Cybersecurity Indexes for eHealth

Conference Paper · January 2019

DOI: 10.1145/3290688.3290721

4 authors, including:

Alireza Jolfaei
Federation University Australia
31 PUBLICATIONS **332** CITATIONS

SEE PROFILE

Cybersecurity Indexes for eHealth

Wendy Burke
School of Science, Engineering and Information Technology
Federation University Australia
Mt Helen, Victoria, Australia
w.burke@federation.edu.au

Taiwo Oseni
School of Science, Engineering and Information Technology
Federation University Australia
Mt Helen, Victoria, Australia
t.oseni@federation.edu.au

Alireza Jolfaei
School of Science, Engineering and Information Technology
Federation University Australia
Mt Helen, Victoria, Australia
a.jolfaei@federation.edu.au

Iqbal Gondal
School of Science, Engineering and Information Technology
Federation University Australia
Mt Helen, Victoria, Australia
iqbal.gondal@federation.edu.au

ABSTRACT

This study aimed to explore the cybersecurity landscape to identify cybersecurity indexes that may be relevant to the health industry. While the healthcare sector poses security concerns regarding patients' records, cybersecurity in the healthcare sector has not been given much consideration. Cybersecurity indexes are a survey that measures security preparedness and capabilities of a country or organisation. 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. In this paper, cybersecurity indexes were reviewed regarding the level of assessment (country level/organisation level), and their consideration of the wider community, the health sector, and their appearance in academic literature. Results from this study found that there was no consistency between the indexes investigated, with each index having a diverse number of categories and indicators. Findings from the initial systematic review suggest that hardly any peer-reviewed journal articles exist on the topic of cybersecurity indexes. The paper concludes that most of the indexes studied are broad and do not consider the eHealth sector specifically. Each index relies on a different process to gauge cybersecurity, with little to no academic rigour. It is expected that this research will contribute to the current (limited) literature addressing cybersecurity indexes.

CCS CONCEPTS

• Security and privacy → Formal security models • Applied computing → Consumer health

HIKM'19, January, 2019, Macquarie University, Sydney, Australia

KEYWORDS

Cybersecurity; cybersecurity indexes; cyber maturity; healthcare

1 Introduction

The prevalence of electronic healthcare technology increases patients' concerns relating to the security of healthcare data and devices. The recent Global State of Information Security Survey (GSISS) indicates that privacy risk management needs revitalisation and stronger integration with cybersecurity [1]. However, the health industry lags. Currently, cybersecurity standards specifically designed for the healthcare sector are non-existent, and none are routinely or consistently applied. The cybersecurity landscape reveals fragmented governance, immense interconnectivity amongst sectors, widespread access, the lack of regulatory pressure on security, and limited resources, and are indicative of a need for healthcare-specific cybersecurity standards and solutions [2]. The healthcare sector is vulnerable to security breaches, such as human error (intentionally and unintentionally), malicious or criminal attacks and systems faults.

To this end, this paper explores the cybersecurity landscape to identify cybersecurity indexes that may be relevant to the health industry. This is particularly relevant given the recent prioritisation of digital health as a key to improving service delivery and health outcomes across all states and territories in Australia [3]. For example, in April 2018, the Victorian Government announced: "$124 million to roll out cutting-edge electronic medical records (EMR) across the Peter MacCallum Cancer Centre, Melbourne Health and Royal Women's Hospital" [4]. In 2017, the Australia Government announced in their budget "the creation of a My Health Record for every Australian to begin nationally from mid-2018" [5]. This implies that soon, an automatic electronic health record (My Health Record), will be created for every Australian. The only people who will not have an electronic health record

(EHR) are those who opt-out by the 15th of November 2018. As of the 12th of August, 2018, approximately twenty-four per cent of Australia's population has been registered [6].

In 2016, the Australian Digital Health Agency commenced operation. The Agency is "responsible for national digital health services and systems, with a focus on engagement, innovation and clinical quality and safety" [7]. As part of the Agency, the Digital Health Cyber Security Centre was established to "strengthen the security of our national digital health systems and services; and to promote increased security awareness and maturity across the digital health sector" [8]. The Agency also played a pivotal role in the development of the National Digital Health Strategy [3].

Much research has already been undertaken in regards to cyber threats to health information systems such as EHRs. Luna, Rhine [9] concluded that "cybercrime poses a serious threat to the healthcare industry, and data breaches remain a serious cause for concern". However, not a lot of research has been conducted to gauge Government, the public-private sector and users' cybersecurity capacity to take on such systems as My Health Record in Australia.

