Healthcare Cyber Security Challenges and Solutions Under the Climate of COVID19: A Scoping Review

Ying He, Aliyu Aliyu, Mark Evans, Cunjin Luo

Submitted to: Journal of Medical Internet Research
on: June 23, 2020

Table of Contents

Healthcare Cyber Security Challenges and Solutions Under the Climate of COVID19: A Scoping Review

Ying He[1] PhD; Aliyu Aliyu[2] MSc; Mark Evans[2] PhD; Cunjin Luo[3, 4] PhD

[1]School of Computer Science University of Nottingham Nottingham GB
[2]School of Computer Science and Informatics De Montfort University Leicester GB
[3]School of Computer Science and Electronic Engineering University of Essex Colchester GB
[4]Key Lab of Medical Electrophysiology, Ministry of Education Institute of Cardiovascular Research Southwest Medical University Luzhou CN

Corresponding Author:
Cunjin Luo PhD
School of Computer Science and Electronic Engineering
University of Essex
Wivenhoe Park
Colchester
GB

Abstract

Background: Coronavirus disease (COVID-19) has been an unprecedented challenge to the global health care system. It has further challenged the resilience of the healthcare information system (HIS), which has affected the ability to achieve the global sustainable goal of health and wellbeing. This research is motivated by the recent security incidents that happened to the hospitals, pharmaceutical companies, the US Department of Health and Human Services, the World Health Organization (WHO) and its partners, etc.

Objective: This study aims to assess the security incidents, identify the challenges and provides cybersecurity recommendations to support the healthcare sector against the heightened cybersecurity risk realised through associated threats, including phishing campaigns and ransomware attacks which have been adapted to exploit vulnerabilities in technology and people introduced through changes to working practices dealing with the current COVID-19 pandemic.

Methods: We performed a review of the topic of health sector security challenges and recommendations during COVID 19, through the searches of two major scientific databases (PubMed and Scopus) references from relevant articles using the search terms “healthcare” and “cybersecurity”. Reports, news articles, or websites were also included only when they related directly to previously published work, or they were the only currently available information source at the moment of manuscript preparation. Only articles in English in the later decade were included, i.e. 2010-2020, in order to focus on the current issues, challenges and solutions.

Results: This research concluded that the most prominent and significant methods of attack and threats of the security incidents that happened during COVID 19 are related to phishing, ransomware, distributed denial of service attack and malware. We have identified challenges (8 themes) that have led to the incidents. The health sector have implemented some solutions (8 themes) to address these challenges. However, more efforts are needed in improving some aspects (4 themes) to strengthen their cybersecurity capacity.

Conclusions: This research identified the most prominent and significant methods of attack and threats related to the security incidents that impacted the health sector initially during the COVID 19 pandemic, the cybersecurity challenges, solutions as well as the areas that require further efforts in the community. This provides useful insights to the health sector to address their cybersecurity issues during the COVID 19 pandemic as well as other epidemics or pandemics that may materialise in the future.

(JMIR Preprints 23/06/2020:21747)
DOI: https://doi.org/10.2196/preprints.21747

Preprint Settings

1) Would you like to publish your submitted manuscript as preprint?
Please make my preprint PDF available to anyone at any time (recommended).

Please make my preprint PDF available only to logged-in users; I understand that my title and abstract will remain visible to all users.
Only make the preprint title and abstract visible.

✓ **No, I do not wish to publish my submitted manuscript as a preprint.**

2) If accepted for publication in a JMIR journal, would you like the PDF to be visible to the public?

✓ **Yes, please make my accepted manuscript PDF available to anyone at any time (Recommended).**

Yes, but please make my accepted manuscript PDF available only to logged-in users; I understand that the title and abstract will remain v

Yes, but only make the title and abstract visible (see Important note, above). I understand that if I later pay to participate in <a href="http

Original Manuscript

Original Paper

Healthcare Cyber Security Challenges and Solutions Under the Climate of COVID19: A Scoping Review

Ying He[1], Aliyu Aliyu[2], Mark Evans[2] and Cunjin Luo[3,4]*

[1.] School of Computer Science, University of Nottingham, Nottingham, UK

[2.] School of Computer Science and Informatics, De Montfort University, Leicester, UK

[3.] School of Computer Science and Electronic Engineering, University of Essex, Colchester, UK

[4.] Key Lab of Medical Electrophysiology, Ministry of Education, Institute of Cardiovascular Research, Southwest Medical University, Luzhou, China

*Corresponding Author:

Cunjin Luo

School of Computer Science and Electronic Engineering

University of Essex

Colchester, UK

Email: cunjin.luo@essex.ac.uk

Abstract

Background: Coronavirus disease (COVID19) has challenged the resilience of the healthcare information system (HIS), which has affected the ability to achieve the global sustainable goal of health and wellbeing. This research is motivated by the recent cyber-attacks that have happened to the hospitals, pharmaceutical companies, the US Department of Health and Human Services, the World Health Organization (WHO) and its partners, etc.

Objective: The aim of this review was to identify the key cyber security challenges, cyber security solutions adopted by the health sector and the areas to be improved in order to counteract the heightened cyber-attacks such as phishing campaigns and ransomware attacks which have been adapted to exploit vulnerabilities in technology and people introduced through changes to working practices dealing with the current COVID19 pandemic.

Methods: A scoping review was conducted through the searches of two major scientific databases (PubMed and Scopus) using the terms "(covid or healthcare) and cybersecurity". Reports, news articles, industrial white papers were also included only when they are related directly to previously published work, or they were the only available sources at the moment of manuscript preparation. Only articles in English in the last decade were included, i.e. 2011-2020, in order to focus on the current issues, challenges and solutions.

Results: This scoping review identified 9 main challenges in cyber security, 11 key solutions that the healthcare organisations adopted to address these challenges, and 4 key areas that require to be strengthened in terms of the cyber security capacity in health sector. We also found that the most prominent and significant methods of cyber-attacks happened during COVID19 are related to phishing, ransomware, distributed denial of service attack and malware.

Conclusions: This scoping review identified the most prominent and significant methods of cyber-attacks that impacted the health sector initially during the COVID 19 pandemic, the cyber security

challenges, solutions as well as the areas that require further efforts in the community. This provides useful insights to the health sector to address their cybersecurity issues during the COVID 19 pandemic as well as other epidemics or pandemics that may materialise in the future.

Keywords: Healthcare; Security Incidents; Root Causes; Cyber Security Challenges; Cyber Security Solutions; COVID19; Pandemics.

Introduction

Coronavirus disease (COVID19) has been an unprecedented challenge to the global health care system. It has further challenged the resilience of the Health Information System (HIS), which has affected the ability to achieve the global sustainable goal of health and wellbeing. This research is motivated by the recent cyber-attacks that have impacted the healthcare organisations such as Brno University Hospital [1], the US Department of Health and Human Services [2], the World Health Organization (WHO) [3], Gilead Sciences Inc pharmaceutical [4], Romanian hospitals [5], as well as the general supply chain in the health sector [6].

Rationale

The COVID19 pandemic has created a new reality for the health sector. The sector has become a primary target of adapted cybersecurity attacks [7, 8]. The attackers are taking advantage of the COVID19 pandemic and have launched a number of cyber-attacks against healthcare organisations [1-6]. {Jacobs, #762} To manage the pandemic and the extraordinary situation, the health sector has shifted its focus on the security of their systems and practices to their primary duty of deliver healthcare in order to save lives, which has placed themselves in a vulnerable situation. The health sector must be prepared to counteract cyber-attacks in order to protect the availability of essential healthcare services as well as the confidentiality and integrity of healthcare information.

Cybercrime adapts to the changes of the world situation around it very quickly. At the beginning of an escalating of the COVID19 pandemic, malware cyber-attackers have identified common vulnerabilities and have adapted their attacks to exploit these vulnerabilities. The current situation in the UK and worldwide provides a fertile breeding ground for various cyber-attacks [9]. As the cyber attackers are leveraging the increased reliance in remote working, decreased mobility and closure of

borders between different countries, the increase in demand for Personal Protective Equipment (PPE) such as the masks and gloves. The complex healthcare supply-chain is also a target for adversaries [10]. Indeed, all these are leading to increasing fear, uncertainty and doubt in the general population.

There are some research efforts reviewing the literature in cyber security in health sector. Jalali, et al. performed a systematic review of the literature on cybersecurity response plans in healthcare [11]. Coventry, et al. conducted a narrative review on the trends of the cyber threats and ways forward in health sector [12]. Kruse, et al systematically reviewed healthcare related cyber threats and trends [13]. Offner, et al. reviewed the cyber threats and mitigation in Australian healthcare organisations [14]. Sardi, et al. performed a systematic review of Cyber Risk in Health Facilities [15]. However, there are limited research efforts on an in-depth review and analysis of the key cyber security challenges and solutions in health sector specifically under the pandemic situation such as COVID19.

Objective

Through a scoping review, this paper aims to identify the most prominent and significant methods of attack and threats that have affected the health sector during the COVID19 pandemic, the cybersecurity challenges, solutions as well as the areas that require further efforts in the community. This research covers not only the security-related matters as a result of the COVID19 pandemic but also discuss the inherent security challenges in health information systems that can be potentially exploited by attackers during the COVID19 pandemic. It has implications for the whole spectrum of the health sector as a result of the increase of cybersecurity risks such as Distributed Denial of Service (DDoS), phishing and ransomware attacks during the coronavirus crisis and in the long term.

Methods

Protocol and registration

The review followed PRISMA-ScR: Preferred Reporting Items for Systematic Reviews and Meta-Analyses extension for Scoping Reviews, proposed by Joanna Briggs Institute (JBI) [16]. The aim of this review is to identify health sector cyber-attacks, security challenges and solutions. Before undertaking this review, a protocol was created detailing the information sources, searching strategies, eligibility criteria, selection of sources of evidence and data charting processes. The PRISMA-ScR checklist together with the page numbers corresponding to each subsection are presented in Appendix.

Information sources

A search of two major scientific databases (PubMed and Scopus) was performed to identify the relevant articles. These include both the original research articles and review articles.

