International Journal of Innovation

e-ISSN: 2318-9975
Received: 23 Sept. 2020 - **Approved:** 19 Nov. 2020
Evaluation Process: Double Blind Review
https://doi.org/10.5585/iji.v9i1.18246

Check for updates

RISK MANAGEMENT FOCUSING ON THE BEST PRACTICES OF DATA SECURITY SYSTEMS FOR HEALTHCARE

GESTÃO DE RISCOS COM FOCO NAS MELHORES PRÁTICAS DE SISTEMAS DE SEGURANÇA DE DADOS PARA SAÚDE

GESTIÓN DE RIESGOS ENFOCADA EN LAS MEJORES PRÁCTICAS DE LOS SISTEMAS DE SEGURIDAD DE DATOS PARA LA SALUD

Fabio Martins Dias[1]
Mauro Luiz Martens[2]
Sonia Francisca de Paula Monken[3]
Luciano Ferreira da Silva[4]
Ernesto Del Rosario Santibanez-Gonzalez[5]

Cite as – American Psychological Association (APA)

Dias, F. M., Martens, M. L., Monken, S. F. de P., Silva, L. F., & Santibanez-Gonzalez, E. D. R. (2021, Jan./Apr.). Risk management focusing on the best practices of data security systems for healthcare. *International Journal of Innovation - IJI*, São Paulo, *9*(1), 45-78. https://doi.org/10.5585/iji.v9i1.18246.

Abstract

Objective of the study: Statistics shows a worrisome picture of challenges to be overcome by cybersecurity in the healthcare sector. Data evidence that the healthcare industry experiences four data breaches per week in the United States alone, making it the sector most often affected by digital security breaches. Thus, the current article aims to investigate risk management focusing on identifying requirements and best practices for healthcare data security systems.

Methodology/approach: It is based on a systematic literature review. Studies on state-of-the-art data security systems were collected and interpreted through content analysis. Assertive keywords, source-selection criteria, interpretation of selected articles, and database analysis were used to form the investigated sample and to represent the broad applications of this study's objective.

Originality/Relevance: The current study contributes to define a set of minimum requirements and best practices that can be adopted to manage data security risks in the healthcare sector and medical devices.

Main results: Results have pointed out that there is no fully effective way to prevent all violations by cybercriminals; however, cybersecurity must be part of management processes adopted by different organizations.

Theoretical/methodological contributions: It is found that cybersecurity has a great importance for the healthcare sector, the information generated is rich in content and that cybersecurity is neglected in the sector, that is not able to deal with the reality of cyber threats in the industry 4.0 context.

[1]Mestre em Engenharia de Produção. Universidade Nove de Julho – UNINOVE. São Paulo – SP, Brasil. fabioberas30@gmail.com

[2]Doutor em Engenharia de Produção. Universidade de São Paulo – USP. São Paulo – SP, Brasil. mauro.martens@gmail.com

[3]Doutora em Gestão em Saúde. Universidade de São Paulo Faculdade – USP. São Paulo – SP, Brasil. sfmonken@hotmail.com

[4]Doutor em Administração de Empresas. Universidade Nove de Julho – UNINOVE. São Paulo – SP, Brasil. lf_silvabr@yahoo.com.br

[5]Universidade Federal Rio de Janeiro – COPPE/UFRJ. Rio de Janeiro – RJ, Brasil. santibanez.ernesto@gmail.com

Social /management contributions: By the good risk management practices and the adoption of minimum security items, institutions can ensure that managers can prepare and respond efficiently to cyber risks.

Keywords: Cybersecurity. Cyber-Physical System. Industry 4.0. Health Management. Risk Management.

Resumo

Objetivo do estudo: As estatísticas mostram um quadro preocupante de desafios a serem superados pela segurança cibernética no setor da saúde. Dados evidenciam que o setor de saúde enfrenta quatro violações de dados por semana apenas nos Estados Unidos da América- EUA, tornando-o o setor mais afetado por violações de segurança digital. Assim, o presente artigo tem como objetivo investigar a gestão de riscos com foco na identificação de requisitos e melhores práticas para sistemas de segurança de dados de saúde.

Metodologia / abordagem: É baseada em uma revisão sistemática da literatura. Estudos sobre sistemas de segurança de dados de última geração foram coletados e interpretados por meio de análise de conteúdo. Palavras-chave assertivas, critérios de seleção de fontes, interpretação dos artigos selecionados e análise de banco de dados foram usados para formar a amostra investigada e para representar as amplas aplicações do objetivo deste estudo.

Originalidade / Relevância: O presente estudo contribui para definir um conjunto de requisitos mínimos e melhores práticas que podem ser adotados para gerenciar os riscos à segurança de dados no setor de saúde e dispositivos médicos.