In healthcare, the level of consideration of public opinion is an essential element to ensure that health services meet people's needs and are patient-centred. For example, as part of the Australian Commission on Safety and Quality in Healthcare, the National Safety and Quality Health Service (NSQHS) Standard 2 recognises the importance of partnering with consumers to create mutually beneficial outcomes [10]. Consumers are encouraged to have input into clinical governance, quality improvement, and their care. However, a recent consumer survey of healthcare cybersecurity and digital trust found that only 42% of Australian understood digital healthcare data security [11]. This is a potential issue, as the health sector moves to put more medical information online. In the latest 2018 July/September Australian Notifiable Data Breaches Report [12], the healthcare sector recorded the highest data breaches among the top five industry sectors.

Cybersecurity indexes are one method of measuring security preparedness and capabilities of a country or an organisation. 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.

Cybersecurity indexes are often proposed and written by international organisations and universities. They are used as a comparative means for understanding the level of cybersecurity at a national level and, especially for organisations; indexes allow insight into potential vulnerabilities. However, there is very little academic research that investigates their effectiveness and their usefulness in improving cybersecurity capabilities. Also because of their top-down approach, the wider community is often not considered or consulted in the process. Various cybersecurity indexes have been published in the past and emphasise that cybersecurity standards may be relevant even if they are not sector-specific. It does appear that many cybersecurity standards are deliberately not sector-specific. However, with the differences that exist in industry sectors, it may be the case that sector-specific cybersecurity indexes are required to deal with the nuances.

According to the International Telecommunication Union [13], cybersecurity indexes can be broadly split into three major groups; country, organisation, and assessing threats. This study is concerned with the first two groups and is aimed at exploring cybersecurity indexes in the context of the health sector and the wider community. The third group of indexes did not assess countries or organisations. Instead, they reviewed cyber-attack event data and technical aspects of cybersecurity.

Australia's Cyber Security Strategy establishes five themes of actions: national cyber partnership, strong cyber defences, global responsibility and influence, growth and innovation, and cyber smart nation [14]. While four of the five themes primarily look at working relationships between business leaders, the private sector, international partners and the Government, the fifth theme, that is, Cyber Smart Nation, underpins the success of the other four themes. The Cyber Smart Nation theme includes improving the awareness of cybersecurity through partnerships with private and international partners. It also aims to work towards ensuring all Australians understand the risks and benefits of the internet and how to protect themselves online through public awareness initiatives and education campaigns [14]. The findings from this research could provide insights into how useful cybersecurity indexes are regarding measuring eHealth and the impact on the wider community in Australia. The study also aimed to gauge the level of academic research that has been undertaken on cybersecurity indexes.

The rest of the paper is organised as follows: Section 2 describes how cybersecurity indexes were selected for review and the method we employed to begin a systematic literature review. Section 3 outlines the result of our systematic review and each cybersecurity indexes in terms of assessment level and their consideration of broader community and health sector. In Section 4, we look at those cybersecurity indexes that provide an overall score, and finally, Section 5 concludes the paper.

2 Method

The first step in our review was to identify cybersecurity indexes. In a report published by the International Telecommunication Union [13], fifteen indexes were described as "outstanding". These indexes were categorised into three groups, and after drilling further into the fifteen, it was decided that only those indexes dealing at a country or organisation level were appropriate. In addition to these indexes, the Cybersecurity Capability Maturity Model (C2M2) was added to the list. While the C2M2 did not appear in the International Telecommunication Union report, it was initially designed to assess critical infrastructures such as electricity or oil and gas.

The end result was fourteen indexes which had been developed between 2010 and 2017. These include: Capacity Maturity Model for Nations, Cyber Readiness Index (CRI) 2.0, Accenture Security Index, Cyber Maturity in the Asia-Pacific Region, National Cyber Security Index, Information Risk Maturity Index, Cyber Power Index, EU Cybersecurity Dashboard, Kaspersky Cybersecurity

Index, Asia-Pacific Cybersecurity Dashboard, Cybersecurity Poverty Index, Global Cybersecurity Assurance Report Card, the Global Cybersecurity Index and the Cybersecurity Capability Maturity Model (C2M2).

Each index was studied in terms of the level of assessment (country level/organisation level), and their consideration of the wider community, specifically the health sector. As part of this review, we gathered cybersecurity index scores (when available) for countries presiding in the Group of Twenty (G20)[1].

In addition to this, during July 2018, an initial systematic literature review commenced identifying relevant publications in cybersecurity indexes. The Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) framework was used to guide the initial identification of relevant articles. Electronic databases available through the authors' library were used to perform the search queries. The resulting eleven journals that were selected contained one or more research articles on cybersecurity indexed. The final list was as follows: Computer Fraud & Security, Network Security, International Journal of Critical Infrastructure Protection, Computer Law & Security Review, Technological Forecasting & Social Change, Journal of Strategic Studies, Canadian Foreign Policy Journal, Third World Quarterly, Information Security Journal, and the Journal of International Economic Law.