Search

The search formular “(covid or healthcare) and cybersecurity” was used to search for the articles. The articles identified should have either a covid cybersecurity core or a healthcare cybersecurity core.

Eligibility criteria

Only articles in English in the last decade were included, i.e., 2011-2020, in order to focus on the current issues, challenges and solutions. Reports, news articles, or websites were also included only when they are related directly to previously published work, or they were the only currently available information source at the moment of manuscript preparation. Inclusion criteria were as follows:

- relevance to healthcare cybersecurity of the paper as a whole.
- coverage of well-discussed cyber security issues, challenges and solutions.

Selection of sources of evidence

The selection process was illustrated in Figure 1. The results of search were exported to the Endnote library. The title and abstract of each paper were analysed by two of the authors to assess whether it fell into the specified criteria. In cases in which this was not obvious, all four authors looked at the paper and, when necessary, read it to assess relevance. 307 identified papers in total were screened. There were 53 duplicates removed, then 57 papers excluded due to the lack of “healthcare or covid” core or “cybersecurity” core in the abstract. A further 197 papers were excluded due to the lack of “healthcare or covid” core or “cybersecurity” core in the full text. 56 papers were finally included in the review.

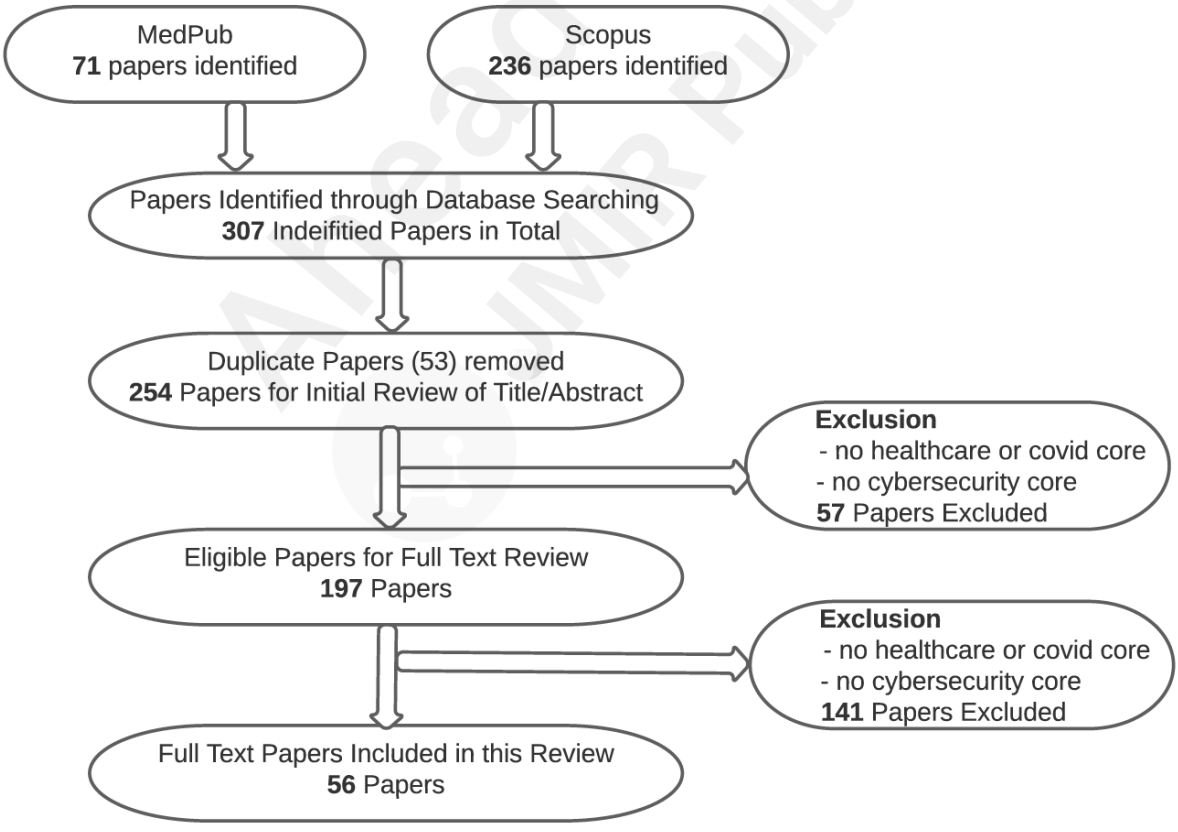


Figure 1: Flowchart showing the article identification and selection process

Data charting process

The data was extracted and stored in a standardized Microsoft Excel form. This was an iterative process whereby the charting table is continually updated. Data charting was carried out both independently and in duplicate by at least two authors to ensure the quality of the extracted key findings from the literature, before being used for results analysis.

Data items

Key data items including title, abstract, authorship, aims, key findings related to the review objectives, evidence document, document type, year of publication, and the location.

Critical appraisal within sources of evidence

Although JBI suggested that the critical appraisal is usually not needed for a scoping review, we had at least two authors checking the quality and source of evidence, making sure that they were relevant, up to date and from reputable sources. In cases in which this was not obvious, all four authors looked at the sources and assessed them.

Synthesis of results

Through aggregating the information from the selected literature, the results were analysed and qualitatively presented in both tabular forms and descriptive format (grouped into themes) which aligned with the objective/s and scope of the review, reported in the Results section.

Results

This section presents the analysis of the selected literature. As illustrated in Figure 1. 307 identified papers in total were screened. There were 53 duplicates removed, 57 papers excluded due to the lack of “healthcare or covid” core or “cybersecurity” core in the abstract. A further 197 papers were excluded due to the lack of “healthcare or covid” core or “cybersecurity” core in the full text. 56 papers were finally included in the review. The source of evidence was checked by at least two authors to make sure that they are relevant, up to date and are from reputable sources. The results are grouped into four themes including health sector condition changes due to COVID 19, healthcare cyber attacks during COVID 19 pandemic, healthcare cyber security challenges, and healthcare cyber security controls.

Health Sector Condition Changes due to COVID 19

This section reviews the changes of conditions as a result of COVID 19. The findings are elaborated below and summarised in Table 1. The main changes to health services caused by the COVID 19 pandemic include decreased mobility and border closures, the increasing reliance on remote working, often with little previous experience and planning. These conditions have made the health sector more vulnerable to potential cyber-attacks [7, 8, 17].

As health staff and patients are restricted in terms of movement due to the lockdown, the decrease in mobility and border closures makes individuals and organisations turn to technology to provide essential health services such as appointments, diagnosis and even operations. Examples are the use of eConsultation services for patients and eMDT (Multi

-Disciplinary Teams). Although these technologies have their advantages, it is leaving the users and receivers of these technologies open to a variety of attacks such as phishing campaigns and ransomware attacks [18].

Furthermore, the health services staff often have little previous experience of remote working and planning of this change in working practice leaving the sector vulnerable to cyber-attacks [9, 14, 19]. As health services make use of a variety of medical devices, the interconnectivity and interoperability create issues as they are now being accessed from outside the health services internal network perimeter. The medium and mode of access creates problems as access to the sensitive parts of the health services can be reached via unsecured network connections or unpatched systems by the remote working staff [19]. Besides, some medical devices use off-the-shelf software, such as commercial operating systems (e.g., older versions of Microsoft Windows). These systems are vulnerable to a large variety of threats such as malware, ransomware, etc. [20, 21]. Overall, the healthcare industry significantly lags behind other industries in terms of cybersecurity, coupled with a lack of digital literacy among staff mostly working from home, making it a prominent target [15, 22].

Additionally, the increase in demand for certain goods such as PPE and other protective merchandise such as masks, gloves, etc. are making health services and even governments exposed to digital scams, especially in the form of phishing attacks. As health services are in need of these essential items, they can be targeted by adversaries with luring emails with the intention of stealing sensitive information [17].

Table 1. Health Sector Condition Changes due to COVID 19

Health Sector Condition Changes due to COVID 19	**Author**
The decreased mobility and border closures, and the increasing reliance on remote working, create challenges to health sector.	Hakak, Khan [7] Williams, Chaturvedi [8] Schneck [17]
New technologies such as eConsultation services for patients and eMDT leaves the users open to a variety of attacks.	Weil and Murugesan [18]
Health services staff often have limited experience of remote working leaving the sector vulnerable to cyber-attacks, such as malwares.	Boddy, Hurst [9] Offner, Sitnikova [14] Jalali, Bruckes [19]

	Hoffman [20] Ronquillo, Erik Winterholler [21]
Healthcare industry significantly lags behind other industries in terms of cybersecurity and lacks digital literacy among staff working from home, making it a prominent target.	Sardi, Rizzi [15] Kim, Choi [22]
The increase in demand for certain goods such as PPE makes health services and governments exposed to digital scams such as luring emails with the intention of stealing sensitive information.	Schneck [17]

Healthcare Cyber Attacks during COVID 19 Pandemic

This section reviews the recent cyber-attacks that happened at the beginning of the global Covid19 pandemic (early 2020) in the health sector. We have selected well documented cyber-attacks with detailed information available including root causes and consequences. The main findings are described below and summarised in Table 2.

Brno University Hospital in the Czech Republic, which is one of the country's main COVID19 testing centres, was struck by ransomware resulting in the postponement of surgeries. The ransomware infection was confirmed in the early hours of the day when the hospital decided to disconnect all computer network. It was noticed that the ransomware infection was gradually replicating, and all the individual systems were failing, and all computers had to be shut down. The hospital is reported to be still recovering capabilities, as it is still not yet fully operational due to the attack [1]. The attack had an impact on the activities of the hospital as there is no database systems, i.e. means of storing data; hence staff have to write and transfer their notes manually. This leads to

slow processes and can potentially endangering lives in these trying times.