Principais resultados: Os resultados apontaram que não há uma maneira totalmente eficaz de prevenir todas as violações por cibercriminosos; no entanto, a cibersegurança deve fazer parte dos processos de gestão adotados por diferentes organizações.

Contribuições teórico-metodológicas: Constata-se que a cibersegurança tem grande importância para o setor saúde, a informação gerada é rica em conteúdo e que a cibersegurança é negligenciada no setor, que não é capaz de lidar com a realidade das ameaças cibernéticas na indústria 4.0 contexto.

Contribuições sociais / de gestão: Por meio das boas práticas de gestão de riscos e da adoção de itens mínimos de segurança, as instituições podem garantir que os gestores possam se preparar e responder de forma eficiente aos riscos cibernéticos.

Palabras-chave: Cibersegurança. Sistema Ciber-Físico. Indústria 4.0. Gestão de saúde. Gerenciamento de riscos.

Resumen

Objetivo del estudio: Las estadísticas muestran un panorama preocupante de los desafíos que debe superar la ciberseguridad en el sector de la salud. Los datos evidencian que la industria de la salud experimenta cuatro violaciones de datos por semana solo en los Estados Unidos, lo que lo convierte en el sector más afectado por las violaciones de seguridad digital. Por lo tanto, el artículo actual tiene como objetivo investigar la gestión de riesgos centrándose en la identificación de requisitos y mejores prácticas para los sistemas de seguridad de datos sanitarios.

Metodología / enfoque: Se basa en una revisión sistemática de la literatura. Se recopilaron e interpretaron estudios sobre sistemas de seguridad de datos de última generación mediante análisis de contenido. Se utilizaron palabras clave asertivas, criterios de selección de fuentes, interpretación de artículos seleccionados y análisis de bases de datos para formar la muestra investigada y representar las amplias aplicaciones del objetivo de este estudio.

Originalidad / Relevancia: El estudio actual contribuye a definir un conjunto de requisitos mínimos y mejores prácticas que se pueden adoptar para gestionar los riesgos de seguridad de los datos en el sector sanitario y los dispositivos médicos.

Resultados principales: Los resultados han señalado que no existe una forma totalmente eficaz de prevenir todas las violaciones por parte de los ciberdelincuentes; sin embargo, la ciberseguridad debe formar parte de los procesos de gestión adoptados por diferentes organizaciones.

Aportes teóricos / metodológicos: Se encuentra que la ciberseguridad tiene una gran importancia para el sector salud, la información generada es rica en contenido y que la ciberseguridad está desatendida en el sector, que no es capaz de enfrentar la realidad de las ciberamenazas en la industria. 4.0 contexto. Contribuciones sociales / de gestión: mediante las buenas prácticas de gestión de riesgos y la adopción de elementos de seguridad mínimos, las instituciones pueden garantizar que los administradores puedan prepararse y responder de manera eficiente a los riesgos cibernéticos.

Palabras-clave: La seguridad cibernética. Sistema ciberfísico. Industria 4.0. Manejo de la salud. Gestión de riesgos.

1 Introduction

This article contributes to the analysis of cybersecurity in the healthcare sector since this sector is one of the most vulnerable to cybercrime in the world. According to Kabir, Ezekekwu, Bhuyan, Mahmood and Dobalian (2020) “Healthcare organizations are a major target for cyberattacks” (p.1). Cybersecurity is an extremely arduous task, requiring a lot of effort, resources, and focus. Cybercrime emerged in the late 1970’s, when the information technology (IT) sector was still developing (Kruse, Frederick, Jacobson & Monticone, 2017). Cybersecurity is a comprehensive concept that involves, among other topics, best practices, policies, safeguards, training, guidelines, risk management, crisis management, and technologies that can be used to protect the end-user, the cyber environment, and the assets of an organization (Alexander, Haseeb & Baranchuk, 2019).

In addition, according to Ondiege, Clarke and Mapp (2017), cybersecurity is defined by the Food and Drug Administration (FDA) as a set of practices to prevent unauthorized access, modification, misuse or denial of use of information stored, accessed, or transferred from a doctor’s device to an unauthorized external recipient. Still according to the same authors, a cyber-attack can result not only in the compromise of the data but also in the compromise of vital life-saving devices; therefore, it is essential that the healthcare sector realizes that the responsibility for cybersecurity is not only of the medical device manufacturers. In 2016, cyber-attackers demanded approximately $3.6 million in Bitcoins to unlock the hospital’s computers of the Presbyterian Medical Center in Los Angeles, California (Abraham, Chatterjee & Sims, 2019).

The Covid-19 pandemic scenario has made the need to access accurate real-time health data evident. The action of health professionals depends on reliable data used to map diseases. The medical and hospital supply industry needs data to plan market segmentation. Government agencies need to limit contamination outbreaks based on epidemiological data. Research

institutes rely on health statistics and on their records to define strategies in the clinical analysis of vaccine trials (Okereafor & Marcelo, 2020).