The criteria that were used to gather material was very open. There were no date restrictions[2], all material was retrieved including peer-reviewed journal articles, systematic reviews, theses, books, conference papers, and presentations and articles from non-English sources.

The following combinations of keywords were used: "*Cybersecurity Capacity Maturity Model*" OR "*Cybersecurity Capacity Maturity Model for Nations*" OR "*Cyber security Capacity Maturity Model*" OR "*Cyber Readiness Index (CRI) 2.0*" OR "*Cyber Readiness Index 2.0*" OR "*Accenture Security Index*" OR "*Cyber Maturity in the Asia-Pacific Region*" OR "*National Cyber Security Index*" OR "*Information Risk Maturity Index*" OR "*Cyber Power Index*" OR "*EU Cybersecurity Dashboard*" OR "*Kaspersky Cybersecurity Index*" OR "*APAC Cybersecurity Maturity Dashboard*" OR "*Asia-Pacific Cybersecurity Dashboard*" OR "*Cybersecurity Poverty Index*" OR "*Global Cybersecurity Assurance Report Card*" OR "*Global Cybersecurity Index*" OR "*Cybersecurity Capability Maturity Model (C2M2)*".

3 Results

From our literature search, we identified fourteen common cybersecurity indexes developed between 2010 and 2017. These indexes are now presented in terms of the level of assessment (country level/organisation level), and their consideration of the wider community, specifically the health sector. There was a distinctive lack of academic publications.

3.1 Indexes for assessing countries

A total of nine indexes were found to be relevant for country-level cybersecurity assessment. Indexes at the country level use secondary and primary sources for evaluating cybersecurity. They are designed to gauge the level of cybersecurity of a country by reviewing secondary and primary sources to answer both quantitative and qualitative questions. Data is often gathered from government publications and selected communities such as all the Member States in the International Telecommunication Union [15]. The Kaspersky Cybersecurity Index is the exception to this as it asks the wider community to complete surveys to gauge the current cybersecurity landscape for a country [16].

Developed by the Economist Intelligence Unit and sponsored by Booz Allen Hamilton in 2010, the **Cyber Power Index** consists of four categories and thirty-nine sub-indicators which evaluate/benchmark the ability of a country to withstand cyber-attacks. Legal and regulatory framework, economic and social context, technology infrastructure and industry application make up the four categories. Quantitative secondary sources or estimates (where quantitative data was missing) are then used to score each indicator out of one hundred. Each category and overall score for the country is then calculated from the averages. Nineteen countries of the G20 were selected for analysis [17].

The **EU Cybersecurity Maturity Dashboard** and the **Asia-Pacific Cybersecurity Maturity Dashboard** was developed by BSA, The Software Alliance in 2015. While both indexes are similar, the Asia Pacific Cybersecurity Dashboard has an additional category called cyberlaw indicators[3]. Both Dashboards also review legal foundations, operational entities, public-private partnerships, sector-specific cybersecurity plans and education. Secondary sources were used to evaluate criteria and a status of 'Yes', 'No', 'Partial' or 'Not Applicable' is awarded [18, 19]. Unlike the Cyber Power Index, both Dashboards do not rank their results in 'league' tables. Twenty-eight countries in the European Union and ten countries in the Asia-Pacific region were selected for analysis [20, 21].

The **Cyber Readiness Index 2.0** (2015), created by the Potomac Institute for Policy Studies, builds upon the previous Cyber Readiness Index 1.0 (2013). The index now covers seven categories; national strategy, incident response, e-crime and law enforcement, information sharing, investment in research and development, diplomacy and trade, and defence and crisis support[4]. Across the seven categories, there are seventy indicators. Each indicator can be assessed as wholly or partially operational or insufficient evidence. Primary and secondary sources are used to evaluate each indicator, and 125 countries were assessed. The index evaluates what it means for a country to be "cyber-ready" and is intended to be used to inform national leaders [22].

First introduced in 2014, the **Global Cybersecurity Index** was designed by the International Telecommunication Union (ITU) and

[1] For this analysis the European Union was removed from the G20 list of countries.

[2] The only exception to this is when search for the "Global Cybersecurity Index" which was limited to material written between 2017 and 2018

[3] The EU Cybersecurity Maturity Dashboard consists of twenty indicators across five categories The Asia-Pacific Cybersecurity Dashboard consists of thirty-one indicators across six categories.

[4] The Cyber Readiness Index 1.0 assessed countries across five categories; national strategy, incident response, e-crime and law enforcement, information sharing and cyber readiness and development.

is built upon the ITU Global Cybersecurity five pillars; legal, technical, organisational, capacity building and cooperation. The Index has gone through three iterations, the last being in 2018 and uses primary and secondary information sources. An online survey platform is used to administer the questions, and once completed the questions are weighted, and an overall score is calculated. All Members States (n= 193) were invited to complete the online survey, of which 134 did so. Those who did not respond (n=59) were "invited to validate responses determined from open-source research" [23].