The US Department of Health and Human Services (HHS) that suffered a Distributed Denial of Service (DDoS) attack intended to disrupt the organisation's responses to the COVID19 pandemic. This attack targeted the servers of the HHS by overloading it with millions of hits over several hours [2]. It was reported as a campaign of disruption aimed at hindering the response to the coronavirus pandemic as the targeted agency was tasked with protecting the health of citizens and delivering essential human services. Although the agency claimed the attack was not successful, and the attackers did not infiltrate the internal network nor steal any data. It does show attacks like these can cause damage not just to the services of health agencies but to lives that depend on it, especially in times of emergencies.

Increased phishing website hacking attempts on the World Health Organization (WHO) and its partners, has led to the WHO to put out a warning, informing the general public to be more careful [3]. As it has been reported that over 4,000 coronavirus-related domains, i.e. domains that contain words like "corona" or "covid" have been registered since the beginning of this year 2020. These registered domains were used by adversaries for phishing related activities. Thus, the WHO incident was orchestrated by hackers in order to steal passwords. It was reported that a group of hackers created a malicious website posing as an email login portal for WHO employees in an attempt to steal their passwords. Although WHO claims the attack was not successful, it still shows that phishing attacks can be leveraged to target health organisations.

Coronavirus drug maker Gilead was targeted by hackers [4]. Staff at the Gilead Sciences Inc pharmaceutical company were targeted. A fake email login page was designed to steal passwords, and these were sent to a top Gilead executive involved in legal and corporate affairs. It was reported

that the attack was an attempt to compromise email accounts of staff at the company using messages that impersonated journalists.

Romanian hospitals suffered from ransomware attacks by hackers [5]. The hackers were planning to use COVID19-themed emails to infect Romanian hospitals with ransomware. Their motivation was the protest against the COVID19 quarantine measures of the country. The hackers owned malwares (e.g. remote access trojans, ransomware, website defacements and SQL injection tools) that can be used to bring down servers and steal information. It was reported that they intended to send emails with COVID19 lures to hospitals to infect computers, encrypt files, and disrupt hospital activities However, the attack was not as successful as they were tracked down and arrested by Romanian law enforcement.

It has been reported that Interpol has cautioned agencies around the world about a significant rise in the global number of ransomware attacks explicitly targeting hospitals and health institutions [6]. It discovered that there is an increase in the number of attempted ransomware attacks to organisations in the 194 member countries. Additionally, cyber warning was issued for key healthcare organisations involved in the coronavirus response both in the UK and US. The advisory was a joined statement by the UK's National Cyber Security Centre (NCSC) and US Cybersecurity and Infrastructure Security Agency (CISA) stating that it has uncovered malicious cyber campaigns as it witnessed large-scale 'password spraying' campaigns against healthcare bodies and medical research organisations in both nations [23].

Furthermore, the healthcare supply-chain is not also omitted as it has been reported that the FBI has issued a warning about a malware targeting healthcare supply chains. The malware is called Kwampirs, a Remote Access Trojan (RAT) that exploits network vulnerabilities of the targeted

organisations ranging from the United States, Europe, Asia, and the Middle East [24].

The infected supply chain components included cyber physical systems assets in healthcare organisations. The bureau alerted the healthcare sector against future cyber-attacks, as Kwampirs have been historically targeting healthcare organisations.

The analysis of the above-mentioned incidents show that the health sector has become a primary target of cybersecurity attacks. The attackers are taking advantage of the COVID19 pandemic and launch attacks, which are mainly Ransomware, DDoS, Phishing, and other type of malwares. The healthcare supply-chain can be more vulnerable to cyber-attacks especially during pandemics. The cyber-attacks have resulted in negative impacts on the availability of essential healthcare services and challenged the healthcare organisation in the protection of the confidentiality and integrity of healthcare information.

Table 2. Security Incidents During COVID 19

Security Incidents	**Type of attack**	**Impact**
Brno University Hospital [1]	Ransomware	Postponement of surgeries, appointments, etc.
The US Department of Health and Human Services [2]	Distributed Denial of Service	Disruption to responses to the Covid19 pandemic
The World Health Organization [3]	Ransomware/Phishing	Defacement and misinformation
Gilead Sciences Inc pharmaceutical [4]	Phishing	Impersonation and exfiltration
Romanian hospitals [5]	Phishing/Ransomware	Disruption and exfiltration
The supply chain in the health sector [6]	Malware	Disruption of activities

Healthcare Cyber Security Challenges

This section identifies the main challenges of cybersecurity in the health sector. The selected papers were reviewed. The main findings are elaborated below and summarised in Table 3.

Remote working security assurance. As remote working is now an integral element of healthcare service delivery, health staff are relying on enterprise Remote Desktop Protocol (RDP) and Virtual Private Network (VPN) to access the internal network. However, these come with certain risks that adversaries are looking to exploit as RDP has a history of security issues and generally should not be publicly accessible without additional protections such as firewall, whitelist and multi-factor authentication [10]. Likewise, VPNs also have some known and unknown vulnerabilities, both on the client and server-side which have been exploited for years by adversaries [19]. The DDoS attacks to the healthcare systems [14] and the innumerable wireless connected devices [9] have created further challenges to a remote working environment.

Endpoint device management. A number of endpoint devices entailing various patient monitoring equipment that either connects to the Internet or via legacy dispersed networks are often unpatched [12]. This risk further increased during the pandemic as a result of organisations competing to procure IoT devices during the COVID19 pandemic for their staff, which resulted in more employees than before actually using personal devices to perform work from home. From an Enterprise Architecture (EA) perspective, having tighter integration across the IT environment is positive in terms of the organisation being more agile and having tighter data integration, however, it makes the network vulnerable to cyberattacks such as email phishing, ransomware, DDoS and network data breaches [13]. The integration of new endpoint devices with outdated legacy systems can increase vulnerabilities [13, 25]. However, the organisations overly rely upon perimeter defence (antivirus, firewalls) and other forms of basic protection for protection against cyber-attacks [26]. Through interviewing 19 C-Suite cyber security professionals, Jalali, et al. also confirmed the factor that most influences the cyber security in a hospital is end point complexity [27].

Human factor in cybersecurity. Existing research showed that the majority of information security

incidents are related to human error [28]. There is a tendency for human error when staff are busy focusing on saving lives, working in different ways using new technologies. With the sudden change of working practice, being under stress for an extended period of time, it makes employees vulnerable to falling into malicious trickery and making mistakes [28]. According to Jalali, at al. there is a statistically significant positive correlation between the workload and the probability of a health care staff opening a phishing email [19]. Naidoo, et al. developed a multi-level influence model to explore how cybercriminals exploited the COVID19 pandemic using social engineering techniques [25]. However, the health sector lacks root cause analysis [28] to prevent human error related security incidents especially those through unintentional human error [29]. Although some efforts made in applying the Information Security Human Reliability Analysis technique such as IS-CHEC [30] to analyse human error, such approach has not been widely adopted.

Lack of security awareness. The cybercriminals are exploiting people's anxieties during the COVID19 pandemic. Gordon, et al. identified that there is low awareness in the health sector of the risk [31]. Furnell, et al. identified that the most common action taken in response to the most disruptive breaches or attacks is "additional staff training or communication"[32]. Coventry, et al. reported that heath staff has poor awareness of consequences of behaviour, and there is a lack of policies and reinforcement of secure behaviour [33]. However, an increased cyber security awareness is required for the health sector to protect themselves and their patients from potential cyber threats such as phishing and ransomware. Due to the lack of prior planning and training to work under pandemic situations, the healthcare staff require more training and support, such as pandemics tailored cyber security training campaigns, documented procedures and guidance on revised procedures and technologies [34]. For example, health sector staff should be made aware of and able to flag phishing emails containing buzzwords during a pandemic, such as "WHO," or "donation". They should also be advised on how to validate the trusted information source in order to avoid

ransomware attacks [7].

Inadequate board-level risk assessment communication. There is a lack of understanding of security risks and its impact on organisational wide risk management, such as the impacts on patient care and clinical outcomes [35]. The health sector lacks a matrix that can translate the strategic improvement needs of a healthcare system into prioritised information/cyber improvement needs [36]. Schwartz et al. identified that there is a lack of appreciation amongst healthcare executive management of the business risk impacts of cyber breaches [37].

Inadequate business continuity plans. The health sector does not have enough data protection mechanisms; Walker-Roberts, et al. confirmed that the health sector lacks sophisticated data security tools compared to other industries [38]. Security was not built into its supply chain and third-party vendors. Existing research shows that the key security risks challenging business continuity are vendor dependence, inappropriate encryption configurations, and the inability to handle health information sharing and exchange with third-party and cross border partners [39-42]. Risks will continue to grow if cybersecurity is not designed into from the beginning of the project lifecycle [12]. Cybersecurity capability is a strategic asset that every health organisation must adopt, along with the concepts of building organisational resilience and the capacity to recover from incidents and learn from mistakes in order to maintain business continuity [11].

Lack of coordinated incident response involving different parties. As highlighted by [12], the health care sector has a trend of having time lag between an attack occurring and detection of the breach. Indeed, this help in giving adversaries more time to explore the network and perform lateral movement, which increases the damage of security breaches. Current healthcare cyber-defence is often reactive and undertaken after malicious attacks [43], lacking a coordinated incident response

capacity to counteract constantly emerging and evolving malware threats [44]. The failure of health care organisations in having a successful and secure backup mechanism in place makes it frail in terms of incident response and recovery [12]. Pullin, et al. also confirmed that cyber security should be a team effort, from the board members to front line employees, all held account for cyber security [45].

Limited budget and the need to deliver healthcare services without disruption. Although the healthcare services are spending funding to become more integrated to deliver healthcare services without disruption [9]. The emphasis is not given to the security aspect in terms of keeping software updated and systems secure. However, this is reported to be due to the shortage of experienced cybersecurity experts within healthcare organisations with the required skills and experience to enable healthcare organisations to change their business operations at significant pace without undertaking the 'usual' levels of cybersecurity assurance [46]. Boddy, et al. identified the needs of a value-based system to weigh and balance the benefits and risks in aspects of security, privacy and adoption of technology [9].