Therefore, studies are necessary to increase awareness about the importance of cybersecurity, change the basic concepts and effectively build an organizational culture oriented to cybersecurity. (Natsiavas et al., 2018). The healthcare sector is an extremely attractive and vulnerable target for cybercriminals due to its economic size and inefficient cybersecurity (Blanke & McGrady, 2016). Thus, information is the new oil of Industry 4.0, with a vast amount of information generated that must be protected (Baaziz & Quoniam, 2013)

Burns et al. (2011) understand that the healthcare sector is structured by health system, which include the government; companies; individuals and groups of companies; financial intermediaries, which include health insurance companies, health maintenance organizations (HMOs), and pharmaceutical benefits administration; providers of health products and services, which include hospitals, doctors, integrated networks of health services, and pharmacies; buyers, which include health product distributors and purchasing organizations; as well as manufacturers, which include the pharmaceutical industry, manufacturers of health equipment, and manufacturers of medical and surgical products. In times of innovation, (Burns et al., 2011) consider valuable to also incorporate the information technology providers in connection with manufacturers. Burns et al. (2011) justifies this addition considering the size of the information technology market in healthcare, its relevance to healthcare organizations and patients, as well as the fact that these providers are one of the sources of innovation in the value chain.

Previously, the healthcare industry was believed to be immune to cyber-attacks, and protective measures had not been considered over the years. In recent decades, the industry has concentrated its efforts in medical care, scrapping its devices to protect against cyber-attacks. It is believed that 90% of organizations in the sector have already been victims of cybersecurity violations in recent years, presenting several factors that contributed to the sector becoming one of the main targets of cyber-attacks (Coronado & Wong, 2014; Kruse et al., 2017).

It is a huge challenge for every organization in the 21st century to protect against cybercrime. Just as any innovation is a great challenge for organizations (Silva F., Braga, & Reboucas, 2016). Although there is no foolproof solution, the literature shows that effective risk management is the most appropriate solution to combat the growing action of cybercriminals (Coronado & Wong, 2014). According to Dionnne (2013), the ISO/IEC 27000 (2013) - Information technology, shows security techniques and information security management systems. In addition, in ISO 31000 (2018), risk management is defined as

"coordinated activities to direct and control an organization with regard to risk". Therefore, in this paper cybersecurity risk management refers to coordinated activities to direct and control an organization with regard to risk derived from cyber-attacks or cybersecurity breaches?. Various authors note that a possible cyber-attack is imminent; however, only 22% of healthcare organizations and 41% of medical equipment manufacturers have a cybersecurity risk management plan (Blanke & McGrady, 2016; Busdicker & Upendra, 2017), which represents a large gap in scientific and technological research.

Abraham et al. (2019), Natsiavas et al. (2018), PMI (2017) and Ward and Chapman (2008) conclude that it is important to have a comprehensive risk management method that covers all stages of the risk management process, from risk identification to a possible response to that risk. Other approaches found in the literature emphasize the assessment and vulnerability of the identification of threats. However, there is a lack of emphasis on sequencing actions after risk identification. Likewise, the authors point to the need to create a risk management plan for healthcare data security (Abraham et al., 2019; Gordon, Stern, Landman & Kramer, 2019; Kure, Islam & Razzaque, 2018).

According to an analysis of the academic literature, the Table 1 shows the five gaps found:

Table 1 – Five gaps found in the academic literature (continued)

Authors	Cybersecurity is an extremely important topic In the healthcare sector	Cybersecurity in the healthcare sector is neglected	There are no significant investments in the healthcare sector	The information generated by the healthcare sector is rich in content	There is a lack of actions protection of data in the healthcare sector
Abraham et al. (2019)	*X*	*X*	*X*	*X*	*X*
Ahmed and Ahmed (2019)		*X*		*X*	
Alexander et al. (2019)	*X*	*X*	*X*	*X*	*X*
Al-Muhtadi et al. (2019)	*X*			*X*	*X*
Askar (2019)	*X*	*X*			
Berger and Schneck (2019)	*X*	*X*	*X*	*X*	*X*
Bilek, Muscionico and Amiel (2017)	*X*	*X*			*X*
Bissonnette and Bergeron (2017)	*X*	*X*	*X*		
Blanke and McGrady (2016)	*X*	*X*	*X*	*X*	*X*
Bojanova and Voas (2017)			*X*		*X*
Braga, Dahab, Antunes, Laranjeiro and Vieira (2019)				*X*	