Last run in 2018, the **National Cyber Security Index 2.0** was developed by the eGovernance Academy in Estonia. Initially, the National Cyber Security Index had sixty indicators across three categories, but this was modified in 2018 to forty-six indicators across twelve capacities. The three categories remained the same and are general cybersecurity, baseline cybersecurity and incident and crisis management. To work out an overall score, each indicator was given a value based on publicly available evidence. This 'evidence' is collected directly from government officials, organisations or individuals or through public data collection. One hundred countries have been ranked as of the 23rd of July, 2018 [24].

The **Cyber Maturity in the Asia – Pacific Region** index was developed by the Australian Strategic Policy Institute (ASPI) International Cyber Policy Centre. It is based on International Cyber Policy Centre's (ICPC) 'cyber maturity metric' methodology and assesses governance financial cybercrime enforcement, military application, digital economy and business and social engagement. Evolving methodology. In 2017, the indicators were updated, and the number of countries assessed in the Asia – Pacific – North America region increased to twenty-five. Each indicator is "weighted according to their importance to a state's cyber maturity" and then averaged to produce an overall score. The data used in the Index (for each country) had to be publicly available and from English language sources [25].

Unlike the Indexes mentioned above, the **Kaspersky Cybersecurity Index** takes a different approach to measure country's cybersecurity practices. Twice a year, Kaspersky Lab runs an online survey of internet users around the world. In the second half of 2017, 17,918 responses were gathered from twenty-nine countries. Three main indicators are used to "provide a multi-dimensional picture of the level of danger users are currently exposed to online". These indicators are unconcerned (percentage believing that they will not be a target for cybercrime), unprotected (rate who do not have security solutions) and affected (percentage who have experienced a cybersecurity incident during the last six months). Respondents are also asked about how many and the type of connected devices in their household, the use of security solutions to protect their equipment, their online activities, cyberthreats encountered in the last six months, and the costs of the cyber threat [16].

The **Cybersecurity Capacity Maturity Model for Nations** was developed by the Global Cyber Security Capacity Centre – Universality of Oxford. It was first deployed in 2015 and later revised, with the result being an index with five dimensions and forty-nine indicators. The dimensions cover cybersecurity policy and strategy, cyberculture and society, cybersecurity education, training and skills, legal and regulatory frameworks and, standards, organisations and technology. Within each dimension, there are some 'factors' which "describe what it means to possess cybersecurity capacity". All factors are then made up of several aspects, stages and indicators. The maturity levels of each aspect is characterised on a five-point scale; start-up, formative, established, strategic, and dynamic [26, 27]. Between 2015 and 2017, this model was used to undertake a review of cybersecurity capacity in the United Kingdom, Bhutan, Madagascar, Kosovo, Cyprus, Indonesia, Senegal, Lithuania, Sierra Leone, and the Kyrgyz Republic.

3.2 Indexes for assessing organisations

A total of five indexes were found as relevant for organisation-level cybersecurity assessment. Organisational-level cybersecurity indexes are often undertaken by security experts within a company. Accenture developed the **Accenture Security Index** in 2017. The index has thirty-three capabilities classified into seven domains (business alignment, cyber response readiness, strategic threat context, resilience readiness, investment efficiency, governance and leadership and extended ecosystem). Two thousand executives from twelve industries, across fifteen counties, undertook a survey which aimed to measure their company's performance across the capabilities [28]. No public access to the survey questions, or how each capability is measured, is available from their website.

Created by the Department of Energy in the United States of America in 2014, the **Cybersecurity Capability Maturity Model** (C2M2) was originally designed to be utilised by the energy sector to measure the maturity of an organisation's cybersecurity capability. The index covers ten domains, such as risk management, information sharing and communications, supply chain, workforce, and cybersecurity management. Overall, there are thirty-seven objectives across the ten domains, and each objective has four maturity index levels ranging from zero to three [29].

The **Cybersecurity Poverty Index** was last completed in 2016 by 878 respondents across twenty-four industries. Developed by RSA, this index collected data from organisations from North and South America (n = 438), Europe, the Middle East and Africa (n = 240), and Asia-Pacific (n = 200). The survey consisted of eighteen questions that covered five critical functions outlined by the NIST Cybersecurity Framework (CSF): identify, protect, detect, respond, and recover. Respondents were asked to rate their capabilities using a five-point scale, and each respondent received an overall score based on their answers [30].