Vulnerable Medical Cyber Physical Systems (MCPS). Cybersecurity measures such as vulnerability scans or patch management are often not available or only possible by manufacturers [47]. Their basic limited capability makes them vulnerable to compromise [48]. Cybersecurity measures such as vulnerability scans or patch management are often not available or only possible by manufacturers. Moreover, their connection and reliance upon the healthcare network significantly increase the cybersecurity risk to the entire healthcare system [49]. With the widely spread use of the IoT medical devices, cyber threats can be introduced to the MCPS though vulnerable IoT devices [44].

The analysis shows that the main cyber security challenges of health sector are the remote working

security assurance, endpoint device management, human errors, the lack of security awareness, inadequate senior level security risk assessment, inadequate business continuity plans, the lack of coordinated incident response, constrains on budget and resource as well as the vulnerable medical systems. These challenges cover not only the security-related matters as a result of the COVID19 pandemic but also the inherent security challenges in health sector that can be potentially exploited by attackers during the COVID19 pandemic. It is imperative for the healthcare organisations to identify these challenges and take actions for prevention.

Table 3. Key Health Sector Security Challenges and Associated Vulnerabilities

Key Challenges	**Published Vulnerabilities**	**Author**
Remote working security assurance	There are known security vulnerabilities with RDP and VPN.	Argaw, Troncoso-Pastoriza [10]
	There are known attacks to Healthcare System (HCS) such as DDoS, malware, etc.	Offner, Sitnikova [14]
	Cyber-attacks target on innumerable wireless connected devices in healthcare.	Boddy, Hurst [9]
Endpoint device management.	Endpoint device can provide an entry point to the larger healthcare networks.	Coventry et al. [12]
	The integration of new endpoint devices with outdated, legacy or unsupported operating systems compromises interoperability and increases cybersecurity vulnerability.	Kruse, Frederick [13] Naidoo [25]
	Heath sector heavily relies upon perimeter defence (antivirus, firewalls) for protection against cyber risk.	Reagin and Gentry [26]
	The factor that most influences the cyber security in a hospital is end point complexity	Jalali and Kaiser [27]
Human factor in cybersecurity	The majority of information security incidents are related to human error.	Evans, He [28], Evans, He [29]
	There is a statistically significant positive correlation between the workload and the probability of a health care staff opening a phishing email	Jalali, Bruckes [19]
	The health sector lacks root cause analysis and preventing cyber security incidents especially those through unintentional human error.	Evans, He [28], Evans, He [29]
	Although some efforts made such as the use of IS-CHEC to analyse human error, such approach has not been widely adopted.	Evans, He [30]
Lack of security awareness.	There is low awareness in the health sector of the cyber risks.	Gordon, Fairhall [31]
	The most common action taken in response to the breaches or attacks is additional staff	Furnell and Shah [32]

	training or communication.	
	Heath staff has poor awareness of consequences of behaviour; and there is a lack of policies and reinforcement of secure behaviour.	Coventry, Branley-Bell [33]
	There is a lack of pandemics tailored cyber security training campaigns, documented procedures and guidance on revised procedures and technologies	Kaplan [34]
Inadequate board-level risk assessment communication	There is a need of a matrix that can translate the strategic requirements of a healthcare system into prioritised cyber improvement needs.	Barad [36]
	There is a lack of understanding of security risks and its impact on organisational wide risk management	Tully, Selzer [35]
	There is a lack of appreciation amongst healthcare executive management of the business risk impact of cyber breaches.	Jones and Katzis [37]
Inadequate business continuity plans	Risks will continue to grow if cybersecurity is not designed into the product from the beginning of the product or project lifecycle.	Coventry and Branley [12]
	the key security risks challenging business continuity are vendor dependence, inappropriate encryption configurations, and the inability to handle health information sharing and exchange with third-party and cross border partners	Frontoni, Mancini [39], Bhatia and Ibrahim [40], Natsiavas, Rasmussen [41], Nalin, Baroni [42]
	The health sector lacks sophisticated data security tools compared to other industries.	Walker-Roberts, Hammoudeh [38]
	Cybersecurity capability is a strategic asset that every health organisation must adopt, along with the concepts of building organisational resilience and the capacity to learn from mistakes.	Jalali, Russell [11], Reagin and Gentry [26]
Lack of coordinated incident response	The health sector has a trend of having time lag between an attack occurring and detection of the breach.	Coventry and Branley [12]
	Current healthcare cyber defence is often reactive and undertaken after malicious attacks.	Akinsanya, Papadaki [43]
	There is a lack of a coordinated incident response capacity to actively counteract constantly emerging and evolving malware threats.	Chen, Ding [44]
	Cyber security should be a team effort, from board members to front line employees, all held account for cyber security	Pullin [45]
Limited budget and the need to deliver healthcare services without disruption	There is a lack of experienced cybersecurity experts in the healthcare industry.	Argaw, Bempong [46]
	The is a lack of a value-based system to weigh and balance the benefits and risks in aspects of security, privacy and adoption of technology	Boddy, Hurst [9]
Vulnerable Medical	The limited MCPS capability makes the health	Almohri, Cheng [48]

Cyber-Physical Systems (MCPS)	sector vulnerable to compromises.	
	The reliance on the healthcare network increases the cybersecurity risks to the healthcare systems.	Zheng, Zhang [49]
	Cyber threats can be introduced to the MCPS though vulnerable IoT devices	Jimenez, Jahankhani [47]

Healthcare Cyber Security Controls

This section identifies the cybersecurity solutions present within the health sector. The authors have thoroughly reviewed the selected papers. The main findings are elaborated below and summarised in Table 4.

Apply the endpoint device protection. During the COVID19 pandemic, the health staff working from home may adopt telehealth technologies or IoT devices. This increases cyber security risks, as it expands the footprint for cyber-attack to the use of new devices outside of the service providers' network [50]. Health staff are advised to restrict the technologies and devices they used to remain compliant with security regulations such as Health Insurance Portability and Accountability Act (HIPAA) during the pandemics [20]. However, healthcare organisations mainly reply on perimeter defence (e.g. antivirus, firewalls) for protection against the potential cyber-attacks [26]. The National Institute of Standards and Technology (NIST) has recently released a draft security guide and recommendations for managing the security IoT devices, but it is unclear whether it will be enforced across heath sector [50].

Secure remote working environment. Existing solutions include the use of the multifactor authentication and the monitoring of the log activity of user accounts and revoking account access if no longer needed [10]. Deebak, et al. proposed a chaotic-map based authenticated security framework for remote point-of-care [51]. Health organisations such as those in the UK have started using services to monitor their remote access infrastructure constantly and to investigate anomalies. For example, NHS has employed attack surface reduction rules (e.g. block macros, executable

content, process creation) [52]. Furthermore, a more recent NHS Digital service, Secure Boundary has been introduced as a perimeter security solution to enable secure access for NHS staff and to provide security monitoring [53].

Raise security awareness. Healthcare organisations already have cyber security programs in place to increase levels of security awareness [45, 54]. Existing solutions include the use of cyber security training programs and cyber security awareness campaign [55]. In a cyber security campaign, the IT department sends out fake phishing emails to their staff and provide further training to those who failed to identify the phishing emails [55]. In the UK, more than 100 NHS boards have completed GCHQ-accredited cybersecurity training since WannaCry attack. Furthermore, the NCSC's Board Toolkit for the NHS provides additional information on ransomware and backups. NHS Digital has also run a cyber awareness campaign named the Keep I.T. Confidential campaign. Over 340 organisations have downloaded the materials since its launch in September 2019 [56]. However, there is not enough work on COVID19 themed training programs such as COVID19 themed social engineering, although the community have already realised the importance of raising the awareness of COVID19 related cyber-attacks [57]. Existing research show that positive organisational climate can influence people's behaviour [58].

Ensure business continuity. Healthcare leadership must embrace cybersecurity and develop strong cultures of cyber-vigilance [59]. Health sector already has business continuity solutions in place such as data backups, intrusion detection and prevention systems [60] . NHS Trusts have been asked to follow and meet the Cyber Essentials and government standard. NHS Digital has launched a Data Security and Protection Toolkit (DSPT) [61], which is a self-assessment tool for organisations that need to access the NHS patient information and systems. DSPT must be applied to ensure that organisations practise good cyber hygiene. Security risk assessment is essential to ensure business continuity. Kim, et al. systematically assessed the impacts of cybersecurity threats on remote

healthcare [22]. Cyber security insurance in healthcare [62] should also be considered as a solution to ensure business continuity management, but has not widely adopted.

Apply technical controls. General technical controls applied by the health sector include encryption, authentication and authorisation to protect the data from cyber threats [63]. Cryptographic security was used to address data sharing and storage of patient information across network systems [64]. Homomorphic encryption (HE) was applied to ensure robust security and privacy guarantees while enabling analysis of encrypted data and sensitive medical information [65]. Blockchain is also applied to facilitate healthcare interoperability due to its immutability, transparency, and decentralisation [66]. Network segmentation and isolation also need to be considered by the health sector [7]. With network segmentation, network traffic can be isolated and/or filtered to limit and/or prevent access between network zones. For example, in case of systems compromise, one should freeze any activity in the system, disconnect the infected machines from any external drive or medical device and go offline from the network.

Policy and Legislation. The health sector already has security policies and legislation in place for cybersecurity management. Laws and regulations are available to protect the Medical Cyber-Physical Systems (MCPS) [65]. The security controls are required to be tailored according to the regulation [67]. Manufacturers are also required to take into account the regulations to design medical devices [68]. However, policymakers may need to alter the policies to allow new technological innovations to be applied to healthcare [69]. The US Congress passed the 21st Century Cures Act to promote the interoperability of electronic health records and promote more patients' control over their own health information while protecting privacy and cybersecurity [20]. However, more efforts are needed on security polices or legislations in handling cyber security related matters during pandemics like COVID19.