Brody, Chang and Schoenberg (2018)	X				
Busdicker and Upendra (2017)	X	X			X
Coveney, Dougherty and Highfield (2016)	X				
Coventry and Branley (2018)	X	X	X	X	
Cleland-Huang (2014)		X		X	
Dandage, Mantha and Rane (2018)				X	
Diggans and Leproust (2019)					X
Elizabeth, Jobin and Dona (2019)		X			X
Frontoni, et al. (2019)			X	X	X
Ghafir, et al. (2018)	X	X	X	X	X
Gordon et al. (2019)	X	X	X	X	X
Habibzadeh et al. (2019)			X	X	
Abdelhamid, Kisekka and Samonas (2018)				X	
Coronado and Wong (2014)	X	X	X	X	X
Goncharov, Kruglov and Dashchenko (2019)	X				X
Good, et al. (2005)			X	X	
Grimes and Wirth (2017)		X		X	X
Handler (2018)					X
Jalali et al. (2019)	X		X	X	
Kessler, Pindek, Kleinman, Andel and Spector (2019)		X			
Kharraz, Robertson and Kirda (2018)	X	X	X	X	X
King, et al. (2018)					X
Koppel and Kuziemsky (2019)	X			X	
Kruse et al. (2017)	X	X	X	X	X
Kure et al. (2018)	X	X	X	X	X
Lebeda, Zalatoris and Scheerer (2018)			X	X	
Lechler and Wetzel (2017)				X	X
Leung, Clark, Sakal, Friesen and Strudwick (2019)		X	X		
Loi, Christen, Kleine and Weber (2019)				X	
Maimó, et al. (2019)	X	X	X	X	X
Martin et al. (2017)	X	X	X	X	X
Natsiavas, et al. (2018)	X	X	X	X	X
Ondiege et al. (2017)	X	X	X	X	X
Pesapane , Volonté, Codari and Sardanelli (2018)	X		X	X	X
Priestman, Anstis, Sebire, Sridharan and Sebire (2019)	X		X		
Primo, et al. (2018)	X	X			
Shneiderman and Plaisant (2015)				X	

Stern, Gordon, Landman and Kramer (2019)	*X*				*X*
Swede, Scovetta and Eugene-Colin (2019)	*X*	*X*			
Ward and Chapman (2008)	*X*			*X*	
Wethington, et al. (2018)				*X*	
Wiltz (2014)			*X*	*X*	
Zhang, et al. (2017)				*X*	

Source: The authors.

For that, this **study proposes to answer** the following research questions: what are the minimum requirements, and what are the best risk management practices applied for a cybersecurity system in healthcare? Thus, this **article aims** to highlight the importance of cybersecurity mainly in the current industry 4.0 and offer healthcare institutions parameters to be used in the fight against cybercrime, investigating risk management focused on identifying requirements and best practices for healthcare data security systems. In this sense, a study of risk management was developed, presenting minimum requirements and best practices that should be employed in safety for medical devices. Through a systematic literature review to expose and describe the characteristics found in the academic literature on the proposed theme, **this article contributes to** a better awareness on the topic, presents the five gaps found in the academic literature and provides subsidies to face the challenges of cybersecurity.

2 Cybersecurity overview in the healthcare industry and risk management

Many modern medical devices contain embedded computer systems, which are increasingly interconnected through networks, this includes devices such as but not limited to: blood pressure and heart rate monitors, glucometers, pacemakers, and insulin pumps (Alexander et al., 2019). There are several benefits to using these devices, such as the rapid transmission of clinical information from patients to doctors and the management of real-time therapy that can improve patient care; however, the existence of this connectivity can put patients at risk for cybersecurity vulnerabilities related to information security and the device's function (Alexander et al., 2019). Medical devices connected to the network using the Internet of Things (IoT) devices may be vulnerable to cybersecurity breaches. Comparatively in 2015, the automotive industry had to implement a recall of 1.4 million vehicles from the Fiat Chrysler company in the United States due to safety problems in which it was possible to remotely control the Jeep Cherokee vehicle, as reported by the same authors.

Cybersecurity reflects the risks experienced as interconnectivity grows and diversifies and with the added resources and speed of storing, processing, and transporting information increase exponentially with each new generation. The internet was developed without concern for the protection of data stored or in transit. Current strategies for dealing with cyber risks focus mainly on remediation or through actions taken by data owners and consumers in the form of data encryption, regulation, organizational support, access control measures, awareness campaigns, risk assessment, blocking, and similar practices (Berger & Schneck, 2019).

For Abraham et al. (2019) the healthcare sector, in which cyber-attacks to the sector have increased by 125% in the last five years, is a vulnerable target. As an example, in the city of Los Angeles in the United States, a healthcare organization paid $17,000 in Bitcoin to a hacker who took control of their systems. Moreover, in the United States, many patients receive bills for medical procedures they have not used or purchases not submitted by the victims. According to the authors, information security breaches in the healthcare sector have the highest costs for companies; in the United States, $400 is spent for each lost or stolen record, compared to the costs faced by other segments of the economy such as the financial sector, $ 215, or retail $ 65.