Developed by Tenable Network Security, the **Global Cybersecurity Assurance Report Card** first ran in 2016 and underwent an update in 2017. Promoted to information security professionals in the United States, Canada, United Kingdom, Germany, France, Australia, Singapore, Japan, and India, its primary goal was to measure the attitudes and perceptions of information technology security professionals. Seven hundred security professionals across seven industries undertook the online survey consisting of twelve questions. The questions related to

general demographics, the organisation's ability to defend against cyber-attacks, the ability to access risks, and their access to tools to perform cybersecurity [31].

The **Information Risk Maturity Index** was last run in 2014 and was created by Iron Mountain and PricewaterhouseCoopers (PwC). This index consists of thirty-four measures covering strategy, people, communications and security. In 2012, 600 telephone interviews were completed across the United Kingdom, Germany, France, the Netherlands, Spain, and Hungary. Respondents worked in either financial services, insurance, legal, manufacturing and engineering, and pharmaceutical sectors. This was followed up with an additional fourteen qualitative interviews to "probe some of the key issues in more detail". In 2014 a further 1,800 interviews were conducted [32, 33].

3.3 The wider community

Of the fourteen cybersecurity indexes reviewed, only one includes data gathered from the wider community; five do not consider wider community perspectives at all and eight consider the wider community from a third-party perspective.

The Cyber Power Index measures the educational levels of the country. This is a composite of tertiary student enrolment and expected years of schooling. The index also reviews the English literacy of a country[5] and the level of the Internet, mobile, Wi-Fi and social media penetration [17].

While the EU Cybersecurity Maturity Dashboard and Asia-Pacific Cybersecurity Maturity Dashboard do not measure the educational level of a country, they both look at whether the country has an "education strategy to enhance cybersecurity knowledge and increase cybersecurity awareness of the public from a young age" [18, 19].

Under capacity building activities, The Global Cybersecurity Index measures the development and implementation of cybersecurity public awareness campaigns. It also asks for the target demographic of these campaigns and education and training strategies in cybersecurity. Unlike the Cyber Power Index, it does not review education levels, English literacy of level of technology penetration. It does, however, question the use of public awareness campaigns and online child protection [34].

The National Cyber Security Index 2.0 measures education and professional development under its general cyber security category. This includes evaluating if the primary or secondary education curricula contains cyber safety and the number of bachelors, master and PhD programs. However, it does not review public awareness campaigns, English literacy or child protection [35].

The 2017 version of the Cyber Maturity in the Asia-Pacific Region Index measures "public awareness, debate and media coverage of cyber issues" and the percentage of individuals who use the internet. It does not measure education, English literacy or child protection [25].

The Kaspersky Cybersecurity Index only considers the wider community in their evaluation. This is also the only country evaluation technique that surveys the population rather than select government/organisational bodies or secondary information sources. Similar to other indexes, the Kaspersky Cybersecurity Index reviews the level of technology penetration (uptake and usage) but also looks at protection means, online activity, threats faced and cost of incidents [16].

The Cybersecurity Capacity Maturity Model for Nations contains two dimensions that measure societal and educational aspects. Dimension 2: Cyber Culture and Society reviews factors such as mindset, trust and confidence on the internet, personal information protection, reporting mechanisms and the media and social media. Dimension 3: Cybersecurity Education, Training and Skills examinations awareness raising in the general population and cybersecurity education. Like the Global Cybersecurity Index, the Cybersecurity Capacity Maturity Model for Nations also addresses child protection under Dimension 4: Legal and Regulatory Frameworks and through Dimension 2. The Model also reviews reporting mechanisms for cyber incidents such as those outlined in Kaspersky Cybersecurity Index [26, 27].

3.4 The health sector

Of the fourteen cybersecurity indexes, only one specifically includes a health perspective. Six indexes include questions, or indicators, surrounding the public-private sector or essential services, of which the health sector might fall under.

The Cyber Power Index "measures the depth and prevalence of digital infrastructure across key sectors" [17]. The five key indicators include smart grids, electronic health e-health, e-commerce, intelligent transportation, and e-government. While Australia was found to lead the industry application category, it only ranked first within the e-health indicator. The e-health indicator looks at e-health initiatives including the "development of medical records, telemedicine provision, and mobile health delivery"[6] [17].

Broadly, the EU Cybersecurity Maturity Dashboard, Asia-Pacific Cybersecurity Maturity Dashboard, and the Global Cybersecurity Index all contain questions relating to the public-private sector. In the Cybersecurity Maturity Dashboards, these questions revolve around "public-private sector cybersecurity plans", "policy, legislation, or other relevant government publications that define security priorities for specific sectors" and "sector-specific cybersecurity risk assessments" [18, 19]. The Global Cybersecurity Index reviews if CERT/CSIRT or CERT has been applied to a variety of areas including health. It also has questions regarding if the government approved and/or endorsed cybersecurity standards and/or framework for public and private sector and the use of cloud for cybersecurity in the public sector [34].