Incident reporting and CTI support. The health sector is required to report cyber security incidents to the supervisory authority, such as the national CSIRT in EU. In the UK, there is government-approved support from the National Cybersecurity Centre (NCSC). NHS Digital has issued two high-severity CareCERT alerts in 2019 (BlueKeep and DejaBlue). After developing a High Severity Alert (HSA) Process Handbook, remediation went from 18 weeks for BlueKeep down to three weeks for DejaBlue [68]. He and Johnson proposed the generic security template which is an evidenced based argumentation approach to facilitate incident reporting and exchange [70, 71]. This approach was applied in a healthcare organisation but have not been widely adopted. Hakak, et al. identified the needs of establishing an international workforce to facilitate threat reporting and cyber threat intelligence (e.g., attack vectors and countermeasures) exchange to combat pandemic-themed cyber threats [7]. Health sector will benefit from such practices during the pandemics in order to avoid similar incidents.

Cybersecurity guidance specific to COVID19. Some healthcare organisations have started providing security guidance specific to COVID19 for their staff. For example, NHS Digital has added guidance on working from home security, ramping up its on-site support for trusts on risk mitigations, data backup, and threat response. They also offer NHS the NCSC's Protective DNS for free [72]. Furthermore, governments also provide cyber security guidance to both individuals and organisations. For example, the UK's Information Commissioner's Office (ICO) created an information hub in order to assist individuals and organisations to protect data during the COVID-19 pandemic [73].

Table 4. Crucial Health Sector Security Solutions

Key Solutions	**Security Solutions**	**Author**
Apply endpoint device management tools	Apply perimeter-based defence (antivirus, firewalls) for protection against the cyber-attacks.	Reagin and Gentry [26]
	Restrict the technologies and devices used by health staff to remain compliant with security regulations such as HIPAA during the pandemics	Hoffman [20]
	Adapt the NIST approach to manage the security IoT medical devices	Kelly, Campbell [50]
Secure remote working environment	Apply multi-factor authentication	Argaw, Troncoso-Pastoriza [10]
	Appy a chaotic-map based authenticated security framework for remote point-of-care	Deebak, Al-Turjman [51]
	Apply remote access monitoring such as the NHS attack surface reduction rules	Zorz [52]
	Apply perimeter security solution such as NHS Secure Boundary to enable secure access	NHS Digital [53]
	Healthcare needs to ensure data protection mechanisms for securing system access and transmitting data.	Rezaeibagha, Win [60]
Raise security awareness.	Apply a holistic, integrated approach to improve staff awareness, competence, and mitigation of threats.	Pullin [45] Sedlack [54]
	Apply cyber security training programs and cyber security awareness campaign.	Gordon, Wright [55]
	Apply the NCSC's Board Toolkit to raise Board level security awareness.	NHS Digital [56]
	Provide comprehensive employee training and education to enable the identification and assessment of risks.	Alzahrani [57]
	Apply positive organisational climate to influence people's behaviour.	Kessler, Pindek [58]
Ensure business continuity	Apply a self-assessment tool such as the NHS Data Security and Protection Toolkit	NHS Digital [61]
	Embrace cybersecurity and develop strong cultures of cyber-vigilance.	Dameff, Selzer [59]
	Ensure business continuity through data backups, intrusion detection and prevention systems	Rezaeibagha, Win [60]
	Apply a systematic risk assessment of the impacts on healthcare business operations	Kim, Choi [22]
	Consider cyber security insurance in healthcare	Kabir, Ezekekwu [62]
Apply technical controls	Apply network segmentation to isolate the network traffic.	Hakak, Khan [7]
	Apply general technical controls including encryption, authentication and authorisation	Yaseen, Saleem [63]
	Ally Homomorphic encryption (HE) that ensures strong security and privacy guarantees	Raisaro, McLaren [65]

	while enabling analysis of encrypted data and sensitive medical information.	
	Apply Blockchain to facilitate healthcare interoperability.	Narikimilli, Kumar [66]
	Apply cryptographic security to address data sharing and storage of patient information across network systems.	Pussewalage and Oleshchuk [64]
Policies and legislations	Laws and regulations can help in combatting the issues of Medical Cyber-Physical Systems (MCPS)	Raisaro, McLaren [65]
	Security instructions and control designs should be tailored.	Wang and Jones [67]
	Regulatory changes or manufacturers should become more security-minded in the medical device design phase	DHSC [68].
	Policymakers may need to alter the policies to allow new technological innovations to be applied to healthcare	Bhuyan, Kabir [69].
	The US Congress passed the 21st Century Cures Act to promote patient control over their own health information while protecting privacy and cybersecurity	Hoffman [20]
Incident reporting and CTI support	NHS Digital issued Two high-severity CareCERT alerts BlueKeep and DejaBlue) and developed a High Severity Alert (HSA) Process Handbook to facilitate incident reporting and sharing	DHSC [68]
	Apply an evidence-based approach, such as the generic security template for incident reporting and exchange.	He and Johnson [70], He and Johnson [71]
	Establish an international workforce to facilitate cyber threat reporting and exchange to combat pandemic-themed cyber threats	Hakak, Khan [7]
Cybersecurity guidance specific to COVID19	NHS has added guidance around working from home securely specific to COVID19.	NHS Digital [72]
	The UK’s Information Commissioner's Office (ICO) created an information hub to assist individuals and organisations to manage data protection during the COVID-19 pandemic	ICO [73]

Discussion

This section summarises the main findings from the review, identifies the key areas of future research and discusses the limitation of the research.

Summary of Evidence

Through a scoping review, this research identifies the key cyber security challenges, cyber security solutions adopted by the health sector and the areas to be improved in order to counteract the cyber-attacks introduced through changes to working practices dealing with the current COVID19 pandemic. This review identified 9 main challenges in cyber security, 11 key solutions that the healthcare organisations adopted to address these challenges. Based on our findings and analysis, we can conclude that the main challenges that the health sector faces due to the COVID19 pandemic include increased reliance on remote working by staff, high demand for PPE by staff at the first line of defence and also decreased mobility due to the lockdown. Indeed, these changes have made the health sector vulnerable to potential cyber-attack. For example, the reliance on remote working was done by users with little previous experience, and there was also no planning, and cybersecurity associated assurance, prior to the shift. Furthermore, evidence can be seen from the security incidents that took place during the lockdown period such as those of the Brno University Hospital, Romanian hospital, etc. The health sector continues to face security challenges [7, 17]. Challenges such as remote working security assurance, endpoint device management, inadequate business continuity plans, lack of security awareness and so on are apparent in the health sector. There are some existing solutions in healthcare organisations, especially in the UK, such as remote access monitoring. Figure 2 summaries the main finding from the literature review and highlights the gaps/vulnerabilities that were exploited during the cyber-attacks that took place at the time of the COVID-19 pandemic.

However, there are still challenges and gaps to be addressed, as discussed below.

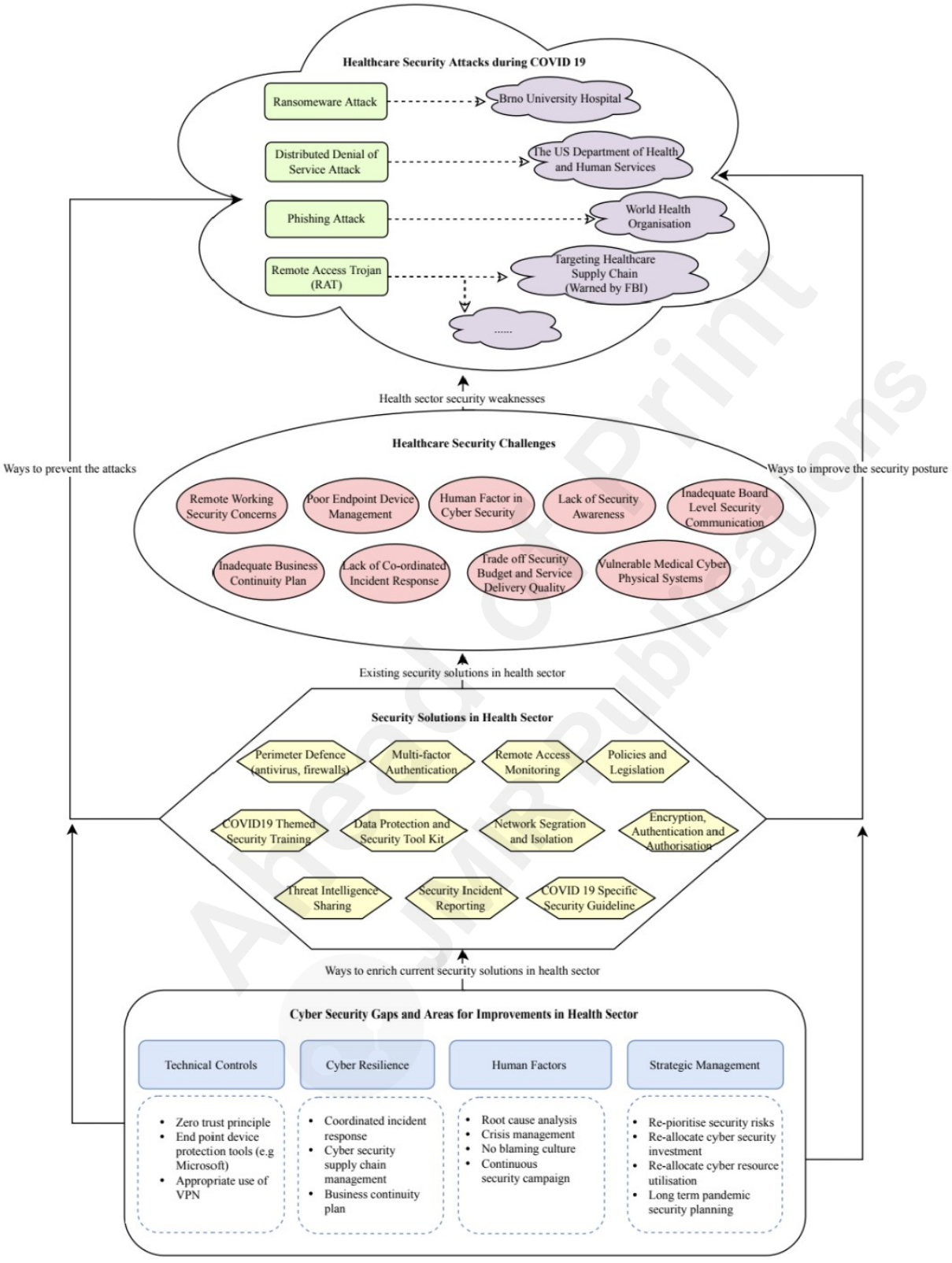


Figure 2. Security Attacks, Key Security Challenges, Solutions and Areas to Improve

Implications for future research

Although the health sector has made some efforts to address these challenges, more research efforts are still required in some domains.