From the statistics, it is clear that the healthcare sector has become a significant target for cybercriminals. Ondiege et al. (2017) indicate in their study that 90% of organizations have recently been targeted by cybercriminals. For cybercriminals, the healthcare sector is an attractive target for two reasons: it is a source of valuable information and an extremely vulnerable target (Martin, Martin, Hankin, Darzi & Kinross, 2017). In 2013, there were 622 cybersecurity breaches in the industry, and the number of breaches is increasing each year with a record increase of 24.8% between 2012 and 2013 (Blanke & McGrady, 2016). In 2014, reports of cyber threats to the industry in the United States, given by Norse and SANS, over a period of one month, reported 49,917 attacks on more than 700 devices, with 375 compromised organizations (Ondiege et al., 2017).

In 2014, the Society for Health Information and Management Systems (HIMSS) reported that 19% of hospitals had a security breach. According to a 2013 survey on medical identity theft, medical fraud increased by almost 20%, affecting about 1.84 million Americans (Martin et al., 2017). In this sense, the Ponemon Institute has been warning about data breaches annually through reports, such as FireEye and the Experian Security Report, that state that healthcare companies are vulnerable to cybercriminals (Blanke & McGrady, 2016). In addition, the Ponemon Institute explained in its annual study ofpatient privacy and data security that

criminal attacks on healthcare systems have increased 100% since the first study conducted in 2010. In 2017, the institute researched 500 cybersecurity professionals in the industry and found that only 15% of organizations, and 17% of medical device manufacturers, took relevant steps to prevent cyber-attacks. As previously stated, several authors empathize cyber-attacks as imminent and that few health organizations and medical equipment manufacturers have a cybersecurity risk management plan (Blanke & McGrady 2016; Busdicker & Upendra, 2017) which deserves attention from practitioners and the academy.

In the same line of reasoning, the Ponemon Institute reported that in 2016, 64% of healthcare organizations reported attacks, 9% more than in the previous year, with 90% of attacks causing data breaches in organizations. The the United States operator Verizon's data breach report in 2018 found that ransomware malware, which encrypts the file system and requests a payment to decrypt it, was responsible for 85% of all healthcare malware and more than 70% of attacks (Maimó et al., 2019). Similarly, the company Symantec, which focuses its activities on data security, reported that various medical devices spread more than 50% of security problems, and more than 30% of these devices had problems with viruses or other malware (Maimó et al., 2019).

Martin et al. (2017) sad that the healthcare sector is one of the sectors most attacked by cybercriminals worldwide, and in 2014 the global cost of cybercrime was estimated at $575 billion. Also, according to the same authors, in 2015, more than 80% of the 223 organizations surveyed had their data compromised, and only 50% of these organizations believe they have effective cybersecurity. Additionally, more than 110 million patients in the U.S. alone have had their medical data breached, with a 300% increase in attacks analyzed from 2014 to 2016.

In 2018, Hancock Health Hospital in the U.S. paid cybercriminals $55,000 to unlock their systems after a ransomware infection and previous outbreaks, such as the infamous NotPetya and WannaCry cases in 2017, which also affected hospitals worldwide, and it reportedly forced some hospitals to end their activities (Maimó et al., 2019).

According to Ghafir et al. (2018) the healthcare sector does not see data protection as a priority; with this mindset, they invest few resources for these activities. Statistics show a worrying picture of the challenges to be overcome by cybersecurity and digital risks in the health sector. Still according to the same authors, a report by the U.S. Department of Health and Human Services reports that the healthcare industry suffered four data breaches a week in 2016, to put it in perspective, one in three American citizens was a victim of information

breaches as the sector being the one in which more digital security holes are found for information-rich records.

Thus, it is essential to advance research to broaden the perception in this field regarding cybersecurity risk management methods through the inclusion of fundamental understandings, changing corporate habits aimed at cybersecurity at all organizational levels of healthcare institutions (Natsiavas et al., 2018).

Although risks stem from uncertainty, they are not exactly unpredictable since it is possible to determine their frequency, qualification, impact, probability, among other factors, and consequently, to get ready for them in case they appear, by mitigating, transferring or simply eliminating them based on risk management plans (PMI, 2017). Therefore, as organizations become more dependent on cyber processes, they also need to manage the risks to which they are exposed within this new reality (World Economic Forum, 2017).

2.1 Healthcare cybersecurity risk management

According to the PMI (2017), risks are uncertainties, events, conditions, or future circumstances that it may have a negative impact on the organization with or without reputational damage to the organization. The more one knows beforehand about risks and their impacts, the more prepared one is to deal with them if they happen. Accordingly, the risk is defined as the combination of the likelihood of incidence of a given event and the negative impacts resulting from it if it ever happens. Risk is inevitable in any organization; however, members are accountable for ensuring that risks are mitigated to the minimum level possible in order to achieve organizational goals (Abraham et al., 2019; Coronado & Wong, 2014; Kure et al., 2018).