The Cyber Readiness Index 2.0 does contain a question that measures the "commercial-sector entities affected by, and/or, responsible for the implementation of the national cybersecurity strategy (recognising commercial-sector dependencies)" [22].

[5] This is measured on a five-point scale from very low proficiency to very high proficiency

[6] This is measured on a five-point scale; e-Health technology does not exist, minimal infrastructure, moderate deployment, deployment across most common areas, well-developed deployment.

However, it is hard to tie this to the health sector as this sector, in Australia, is considered both public and private [36].

The National Cyber Security Index 2.0 contains a handful of indicators that the health sector might generically fall under. For example, the operators of essential services indicators review if any crucial services have been identified and if their unique cybersecurity requirements have been analysed and managed. There is also a section of the Index that evaluates the protection of personal data [35]. The health sector, as an essential service, could be listed under this indicator. However, there are no requirements within this index to do so.

The 2017 version of the Cyber Maturity in the Asia-Pacific Region Index contains one indicator that the generically considers if there is a "dialogue between government and industry regarding cyber issues" and the quality of the interaction [25]. This indicator makes no mention of the health sector, or any other sector and is primarily reviewing a governments link to businesses and their potential to respond to cyber concerns and cyber investment.

The Kaspersky Cybersecurity Index does not consider the health sector in any way. It does ask respondents to indicate their online activity in several areas such as banking, shopping, and adult entertainment [16].

Similar to the Kaspersky Cybersecurity Index, the Cybersecurity Capacity Maturity Model for Nations does not explicitly consider the health sector. However, it does mention areas in general under Dimension 5, that is, the use of cybersecurity technology to protect individuals, organisations and national infrastructure [26, 27].

Finally, the Cybersecurity Capability Maturity Model (C2M2), while not originally written for the health sector, claims to assist organisations, regardless of industry [29]. This index has been used in areas such as information technology services, electricity subsector, and water and dam infrastructure. However, there is currently no evidence that it has been applied to the health sector.

3.5 Academic literature on Cybersecurity Indexes

There was very little academic literature found on the cybersecurity indexes mentioned in Section 3.1 and 3.2, using the keywords listed in Section 2. The Cybersecurity Capability Maturity Model returned the highest number of documents (n = 17), followed by Cyber Power Index (n = 7). The documents found were published in the last six years, with the majority published in 2018. A list of indexes that returned a search result and the document type (journal article, conference paper, dissertations) is reported in Table 1. Table 2 contains an indication of when the documents were published.

Table 1: Cybersecurity indexes and document types

Index	Conference Proceedings	Journal Article	Dissertations	Total
Cyber Power Index	-	5	2	**7**
Cyber Readiness Index 2.0	-	-	2	**2**
Cybersecurity Capability Maturity Model	2	3	12	**17**
EU Cybersecurity Dashboard	-	1	2	**3**
Information Risk Maturity Index	-	2	1	**3**
RSA Cybersecurity Poverty Index	-	1	-	**1**

Table 2: Cybersecurity indexes and publication dates

Index	Publication Year						Total
	2013	2014	2015	2016	2017	2018	
Cyber Power Index	2	1	-	1	1	2	**7**
Cyber Readiness Index 2.0	-	-	-	1		1	**2**
Cybersecurity Capability Maturity Model	2	2	3	3	3	4	**17**
EU Cybersecurity Dashboard	-	-	-	2	-	1	**3**
Information Risk Maturity Index	1	-	1	-	-	1	**3**
RSA Cybersecurity Poverty Index	-	-	-	-	-	1	**1**

Table 3: Cybersecurity scores for the G20 countries

	Cyber Power Index (2010)	Global Cyber-security Index (2017)	National Cyber Security Index 2.0 (2018)	Cyber Maturity in the Asia-Pacific Region (2017)	Median	Average
Argentina	35.4	48.0	36.4	-	**36.4**	**39.9**
Australia	71.0	82.0	55.8	88.0	**76.5**	**74.2**
Brazil	38.6	59.0	29.9	-	**38.6**	**42.5**
Canada	66.6	81.0	57.1	-	**66.6**	**68.2**
China	34.6	62.0	35.1	70.2	**48.5**	**50.5**
France	61.8	81.0	83.1	-	**81.0**	**75.3**
Germany	68.2	67.0	83.1	-	**68.2**	**72.8**
India	28.3	68.0	50.7	55.8	**53.2**	**50.7**
Indonesia	23.5	42.0	19.5	54.3	**32.8**	**34.8**
Italy	49.5	62.0	64.9	-	**62.0**	**58.8**
Japan	59.3	78.0	62.3	88.0	**70.2**	**71.9**
Korea[8]	59.7	78.0	-	86.8	**78.0**	**74.8**
Mexico	36.3	66.0	36.4	-	**36.4**	**46.2**
Russia	31.7	78.0	63.6	-	**63.6**	**57.8**
Saudi Arabia	25.7	56.0	23.4	-	**25.7**	**35.0**
South Africa	30.2	52.0	27.3	-	**30.2**	**36.5**
Turkey	30.4	58.0	41.6	-	**41.6**	**43.3**
United Kingdom	76.8	78.0	75.3	-	**76.8**	**76.7**
United States	75.4	92.0	64.9	90.8	**83.1**	**80.8**