Technical Controls. The health sector has applied some technical solutions to tackle the cybersecurity challenges in order to secure the remote working environment and monitor endpoint applications. These include but are not limited to network security (e.g. network segmentation), multifactor authentication, password protection, and patching systems and the use of intrusion detection and prevention systems. There are also innovative security solutions such as zero-trust principle (i.e., to treat all devices as untrusty devices before access or authorisation can be considered). The use of the VPN is a popular technique in remote working environment but is not always required. Healthcare organisations should avoid the abuse of VPN and make sure it is applied to specific tasks, such as for system admin use purpose and for medical diagnosis purpose through accessing the legacy systems (e.g., patient records management systems) stored on private data servers. Future research should explore innovative solutions such as Blockchain as it can facilitate healthcare interoperability due to its immutability, transparency, and decentralisation. In general, the health sector significantly lags behind other sectors for cyber security. Future research should borrow experience from general cyber security practices (e.g. NIST guidelines) and adapt it to fit into the needs of health sector, especially under the pandemics situation.

Cyber Resilience. In order to improve system resilience, the health organisations have some business continuity planning in place for data protection and recovery but lack a systematic way to maintain cyber resilience [18]. The vulnerabilities in the cyber supply chain makes it difficult to recover from an incident caused by third parties [39-42]. In the case of impact on medical devices or clinical information systems, incident response should be coordinated with the device manufacturers and the vendors. Healthcare organisations have realised the importance to have a comprehensive view of cyber security management in order to prevent cyber-attacks [18] but have not built this coordinated

capacity. There is a lack of a cyber resilience program to evaluate vendor's capabilities around threat protection, particularly across email servers (phishing and ransomware), breadth of portfolio coverage in addressing cloud and endpoint security. Future research should focus on building a coordinated cyber security capacity in order to systematically assess vulnerabilities and respond to cyber threats.

Human Factors in Cyber Security. People are likely to make mistakes, especially in the circumstance of changing their traditional way of working. The health care organisations are required to adopt a non-blaming culture in reporting incidents. The health sector should focus on root cause analysis [28] and prevents the incidents from happening especially through unintentional human error. Published research has presented that the majority of information security incidents relate to human error [28, 29] which is a vulnerability that attackers will look to exploit. A human error analytical approach such as IS-CHEC could be deployed both reactively, through incorporation within incident management practices [29, 30], and proactively, through simple interaction with operational personnel [29], to detect current human error areas of weaknesses and apply associated remedial and preventative measures. Moreover, the healthcare staff in the organisation need to be educated, build awareness of the ongoing situation during the COVID19 pandemic. For example, in the case of infection, the staff are required to disconnect from the network to contain the spread. The organisations should continuously raise awareness internally by launching campaigns even during the time of crisis (i.e. to inform health staff not to open suspicious emails). Future research should focus on creating pandemics-themed security awareness campaigns. Moreover, a positive and empowering culture is also required, e.g. by sharing the rate on people not clicking on the phishing negative emails during the training campaign. Experience can be borrowed from the organizational climate literature to positively influence people's behaviour [58].

Strategic Cyber Security Management. Although the healthcare organisations have invested in

cybersecurity to counteraction security attacks, further efforts are needed to reprioritise the cyber security risk assessment during the COVID19 pandemic and reallocate the security investment and optimise resource utilisation to obtain adequate assurances. According to Argwa, et al, healthcare organisations are advised to allocate more resources and funding to cyber security [46]. Strategic cyber security investment is still an immature research area in healthcare largely due to the board inability to fully understand and anticipate the direct and indirect impact on their health services. There are language barriers between the technical team and the board [27]. Another reason is that the board find it difficult to estimate the costs of investing and balancing these against potential benefits procured or impacts mitigated [6] as the cyber security investments prevent potential losses but may not generate business benefits directly. Moreover, organisations should not only create specific security guidelines for COVID19 pandemic, but also plan for the long way for remote working and spend efforts on strengthening their security mechanisms and cyber security crisis management capabilities. More research efforts are needed to support the top management of health sector to understand the threat-landscape and make better-informed decisions by allocating resources not just to providing services to staff and patients but also for the protection and resilience, in order to continuously serve even in times of emergency such as the current pandemic and beyond.

Limitations

As is different from systematic reviews, scoping reviews are used to identify knowledge gaps, scope a body of literature, clarify concepts. However, scoping reviews has limitations. It usually provides descriptive information in order to address the objectives of the review, which often leads to less defined searches. This review mitigated the risk by clearly define the search terms and search formula. Scoping reviews are also at risk for bias from different sources. All four authors are involved in the article identification, selection and analysis processes in order to reduce the risks of bias. Because of variability in such conduct of scoping review, there is a need for methodological standardization to ensure the strength of evidence. This review followed the PRISMA-ScR to

standardize the process and improve the strength of evidence. Another limitation is that this review included the exact terms used for searching in the titles or abstracts of existing publications. Any articles that used different terms, e.g, “computer security” would not have been included. In addition, the exclusion criteria exclude the publications that was not written in the English. Moreover, although this scoping review focused on healthcare, the solutions identified could be applied to other industries.

Conclusions

The COVID19 pandemic has challenged the resilience of the healthcare information system (HIS). This research is motivated by the urgency of counteracting the cyber-attacks that have recently happened to the hospitals, pharmaceutical companies, the US Department of Health and Human Services, the World Health Organization (WHO) and its partners, etc. We performed a review of the topic of health sector security challenges and solutions during COVID19. We identified the root causes of the security incidents that has impacted the health sector during the COVID19 pandemic, the cybersecurity challenges, solutions as well as the areas that require further efforts in the community. The results show that the main root causes of the security incidents that happened during the COVID19 pandemic are mainly from phishing, ransomware, distributed denial of service attack and malware. The main challenges facing the healthcare organisations are the inadequate endpoint device management, lack of security awareness, insecure remote working environment, inadequate business continuity plans, lack of coordinated incident response, difficulty in trading off security investment and service delivery quality. Needless to say, another major challenge is human error, both from the perspective of the healthcare worker at the frontline and those working from home. As the COVID-19 pandemic has shifted our priorities, there is a tendency for human error when staff are busy focusing on saving lives, working in a strange or different environment and also working in

different ways using new/different technologies. Coupled with little or no experience and the lack of prior planning and training to work under such situations, the healthcare workers requires more than training and support, such as adequate time, documented procedures and guidance on revised procedures and technology.

Although the health sector has made some efforts to address these challenges by applying technical measures, raising security awareness, enforcing policies, and developing COVID19 specific guidelines, however, more research efforts are still required in some domains. Future research should focus on: exploring enhanced technical controls through exploring the adaption of general cyber security practices (e.g. NIST guidelines); improving cyber resilience through building a coordinated cyber security capacity to systematically assess vulnerabilities of the complex healthcare supply chain and respond to cyber threats; reducing human related security incidents through exploring human error reduction approaches and pandemics- themed awareness campaigns; and enhancing strategic cyber security management though exploring crisis management planning, security risks reprioritisation, and the optimisation of cyber security budget and resource reallocation.

Many healthcare organisations are applying a temporary solution to counteract cyber threats during the COVID19 pandemic. The organisations should plan for the long-term, provide adequate levels of cybersecurity resource to deal with fast-changing situations and provide the required assurance within these changes. For example, remote working being an integral element of its services and strengthen their security mechanisms and cybersecurity crisis management capabilities. This paper provides useful insights for the health sector to address their cybersecurity issues during the COVID19 pandemic or under other epidemics or pandemics situation in the future. Moreover, cybersecurity experience in other sectors can be borrowed and applied in the health sector.

Funding

This work was supported by the National Natural Science Foundation of China (Grant No. 61803318).

Conflicts of Interest

None declared.

References

1. Porter, S., *Cyberattack on czech hospital forces tech shutdown during coronavirus outbreak.* https://www.healthcareitnews.com/news/europe/cyberattack-czech-hospital-forces-tech-shutdown-during-coronavirus-outbreak.
2. Jacobs, S.S.a.J., *Cyber-attack hits U.S. health agency amid covid-19 outbreak.* https://www.bloomberg.com/news/articles/2020-03-16/u-s-health-agency-suffers-cyber-attack-during-covid-19-response.
3. *Beware of criminals pretending to be WHO* https://www.who.int/about/communications/cyber-security
4. Bing., J.S.a.C., *Exclusive: Iran-linked hackers recently targeted coronavirus drugmaker gilead - sources* https://www.reuters.com/article/us-healthcare-coronavirus-gilead-iran-ex/exclusive-iran-linked-hackers-recently-targeted-coronavirus-drugmaker-gilead-sources-idUSKBN22K2EV.
5. Cimpanu., C., *Hackers preparing to launch ransomware attacks against hospitals arrested in romania.* https://www.zdnet.com/article/hackers-preparing-to-launch-ransomware-attacks-against-hospitals-arrested-in-romania/.
6. *Cybercriminals targeting critical healthcare institutions with ransomware* https://www.interpol.int/en/News-and-Events/News/2020/Cybercriminals-targeting-critical-healthcare-institutions-with-ransomware.
7. Hakak, S., et al., *Have you been a victim of COVID-19-related cyber incidents? Survey, taxonomy, and mitigation strategies.* IEEE Access, 2020. **8**: p. 124134-124144.
8. Williams, C.M., R. Chaturvedi, and K. Chakravarthy, *Cybersecurity Risks in a Pandemic.* J Med Internet Res, 2020. **22**(9): p. e23692.
9. Boddy, A., et al. *A study into data analysis and visualisation to increase the cyber-resilience of healthcare infrastructures*. in *Proceedings of the 1st International Conference on Internet of Things and Machine Learning*. 2017.
10. Argaw, S.T., et al., *Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks.* BMC Medical Informatics and Decision Making, 2020. **20**(1): p. 1-10.
11. Jalali, M.S., et al., *EARS to cyber incidents in health care.* J Am Med Inform Assoc, 2019. **26**(1): p. 81-90.
12. Coventry, L. and D. Branley, *Cybersecurity in healthcare: A narrative review of trends, threats and ways forward.* Maturitas, 2018. **113**: p. 48-52.
13. Kruse, C.S., et al., *Cybersecurity in healthcare: A systematic review of modern threats and trends.* Technol Health Care, 2017. **25**(1): p. 1-10.
14. Offner, K.L., et al., *Towards understanding cybersecurity capability in Australian healthcare organisations: a systematic review of recent trends, threats and mitigation.* Intelligence and National Security, 2020. **35**(4): p. 556-585.
15. Sardi, A., et al., *Cyber risk in health facilities: A systematic literature review.* Sustainability (Switzerland), 2020. **12**(17).
16. Moher, D., et al., *Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement.* Int J Surg, 2010. **8**(5): p. 336-41.
17. Schneck, P.A., *Cybersecurity during COVID-19.* IEEE Security and Privacy, 2020. **18**(6): p. 4-5.
18. Weil, T. and S. Murugesan, *IT Risk and Resilience-Cybersecurity Response to COVID-19.* IT Professional, 2020. **22**(3): p. 4-10.
19. Jalali, M.S., et al., *Why employees (still) click on phishing links: investigation in hospitals.* Journal of Medical Internet Research, 2020. **22**(1): p. e16775.