Although risks stem from uncertainty, they are not exactly unpredictable since it is possible to determine their frequency, qualification, impact, probability, among other factors, and consequently, to get ready for them in case they appear, by mitigating, transferring or simply eliminating them based on risk management plans (PMI, 2017). The cybersecurity risk management plan in the healthcare industry requires making decisions daily. Currently, organizations are competing for new technologies as well as for greater use of data analysis and processing of innovations and growth in interconnected environments. Therefore, as organizations become more dependent on cyber processes, they also need to manage the risks to which they are exposed within this new reality (World Economic Forum, 2017).

Thus, it is often necessary to apply to compensate controls, without disturbing the clinical workflow of equipment in order to enable cybersecurity management in healthcare and medical devices. Professionals in this field should find alternatives when controls are not supported and / or when they obstruct the necessary performance of the equipment. Therefore, the management of residual and uncontrolled risks must be a continuous process throughout the life cycle of medical devices (Busdicker & Upendra, 2017).

Similarly, managing cybersecurity risks must be seen as a balancing act between security and resilience. No organization can be completely secure, but it can develop the ability to minimize threats and quickly recover from attacks (Abraham et al., 2019). It is important to have an overview of several important issues of real cybersecurity threats and risk assessment for supervisory control and data acquisition (SCADA) and distributed control systems (DCS) (Abraham et al., 2019; Kure et al., 2018).

Additionally, the modern risk-management method includes existing regulatory requirements and converts them into organization-control goals. The structures and standards included in this risk management method are: National Institute of Standards and Technology (NIST), ISO 31000 (2018), ISO/IEC 27001 (2013), Health Insurance Portability and Accountability Act (HIPAA), Project Management Body of Knowledge (PMBOK), and objective-oriented risk management framework, whose standards provide guidelines for risk-management activities (Ondiege et al. 2017). In addition, risk management plans must associate different attack and breach scenarios to enable healthcare organizations to analyze negative consequences at the time of the breach to assess cyber risks. Among these consequences, one finds payment of ransomware, sending patients/clients to alternative locations for assistance services, damaged reputation, government sanctions, data recovery costs, and finally equipment replacement and implementation of additional security measures (Abraham et al., 2019).

This assessment must be based on the cost of investing in several preventive and mitigating recovery measures (Abraham et al., 2019). Thus, the risk-management plan should work as a guide, as the main reference for managers and employees. It should describe how security risks faced by the organization are to be monitored, controlled and executed. Risks in the organization should be assessed in the same way as financial, clinical, or operational risks (Martin et al., 2017). In addition, it should include attack descriptions, vulnerability identification, recommendation of specific vulnerability controls, and control plan implementation (Blanke & McGrady, 2016).

Thus, because security threats have grown exponentially in recent years, organizations need to implement comprehensive cybersecurity risk management systems to identify unique threats or trends. One solution for such an issue lies on the layered approach used to assess security-based risks in order to prevent, mitigate, and tolerate attacks on medical devices and cyber infrastructures (Abraham et al., 2019; Kure et al., 2018).

Accordingly, risk management is defined as a process (a journey) structured into eight stages. This strategy helps to identify the risk to be controlled by following different control strategies, as shown in Table 2 (Abraham et al., 2019; Blanke & McGrady, 2016; Coronado & Wong, 2014; Kure et al., 2018; PMI, 2017).

Data breaches resulting from these attacks represent a significant threat to the viability of healthcare organizations. Damages resulting from such breaches range from financial losses to compromised patient safety. Cybersecurity insurance has become an essential tool to help to mitigate financial liabilities resulting from breaches in many organizations (Kabir et al., 2020; Jalali, Russell, Razak & Gordon, 2019).

Table 2 – Risk identification and control strategy

Stage	Authors
Identify cyber risks	(Abraham et al., 2019; Busdicker & Upendra, 2017; Coronado & Wong, 2014; Dandage, Mantha & Rane, 2018; Kure et al., 2018; Natsiavas et al., 2018; Ondiege et al., 2017; PMI, 2017)
Quantitatively and qualitatively assess cyber risks	(Abraham et al., 2019; Blanke & McGrady, 2016; Coronado & Wong, 2014; Kure et al., 2018; Kruse et al., 2017; PMI, 2017)
Analyze the likelihood of cyber risks occurring	(Abraham et al., 2019; Blanke & McGrady, 2016; Kure et al., 2018; PMI, 2017)
Check the impact of cyber risks	(Abraham et al., 2019; Blanke & McGrady, 2016; Kure et al., 2018; PMI, 2017)
Classify cyber risks	(Abraham et al., 2019; Coronado & Wong, 2014; Kure et al., 2018; PMI, 2017)
Plan responses to cyber risks	(Abraham et al., 2019; Blanke & McGrady, 2016; PMI, 2017)
Monitor cyber risks	(Abraham et al., 2019; Blanke & McGrady, 2016; Coronado & Wong, 2014; Kure et al., 2018; PMI, 2017)
Manage risks and residual risks	(Abraham et al., 2019; Blanke & McGrady, 2016; Coronado & Wong, 2014; Kure et al., 2018; Ondiege et al., 2017; PMI, 2017)

Source: The authors.

