurity. *Daedalus* 2011; 140: 70–92.
25. Australian Digital Health Agency (ADHA). Cyber Security Strategy 2022-2025. 2022.
26. Australian Cyber Security Centre (ACSC). ACSC Annual Cyber Threat Report, July 2021 to June 2022. 2022.
27. National Institute for Standards and Technology (NIST). Special Publication 800-37 Rev. 2: Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. 2018.

28. Australian Broadcasting Corporation (ABC). Healthcare industry continues to be main target of data breaches, with 79 reported in six months, https://www.abc.net.au/news/science/2022-11-10/data-breach-medibank-healthcare-system/101612056 (2022).
29. Australian Cyber Security Magazine. Cyberattacks on Australian Healthcare Doubles. *Australian Cyber Security Magazine*, 2022.
30. Landi H. Relentless cyberattacks are putting financial pressure on hospitals: Fitch Ratings, https://www.fiercehealthcare.com/tech/relentless-cyber-attacks-are-putting-pressure-hospital-finances-fitch-ratings (2021, accessed 10/12/2022).
31. Porcedda MG. Patching the patchwork: appraising the EU regulatory framework on cyber security breaches. *Comput Law Secur Rev* 2018; 34: 1077–1098.
32. Chen J, Su C, Yeh K-H, et al. Special issue on advanced persistent threat. *Future Gener Comput Syst* 2018; 79: 243–246.
33. Chen P, Desmet L and Huygens C. A study on advanced persistent threats. In: *IFIP international conference on communications and multimedia security*. Springer, 2014, pp.63–72.
34. Tankard C. Advanced persistent threats and how to monitor and deter them. *Netw Secur* 2011; 2011: 16–19.
35. Singapore Ministry of Communications and Information. Public Report of The Committee of Inquiry Into The Cyber Attack on Singapore Health Services Private Limited's Patient Database on or Around 27 June 2018. 2019.
36. Bu L and Karpovsky MG. A design of secure and reliable wireless transmission channel for implantable medical devices, in Proceedings of the 3rd International Conference on Information Systems Security and Privacy (ICISSP). SCITEPRESS, 2017, pp.233–242.
37. Khera M. Think like a hacker: insights on the latest attack vectors (and security controls) for medical device applications. *J Diabetes Sci Technol* 2017; 11: 207–212.
38. Freundlich RE, Freundlich KL and Drolet BC. Pagers, smartphones, and HIPAA: finding the best solution for electronic communication of protected health information. *J Med Syst* 2018; 42: –3.
39. Pycroft L, Boccard SG, Owen SL, et al. Brainjacking: implant security issues in invasive neuromodulation. *World Neurosurg* 2016; 92: 454–462.
40. Mirsky Y, Mahler T, Shelef I, et al. *CT-GAN: Malicious Tampering of 3D Medical Imagery using Deep Learning*. 2019.
41. ISO/IEC 27035-2:2016. Information technology — Security techniques — Information security incident management — Part 2: Guidelines to plan and prepare for incident response.
42. Cichonski P, Millar T, Grance T, et al. Computer security incident handling guide. *NIST Spec Publ* 2012; 800: 1–147.
43. Miroslav R and Stikvoort D. *Good practice guide for incident management*. European Network and Information Security Agency (ENISA), 2010.
44. Kral P. *The incident handlers handbook*. SANS Institute, 2011.
45. Sharif AM. Paralysis by analysis? The dilemma of choice and the risks of technology evaluation. *J Enterp Inf Manag* 2008; 21: 11.
46. Tøndel IA, Line MB and Jaatun MG. Information security incident management: current practice as reported in the literature. *Comput Secur* 2014; 45: 42–57.
47. Kossakowski K-P, Allen J, Alberts C, et al. *Responding to Intrusions*. 1999. CARNEGIE-MELLON UNIV PITTSBURGH PA SOFTWARE ENGINEERING INST.
48. ISO/IEC. 27000 Information technology – Security techniques – Information security management systems.
49. Alazab M, Hong S-H and Ng J. Louder bark with no bite: privacy protection through the regulation of mandatory data breach notification in Australia. *Future Gener Comput Syst* 2021; 116: 22–29.
50. Daly A. The introduction of data breach notification legislation in Australia: a comparative view. *Comput Law Secur Rev* 2018; 34: 477–495.
51. Cambridge Dictionary. Cambridge University Press, 2022.
52. Khan F, Kim JH, Mathiassen L, et al. Data breach management: an integrated risk model. *Inf Manage* 2021; 58: 103392.