20. Hoffman, D.A., *Increasing access to care: telehealth during COVID-19.* J Law Biosci, 2020. **7**(1): p. lsaa043.
21. Ronquillo, J.G., et al., *Health IT, hacking, and cybersecurity: national trends in data breaches of protected health information.* JAMIA Open, 2018. **1**(1): p. 15-19.
22. Kim, D.W., J.Y. Choi, and K.H. Han, *Risk management-based security evaluation model for telemedicine systems.* BMC Med Inform Decis Mak, 2020. **20**(1): p. 106.
23. *Cyber warning issued for key healthcare organisations in UK and USA ,"* https://www.ncsc.gov.uk/news/warning-issued-uk-usa-healthcare-organisations.
24. Cimpanu, C., *FBI re-sends alert about supply chain attacks for the third time in three months*. https://www.zdnet.com/article/fbi-re-sends-alert-about-supply-chain-attacks-for-the-third-time-in-three-months/
25. Naidoo, R., *A multi-level influence model of COVID-19 themed cybercrime.* European Journal of Information Systems, 2020. **29**(3): p. 306-321.
26. Reagin, M.J. and M.V. Gentry, *Enterprise cybersecurity: Building a successful defense program.* Frontiers of health services management, 2018. **35**(1): p. 13-22.
27. Jalali, M.S. and J.P. Kaiser, *Cybersecurity in Hospitals: A Systematic, Organizational Perspective.* J Med Internet Res, 2018. **20**(5): p. e10059.
28. Evans, M., et al., *HEART-IS: A novel technique for evaluating human error-related information security incidents.* Computers & Security, 2019. **80**: p. 74-89.
29. Evans, M., et al., *Evaluating information security core human error causes (IS-CHEC) technique in public sector and comparison with the private sector.* International journal of medical informatics, 2019. **127**: p. 109-119.
30. Evans, M., et al., *Real-time information security incident management: a case study using the IS-CHEC technique.* IEEE Access, 2019. **7**: p. 142147-142175.
31. Gordon, W.J., A. Fairhall, and A. Landman, *Threats to Information Security-Public Health Implications.* The New England journal of medicine, 2017. **377**(8): p. 707.
32. Furnell, S. and J.N. Shah, *Home working and cyber security–an outbreak of unpreparedness?* Computer Fraud & Security, 2020. **2020**(8): p. 6-12.
33. Coventry, L., et al., *Cyber-risk in healthcare: Exploring facilitators and barriers to secure behaviour*, in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. 2020. p. 105-122.
34. Kaplan, B., *REVISITING HEALTH INFORMATION TECHNOLOGY ETHICAL, LEGAL, and SOCIAL ISSUES and EVALUATION: TELEHEALTH/TELEMEDICINE and COVID-19.* International Journal of Medical Informatics, 2020. **143**.
35. Tully, J., et al., *Healthcare Challenges in the Era of Cybersecurity.* Health Secur, 2020. **18**(3): p. 228-231.
36. Barad, M., *Linking Cyber Security Improvement Actions in Healthcare Systems to Their Strategic Improvement Needs.* Procedia Manufacturing, 2019. **39**: p. 279-286.
37. Jones, R.W. and K. Katzis. *Cybersecurity and the Medical Device Product Development Lifecycle*. in *ICIMTH*. 2017.
38. Walker-Roberts, S., M. Hammoudeh, and A. Dehghantanha, *A systematic review of the availability and efficacy of countermeasures to internal threats in healthcare critical infrastructure.* IEEE Access, 2018. **6**: p. 25167-25177.
39. Frontoni, E., et al., *Sharing health data among general practitioners: The Nu.Sa. project.* International Journal of Medical Informatics, 2019. **129**: p. 267-274.
40. Bhatia, S. and A. Ibrahim, *Understanding Security Risks When Exchanging Medical Records Using IHE*, in *Advances in Intelligent Systems and Computing*. 2020. p. 477-481.
41. Natsiavas, P., et al., *Comprehensive user requirements engineering methodology for secure and interoperable health data exchange.* BMC Med Inform Decis Mak, 2018. **18**(1): p. 85.
42. Nalin, M., et al., *The European cross-border health data exchange roadmap: Case study in*

the Italian setting. Journal of Biomedical Informatics, 2019. **94**.
43. Akinsanya, O.O., M. Papadaki, and L. Sun. *Current cybersecurity maturity models: How effective in healthcare cloud?* in *CEUR Workshop Proceedings*. 2019.
44. Chen, Y., et al., *Blockchain-based medical records secure storage and medical service framework.* Journal of medical systems, 2019. **43**(1): p. 5.
45. Pullin, D.W., *Cybersecurity: positive changes through processes and team culture.* Frontiers of health services management, 2018. **35**(1): p. 3-12.
46. Argaw, S.T., et al., *The state of research on cyberattacks against hospitals and available best practice recommendations: a scoping review.* BMC Med Inform Decis Mak, 2019. **19**(1): p. 10.
47. Jimenez, J.I., H. Jahankhani, and S. Kendzierskyj, *Health Care in the Cyberspace: Medical Cyber-Physical System and Digital Twin Challenges*, in *Internet of Things*. 2020. p. 79-92.
48. Almohri, H., et al. *On threat modeling and mitigation of medical cyber-physical systems*. in *2017 IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE)*. 2017. IEEE.
49. Zheng, G., et al. *From WannaCry to WannaDie: Security trade-offs and design for implantable medical devices*. in *2017 17th International Symposium on Communications and Information Technologies (ISCIT)*. 2017. IEEE.
50. Kelly, J.T., et al., *The Internet of Things: Impact and Implications for Health Care Delivery.* J Med Internet Res, 2020. **22**(11): p. e20135.
51. Deebak, B.D., F. Al-Turjman, and A. Nayyar, *Chaotic-map based authenticated security framework with privacy preservation for remote point-of-care.* Multimed Tools Appl, 2020: p. 1-26.
52. Zorz, Z., *Vulnerable VPN appliances at healthcare organisations open doors for ransomware gangs*
53. *NHS secure boundary* https://digital.nhs.uk/cyber-and-data-security/managing-security/nhs-secure-boundary
54. Sedlack, D., *Understanding Cyber Security Perceptions Related to Information Risk in a Healthcare Setting.* 2016.
55. Gordon, W.J., et al., *Evaluation of a mandatory phishing training program for high-risk employees at a US healthcare system.* J Am Med Inform Assoc, 2019. **26**(6): p. 547-552.
56. *Cyber associates network.* https://digital.nhs.uk/cyber-and-data-security/about-us/cyber-associates-network
57. Alzahrani, A., *Coronavirus social engineering attacks: Issues and recommendations.* International Journal of Advanced Computer Science and Applications, 2020. **11**(5): p. 154-161.
58. Kessler, S.R., et al., *Information security climate and the assessment of information security risk among healthcare employees.* Health Informatics Journal, 2020. **26**(1): p. 461-473.
59. Dameff, C.J., et al., *Clinical cybersecurity training through novel high-fidelity simulations.* The Journal of emergency medicine, 2019. **56**(2): p. 233-238.
60. Rezaeibagha, F., K.T. Win, and W. Susilo, *A systematic literature review on security and privacy of electronic health record systems: technical perspectives.* Health Information Management Journal, 2015. **44**(3): p. 23-38.
61. *Data Security and Protection Toolkit.* https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/data-security-and-protection-toolkit.
62. Kabir, U.Y., et al., *Trends and best practices in health care cybersecurity insurance policy.* J Healthc Risk Manag, 2020. **40**(2): p. 10-14.
63. Yaseen, M., et al., *Secure sensors data acquisition and communication protection in eHealthcare: Review on the state of the art.* Telematics and Informatics, 2018. **35**(4): p. 702-