Initially, risks can be identified in several ways. One of the simplest ways to identify risks lies on reviewing the cybersecurity documentation provided by device manufacturers.

Many professionals use the Medical Device Risk Assessment Platform to perform a risk assessment in connected medical devices (Busdicker & Upendra, 2017). Thus, all actors in the organization must help to identify risks in the organization. All risks must be recorded in a single document called the risk management matrix (Abraham et al., 2019; Coronado & Wong, 2014; Kure et al., 2018).

According to HIPAA, a checklist of current security practices should be created and used to identify gaps in these practices. Thus, the organization must compare cybersecurity-related policies to assure compliance with current regulations and best practices (Blanke & McGrady, 2016).

According to Natsiavas et al. (2018) a threat can be defined as a latent danger, in other words, threats are situations or uncontrolled actions that can be associated with malicious people or out-of-control factors, such as bad weather or physical failures, which can take control which can take control, damage or destroy assets within organizations. Threats can refer to technical, functional, legal, personal, or political aspects, although they are not limited to them. Technical threats in systems can be classified as: a) counterfeiting: access to private systems using false identification in order to damage them or obtain advantages; b) tampering: duplicating, modifying reproducing or tampering with information, documents, products, equipment or services without authorization; c) repudiation: denying specific commands or operations in the systems, through legitimate users or not; d) information disclosure: exposing confidential data, information or knowledge about organizations; e) DoS: English acronym for Denial of Service, referring to making resources of a given application, system or equipment unavailable for use. This practice renders devices invalid due to overload. It is often done in two different ways, namely, by making the system overload and consuming all its resources to stop it from working properly or by disabling communication between systems in order to isolate them; f) elevation of privilege: granting privileges to users or attackers other than the permissions initially authorized by the system, allowing users with limited access to have unlimited access to the system as administrators.

Risk analysis provides a framework for managers to know and assess the organization's vulnerabilities, as well as to develop security plans before the event takes place (Blanke & McGrady, 2016). Likewise, the qualitative analysis highlights the subjective aspects of each member (how each member understands and qualifies the risk). This analysis is based on member's experience and is used to investigate member's perception or understanding about

the nature of a given risk, based on their interpretation of it (Blanke & McGrady, 2016; PMI, 2017).

On the other hand, quantitative analysis assigns numerical probabilities to each identified risk as well as examines its potential, impact, and consequences. The risk can be grouped in different categories whenever necessary. The quantitative analysis enables understanding cyber risks based on measurable and quantifiable data, i.e., based on numbers (Blanke & McGrady, 2016; PMI, 2017). It is important to emphasize that the connection between the security of energy applications and the support of infrastructure security in risk assessment processes provides a methodology capable of assessing the likely impacts of risk (Abraham et al., 2019; Kure et al., 2018).

Thus, the countermeasures proposed were based on the risk matrix method with the risk classification. Values attributed to risks were introduced in the information security management system (ISMS) and subjected to quantitative analysis, which enables assessing risks in detail. Quantitative risk assessment allowed for the observation of whether the aforementioned countermeasures could reduce the risks to a certain extent (Abraham et al., 2019; Kure et al., 2018).

The analysis of the cost-benefit ratio applied to the proposed countermeasures is an important assessment to be carried out. An efficient strategy focused on assessing cybersecurity risk of systems Supervision and Data Acquisition System (SCADA) must at least have clear objectives, master the proposed applications, divide risk management stages into manageable parts, master risk management concepts, and measure the impact of risks and probabilistic data sources (Abraham et al., 2019; Kure et al., 2018).

Thus, based on the literature in the field, despite the substantial number of risk assessment methods developed for systems such as the SCADA, it is necessary to develop a comprehensive method comprising all risk management process stages. A good strategy found in the literature has suggested assessing organizations' vulnerability to information security breaches through threat impact and cyber vulnerability indices based on the design of vulnerability trees (Kure et al., 2018).