4 Analysis of Cybersecurity Index Scores

Four of the nine country-level indexes ended with a country receiving a score. All these indexes surveyed a different number of countries, ranging from 19 to 193 countries. It was therefore decided to use the scores, when available, from the countries who are members of the G20. The counties of the G20 were used as they account for "86 per cent of the world economy, 78 per cent of global trade, and the two-thirds of world's population, including more than half of the world's poor" [37]. Where required, scores were rounded to one decimal place, and due to the initial scores from the Global Cybersecurity Index being decimal numbers between zero and one, a decision was made to multiply the scores by one-hundred to help with averaging.

Our observation is that there appears to be no consistency. For example, Australia received a score of 71 in the Cyber Power Index performed in 2010 [17]. In 2017 and 2018 Australia's score ranged from 55.84 (National Cyber Security Index 2.0) to 88 (Cyber Maturity in the Asia Pacific Region). While it is acknowledged that these scores might differ due to different methodologies, the researchers believe that similar scores should be possible. The United Kingdom received 76.8, 78 and 75.32 from the Cyber Power Index, Global Cybersecurity Index and National Cyber Security Index 2.0[7]. A more significant issue that arises, because of the differences in scores, is that it is hard to justify one cybersecurity index over another. A full list of the G20 countries and their scores can be found in Table 3.

The Cyber Power Index was last run in 2010, which could partially explain the differentiation in scores. The scores from this index are lower than those obtained for the G20 countries using the Cyber Maturity in the Asia Pacific Region index. The Global

[7] As the United Kingdom does not reside in the Asia-Pacific Region there are no results from the Cyber Maturity in the Asia-Pacific Region Index

[8] Republic of Korea. In the Cyber Power Index results, South Korea was used. In the G20 list of nations the Republic of Korea is used

Cybersecurity Index faired similar, except for Germany who received a slightly lower score compared to the Cyber Power Index. Eight of the National Cyber Security Index 2.0 scores, however, were lower than the corresponding Cyber Power Index score. Of the Indexes conducted during 2017 and 2018, The National Cyber Security 2.0 resulted, on average, a lower score than the Global Cybersecurity Index and Cyber Maturity in the Asia Pacific Region.

Indonesia consistently received one of the lowest scores across all indexes. Whereas Australia and the United States were the only countries to receive high scores in three of the four indexes.

5 Discussion, Conclusion and Further Work

The findings from this review were mixed. Of the fourteen indexes, nine assessed at a country level and five assessed at an organisational level. There were no standards, with each index having a diverse number of categories and indicators. Some indexes resulted in a score; others did not rank their results in league tables. Evidence to calculate the level of adherence was often obtained from secondary sources, with four of the country indexes using both primary and secondary sources. The Kaspersky Cybersecurity Index measures public perception and experience to come up with scores for a country is unique to the other indexes. Many country indexes survey government officials or use publicly available data. The indexes were also analysed to see if they considered the wider community and/or the health sector in their evaluation. Eight out of fourteen indexes measured areas such as educational level, English literacy, public awareness campaigns, online activity and cybersecurity mindset; all of which were considered by the researcher as public indicators. The Kaspersky Cybersecurity Index was the only index to concentrate on the wider community in their evaluation. When it came to considering the health sector in their evaluation, only one of the fourteen indexes specifically mentioned eHealth. Seven out of the fourteen indexes measured areas such as specific sectors, the public-private sector or generalised essential services.

The last part of the investigation was to use the PRISMA framework to initiate a literature search on each cybersecurity index. There was a distinctive lack of academic publications. The next step of our investigation will involve broadening the literature review, screening the results, and reporting back on those papers that are instrumental in providing guidance in cybersecurity indexes. Currently, we have only searched for in journals available in the researchers' library. However, a quick google scholar search, of all material including theses, books, conference papers and presentation, and articles from non-English sources, has revealed approximately 181 records.

As our research shows, the current indexes evaluate countries and organisations in some broad areas, but very few address eHealth and the individual. This essentially points out the lack of maturity in the indexes themselves. The fact that there was no consensus in indexes alerts us to the fact that we may not take such measures too seriously. In the short term, it is expected that this research will contribute to the current (limited) literature addressing cybersecurity indexes.