726.
64. Pussewalage, H.S.G. and V.A. Oleshchuk, *Privacy preserving mechanisms for enforcing security and privacy requirements in E-health solutions.* International Journal of Information Management, 2016. **36**(6): p. 1161-1173.
65. Raisaro, J.-L., et al., *Are privacy-enhancing technologies for genomic data ready for the clinic? A survey of medical experts of the Swiss HIV Cohort Study.* Journal of biomedical informatics, 2018. **79**: p. 1-6.
66. Narikimilli, N.R.S., et al., *Blockchain Applications in Healthcare – A Review and Future Perspective*, in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. 2020. p. 198-218.
67. Wang, L. and R. Jones. *Big Data, Cybersecurity, and Challenges in Healthcare*. in *Conference Proceedings - IEEE SOUTHEASTCON*. 2019.
68. *Securing cyber resilience in health and care*. https://www.gov.uk/government/publications/securing-cyber-resilience-in-health-and-care-progress-update-2019.
69. Bhuyan, S.S., et al., *Transforming Healthcare Cybersecurity from Reactive to Proactive: Current Status and Future Recommendations.* J Med Syst, 2020. **44**(5): p. 98.
70. He, Y. and C. Johnson, *Improving the redistribution of the security lessons in healthcare: An evaluation of the Generic Security Template.* International journal of medical informatics, 2015. **84**(11): p. 941-949.
71. He, Y. and C. Johnson, *Challenges of information security incident learning: an industrial case study in a Chinese healthcare organization.* Informatics for Health and Social Care, 2017. **42**(4): p. 393-408.
72. *COVID-19 cyber security support* https://digital.nhs.uk/cyber-and-data-security/covid-19-cyber-security-support.
73. *Data protection and coronavirus information hub* https://ico.org.uk/global/data-protection-and-coronavirus-information-hub/

Appendix: PRISMA-ScR CHECKLIST ITEM

SECTION	ITEM	PRISMA-ScR CHECKLIST ITEM	REPORTED ON PAGE
TITLE			
Title	1	Healthcare Cyber Security Challenges and Solutions Under the Climate of COVID19: A Scoping Review	1
ABSTRACT			

Structured summary	2	Abstract provided a structured summary that includes background, objectives, methods, results, and conclusions that relate to the review questions and objectives.	2-3
INTRODUCTION			
Rationale	3	The COVID19 pandemic has created a new reality for the health sector. The sector has become a primary target of adapted cybersecurity attacks. There are some research efforts reviewing the literature in cyber security in health sector. However, there are limited research efforts on an in-depth review and analysis of the key cyber security challenges and solutions in health sector specifically under the pandemic situation such as COVID19.	4-5
Objectives	4	This paper aims to identify the most prominent and significant methods of attack and threats that have affected the health sector during the COVID19 pandemic, the cybersecurity challenges, solutions as well as the areas that require further efforts in the community.	5-6
METHODS			
Protocol and registration	5	This research follows the PRISMA-ScR protocol. The aim of this review is to identify health sector cyber-attacks, security challenges and solutions. Before undertaking this review, a protocol was created detailing the information sources, searching strategies, eligibility criteria, selection of sources of evidence and data charting processes.	6
Eligibility criteria	6	Articles in English in the last decade were included, i.e., 2011-2020. Reports, news articles, or websites were also included only when they are related directly to previously published work, or they were the only currently available information source at the moment of manuscript preparation.	6-7
Information sources	7	PubMed and Scopus	6
Search	8	The search formular “(covid or healthcare) and cybersecurity” was used to search for the articles.	6
Selection of sources of evidence	9	The selection process was illustrated in Figure 1. The results of search were exported to the Endnote library. The title and abstract of each paper were analysed by two of the authors to assess whether it fell into the specified criteria. In cases in which this was not obvious, all four authors looked at the paper and, when necessary, read it to assess relevance.	7-8
Data charting process	10	The data was extracted and stored in a standardized Microsoft Excel form. This was an iterative process whereby the charting table is continually updated. Data charting was carried out both independently and in duplicate by at least two authors to ensure the quality of the extracted key findings from the literature, before being used for results analysis.	8
Data items	11	Key data items including title, abstract, authorship, aims, key findings related to the review objectives,	8

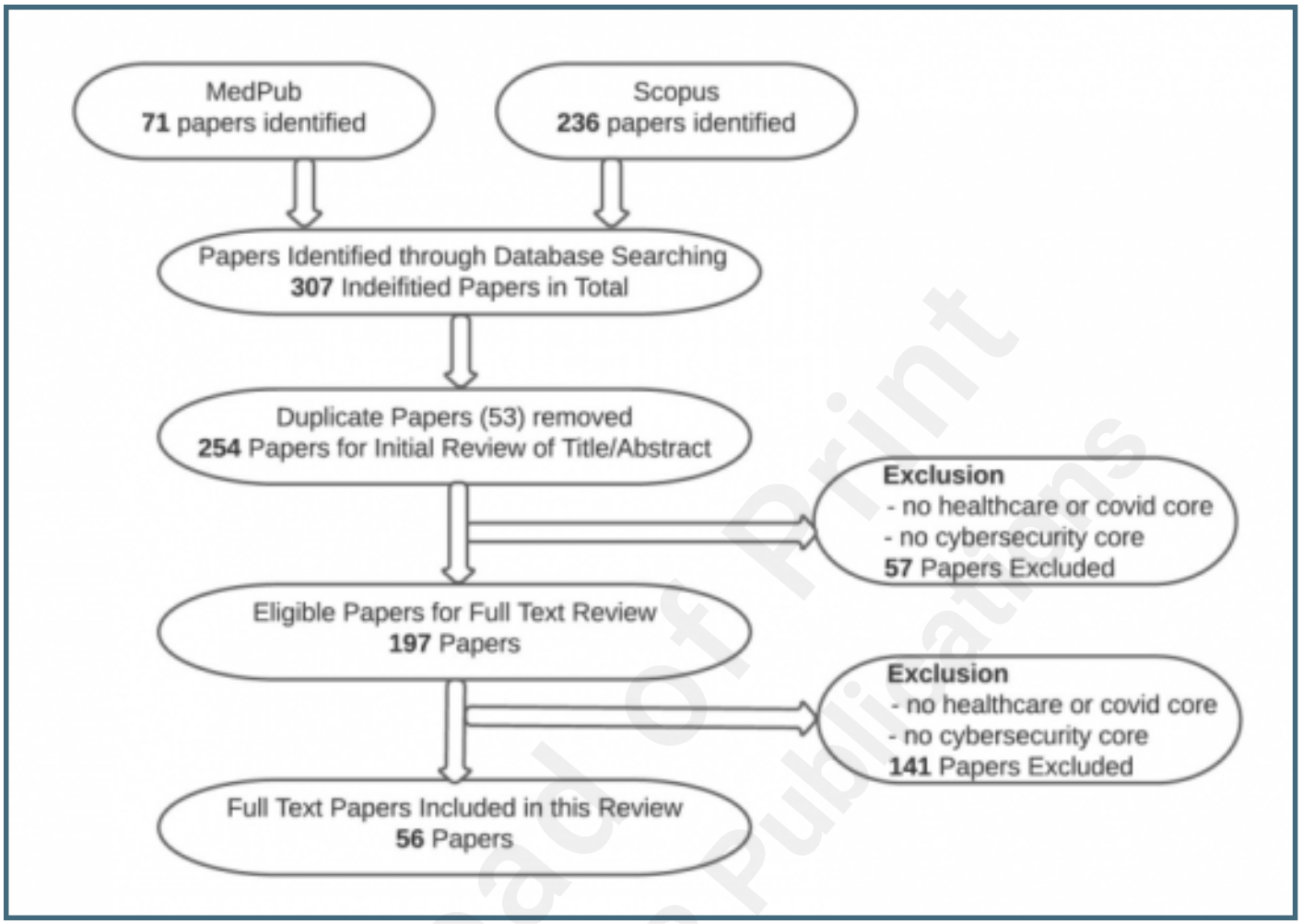
		evidence document, document type, year of publication, and the location.	
Critical appraisal within sources of evidence	12	Although JBI suggested that the critical appraisal is usually not needed for a scoping review, we had at least two authors checked the source of evidence, making sure that they are relevant, up to date and are from reputable sources. In cases in which this was not obvious, all four authors looked at the sources and assessed them.	9
Synthesis of results	13	Through aggregating the information from the selected literature, the results were analysed qualitatively (grouped into themes and presented in tables), reported in the Results section.	9
RESULTS			
Selection of sources of evidence	14	As illustrated in Figure 1. 307 identified papers in total were screened. There were 53 duplicates removed, 57 papers excluded due to the lack of “healthcare or covid” core or no “cybersecurity” core in the abstract. A further 197 papers were excluded due to the lack of “healthcare or covid” core or no “cybersecurity” core in the full text. 56 papers were finally included in the review.	9
Characteristics of sources of evidence	15	For each source of evidence, relevant data with citation was grouped into four major themes and was presented in Table 1-4.	10-27
Critical appraisal within sources of evidence	16	As discussed in the method section, the source of evidence was checked by at least two authors to make sure that they are relevant, up to date and are from reputable sources.	9
Results of individual sources of evidence	17	For each included source of evidence, relevant data that related to the review questions and objectives, was charted and grouped into four themes and was presented in Table 1-4.	10-27
Synthesis of results	18	The charting results related to the review questions and objectives were summarised and presented in themes and in tables.	10-27
DISCUSSION			
Summary of evidence	19	This section provided a summary of the key research results including cyber security challenges, cyber security solutions adopted by the health sector and the areas to be improved in order to counteract the cyber-attacks introduced through changes to working practices dealing with the current COVID19 pandemic, linking to the review questions and objectives.	28-29
Implications for future research		This section provided a summary of the key areas that requires more research efforts in the future, including technical controls, cyber resilience, human factors in cyber security, and strategic cyber security management.	30-32
Limitations	20	Scoping reviews are at risk for bias from different sources. This review followed the PRISMA-ScR to standardize the process and improve the strength of	32-33

		evidence. This review sincluded the exact terms used for searching in the titles or abstracts of existing publications. Any articles that used different terms would not have been included.	
Conclusions	21	This section provided a summary of the interpretation of the results with respect to the review questions and objectives as well as the research areas to be improved in the future.	33-35
FUNDING			
Funding	22	This work was supported by the National Natural Science Foundation of China (Grant No. 61803318).	35

Supplementary Files

Figures

Flowchart showing the article identification and selection process.



Security Attacks, Key Security Challenges, Solutions and Areas to Improve Strategic Cyber Security Management.