53. Hendee LA. The data breach epidemic: a modern legal analysis. *J Technol Law Policy* 2021; 24: 3.
54. Saleem H and Naveed M. Sok: anatomy of data breaches. *Proc Priv Enhancing Technol* 2020; 4: 153–174. doi:10.2478/popets-2020-0067
55. Fleury-Charles A, Chowdhury MM and Rifat N. Data breaches: vulnerable privacy. In: *2022 IEEE international conference on electro information technology (eIT)*. United States: IEEE, 2022, pp.538–543.
56. Collins JD, Sainato VA and Khey DN. Organizational data breaches 2005–2010: applying SCP to the healthcare and education sectors. *Int J Cyber Criminol* 2011; 5: 794–810.
57. IT News. HealthEngine reveals data breach, https://www.itnews.com.au/news/healthengine-reveals-data-breach-496175 (2018, accessed 14/05/2019 2019).
58. Healthcare IT News. Medical records at Victorian hospital get hacked, https://www.healthcareit.com.au/article/medical-records-victorian-hospital-get-hacked (2019).
59. The West Australian. Limited delays after Vic hospital hacks. 2019.
60. Clarke P. Significant data breach from Ambulance Tasmania through interception of its paging service with data of patients who contact ambulances published on line, http://www.peteraclarke.com.au/2021/01/08/significant-data-breach-from-ambulance-tasmania-through-interception-of-its-paging-service-with-data-of-patients-who-contact-ambulances-published-on-line/ (2021).
61. Cunningham M. Staff unable to access patient files after Eastern Health cyber attack. 2021.
62. Kost E. What Caused the Medibank Data Breach?, https://www.upguard.com/blog/what-caused-the-medibank-data-breach (2022).
63. Keshavarzi M and Ghaffary HR. I2CE3: a dedicated and separated attack chain for ransomware offenses as the most infamous cyber extortion. *Comput Sci Rev* 2020; 36: 100233.
64. Ralston W. They told their therapists everything. *Hackers leaked it all WIRED com* 2021.
65. McLeod A and Dolezel D. Cyber-analytics: modeling factors associated with healthcare data breaches. *Decis Support Syst* 2018; 108: 57–68.
66. Williams PAH. IT and security considerations for online clinical records. *Ann R Australas Coll Dent Surg* 2010; 20: 66–70.
67. Langer SG. Cyber-security issues in healthcare information technology. *J Digit Imaging* 2017; 30: 117–125.

68. Jalali MS and Kaiser JP. Cybersecurity in hospitals: a systematic, organizational perspective. *J Med Internet Res* 2018; 20: e10059.
69. Fenrich K. Securing your control system. *Power Eng* 2008; 112: 44–51.
70. Fruhlinger J. *The CIA triad: definition, components and examples*. CSO Online, 2020.
71. Sherman AT, DeLatte D, Neary M, et al. Cybersecurity: exploring core concepts through six scenarios. *Cryptologia* 2018; 42: 337–377.
72. Goel R, Kumar A and Haddow J. PRISM: a strategic decision framework for cybersecurity risk assessment. *Inf Comput Secur* 2020; 28: 591–625.
73. Biddle N, Gray M and McEachern S. Public exposure and responses to data breaches in Australia: October 2022. 2022.
74. Office of the Australian Information Commissioner (OAIC). Privacy, https://www.oaic.gov.au/privacy (2022).
75. Meersman RA. Semantic ontology tools in IS design. In: Raś ZW and Skowron A (eds) *Foundations of intelligent systems*. Berlin, Heidelberg: Springer Berlin Heidelberg, 1999// 1999, pp.30–45.
76. Berardi D, Calvanese D and De Giacomo G. Reasoning on UML class diagrams. *Artif Intell* 2005; 168: 70–118.
77. Mejhed Mkhinini M, Labbani-Narsis O and Nicolle C. Combining UML and ontology: an exploratory survey. *Comput Sci Rev* 2020; 35: 100223.
78. Gruber TR. A translation approach to portable ontology specifications. *Knowl Acquis* 1993; 5: 199–220.
79. Pătraşcu A. Comparative analysis between OWL modelling and UML modelling. *Petroleum-Gas University of Ploiesti Bulletin, Technical Series* 2015; 67.
80. Australian Cyber Security Centre (ACSC). Essential Eight Maturity Model. 2022.
81. Australian Cyber Security Centre (ACSC). Strategies to Mitigate Cyber Security Incidents. 2017.
82. Martin S and Karp P. *Government flags new cybersecurity laws and increase in fines after Optus breach*. The Guardian, 2022.
83. Sutton L,, Fanning K and Huang E. Draft risk management program rules under the SOCI Act now open for consultation, https://www.gtlaw.com.au/knowledge/draft-risk-management-program-rules-under-soci-act-now-open-consultation (2022).