This study has implications for policy and practices in healthcare. In the long term, information gathered from this study will help inform us in the development of a novel cybersecurity eHealth index. It is envisioned that this new security index will be aimed at empowering individuals to undertake their evaluation of security preparedness and capabilities in the area of health. This is particularly relevant as Australia moves towards the introduction of electronic health records.

ACKNOWLEDGMENTS

We acknowledge the support from the Internet Commerce Security Lab (ICSL), Federation University Australia. Westpac, IBM and the Victorian State Government are partners in ICSL.

REFERENCES

[1] PwC. *Revitalizing privacy and trust in a data-driven world: Key findings from The Global State of Information Security Survey 2018.* 2018.
[2] Martin, G., Martin, P., Hankin, C., Darzi, A. and Kinross, J. Cybersecurity and healthcare: how safe are we? *BMJ*, vol. 385, 2017.
[3] Australian Digital Health Agency. *Safe, seamless and secure: evolving health and care to meet the needs of modern Australia*. 2017.
[4] Victorian Government. *Electronic Patient Records to Save Lives*. 2018.
[5] Commonwealth of Australia. *My Health Record*. 2017.
[6] Australian Government. *My Health Record Statistics as at 12 August 2018*. 2018.
[7] Australian Digital Health Agency. *About the Agency*. 2018.
[8] Australian Digital Health Agency. *Digital Health Cyber Security Centre*. 2018.
[9] Luna, R., Rhine, E., Myhra, M., Sullivan, R. and Kruse, C. Cyber threats to health information systems: A systematic review. *Technology And Health Care: Official Journal Of The European Society For Engineering And Medicine*, 24, 1 (2016), 1-9.
[10] Australian Commission on Safety and Quality in Health Care. *National Safety and Quality Health Service Standard 2: Partnering with Consumers*. 2017.
[11] Accenture Consulting. *Digital Trust: Building Digital Trust with Australian Healthcare Consumers*. 2017.
[12] Office of Australian Information Commissioner. *Notifiable Data Breaches Quarterly Statistics Report 1 July – 30 September 2018*. 2018.
[13] International Telecommunication Union. *Index of Cybersecurity Indices*. 2017.
[14] Commonwealth of Australia *Australia's Cyber Security Strategy: Enabling innovation, growth & prosperity*. 2016.
[15] Global Cybersecurity Index. *Cybersecurity Index of Indices*. 2015.
[16] Kaspersky Lab. *Kaspersky Cybersecurity Index*. 2018.
[17] Booz Allen Hamilton. *Cyber Power Index: Findings and Methodology*. 2011.
[18] BSA, The Software Alliance. *Methodology and criteria for the cybersecurity reports - EU Cybersecurity Dashboard*. 2015.
[19] BSA, The Software Alliance. *Methodology and criteria for the cybersecurity reports - Asia-Pacific Cybersecurity Dashboard*. 2015.
[20] BSA, The Software Alliance. *EU Cybersecurity Dashboard. A path to a secure European cyberspace*. 2015.
[21] BSA, The Software Alliance. *Asia-Pacific Cybersecurity Dashboard. A path to a secure global cyberspace*. 2015.
[22] Hathaway, M., Demchak, C., Kerben, J., McArdle, J. and Spidalieri, F. *Cyber Readiness Index 2.0. A plan for cyber readiness: A baseline and an index*. 2015.
[23] International Telecommunication Union. *Global Cybersecurity Index 2017*. 2017.
[24] e-Governance Academy Foundation. *Methodology*. n.d.
[25] Australian Strategic Policy Institute. *Cyber maturity in the Asia-Pacific region 2017*. 2017.
[26] Global Cyber Security Capacity Centre *Cybersecurity Capacity Maturity Model for Nations (CMM) - Revised Edition*. 2016.
[27] Global Cyber Security Capacity Centre. *Cybersecurity Capacity Maturity Model for Nations (CMM) - Revised Edition*. 2016.
[28] Bissell, K., LaSalle, R. and Richards, K. *The Accenture Security Index*. 2017.
[29] U.S. Department of Energy. *Cybersecurity Capability Maturity Model*. 2014.
[30] RSA. *RSA Cybersecurity Poverty Index - 2016*. 2016.
[31] Tenable Network Security and CyberEdge Group. *2017 Global Cybersecurity Assurance Report Card*. 2017.
[32] PwC. *Beyond good intentions: An introduction to the 2014 Information Risk Maturity Index*. 2014.
[33] PwC and Iron Mountain. *Beyond cyber threats: Europe's first information risk maturity index*. 2012.
[34] International Telecommunication Union *Global Cybersecurity Index (GCI) 2018 Questionnaire Guide*. 2018.
[35] e-Governance Academy Foundation. *Ranking*. 2018.
[36] healthdirect. *Understanding the public and private hospital system*. 2017.
[37] Australian Government. *The G20*. 2018.