The value of this tool is how it helps managers determine the current security level in the organization and select the best security mechanisms to be used. Several attack-impact simulations - such as system availability and integrity attacks - must be performed in the system. Several articles available in the literature limit their efforts in detecting attacks on cyber-physical systems (Abraham et al., 2019). However, the overall approach to cybersecurity risk

assessment articles allows for the conclusion that it is important adopting a comprehensive risk management method capable of covering all risk management process stages, from risk identification to the likely response to that risk. Most approaches found in the literature often emphasize the assessment of and vulnerabilities in the identification of threats. However, there is a lack of emphasis on processes adopted after these risks are identified (Kure et al., 2018).

Thus, it is necessary to analyze the likely incidence of cyber risks so that the analysis or numerical measurement of the likelihood of facing a certain identified risk can occur. This analysis enables the industry to identify which risks are most likely to occur in cyber risk management at the expense of other risks. Based on this classification, it is possible to identify the risks to be treated based on their likelihood to happen (Blanke & McGrady, 2016; PMI, 2017). Thus, one must analyze the impact, consequences, and effects that cataloged risks can have on the organization. Questions should also be asked, such as: if this risk materializes, what impact will it have on the organization? Subsequently, direct and indirect impacts of such a risk should be classified (Blanke & McGrady, 2016).

According to Abraham et al. (2019) and Kure et al. (2018), it is essential to measure information in the form of commitment graphs and increased vulnerability trees to help quantitatively determine the likelihood of attacks, the impact of these attacks, and risk reduction in response to a specific countermeasure in order to enable decision-making processes. The Risk Division Structure (RBS) approach plays a key role in managing sector risks. After all, risks are identified, quantitatively and qualitatively assessed, have their likelihood of incidence analyzed and their impacts checked, it is necessary to classify the risk matrix based on risk severity (Coronado & Wong, 2014; Kure et al., 2018).

Thus, risks can be classified based on several safety parameters, namely, operational, non-technical, technical, and governance or regulatory. All security risks must undergo appropriate assessment (Abraham et al., 2019; Kure et al., 2018). Planning responses to risks is the process of designing actions to deal with these risks whenever they take place. The planning process must also enable organizations to identify and select employees to deal with risk whenever it happens. Four different ways to deal with risks were found in the literature (Blanke & McGrady, 2016; PMI, 2017): a) prevention, which is a set of anticipated measures aimed at preventing cyber-attacks; b) mitigation, which minimizes the consequences of cyber-attacks; c) transfer, which transfers the consequences of attacks to hired third parties; d) acceptance, which accepts the consequences of attacks and is often applied when there is no viable solution to the problem.

According to Blanke and McGrady (2016) and PMI (2017) risk monitoring is a continuous process. The identified risks must be monitored and evaluated; residual risks must be monitored, and new risks must be identified. One should identify whether any new risks are likely to be found. It must be done in order to include them in the risk matrix chosen to be subjected to all processes in order to assess whether the risk will appear. Thus, one must actively monitor all these risks and develop plans to mitigate them or find any other solution to counteract them. Risks are the possible unwanted consequences of the system since they can compromise organizations' security (Coronado & Wong, 2014; Kure et al., 2018).

In addition, risk monitoring and management processes take place simultaneously. The monitoring process is constantly checking for risks whereas the management process is constantly evaluating risks, analyzing residual risks, and evaluating the effectiveness of risk management plans (Blanke & McGrady, 2016; PMI, 2017).

Thus, all of these processes must interact with each other, creating a synergy in management against cybercriminals. Each process can involve the effort of one or more people, according to the needs found. Although the processes are presented as distinct elements with a defined sequencing, in practice, they will overlap and interact with each other (Blanke & McGrady, 2016).

3 Research methodology

The methodology adopted in the present study was based on a systematic literature review (Alcântara & Martens, 2018) which mixed bibliometric and content analysis.

According to Bardin (2011) content analysis refers to the grouping of techniques for the evaluation of human communication, using systematic procedures with the objective of defining the content of the message, having as main objective the inference of knowledge related to the perception of the content of a given message. Thus, even according to the same author, it is possible to enrich the interpretation of the data collected through meaning that is often explicit or hidden.

In this way, this study uses the three classic phases of Bardin (2011): pre-analysis, exploration of the material and treatment of the results and interpretations.

The first phase called **Pre-Analysis** was subdivided into five stages.

The stage one refers to **the search in the online research bases**, in which the combination of the keywords: **Healthcare**, **Cybersecutity and Risk Management** were used, in the article title, abstract and keywords fields of the seven online databases that were selected

to provide a broad spectrum to form a solid and consistent theoretical framework for academic studies. In total, 182 articles were found: Scopus (42), Science Direct (38), Esmeralda (19), Wiley Library (17), Proquest (10), Taylor & Francis (08) and Web of Science (48).

The stage two refers to **the selection and exclusion criteria for sources**, and focused on the choice of documents relevant to the research topic. As selection criteria, only documents in the format of articles and review articles were used, only articles published in global journals from 2016 to 2020 were also included, only articles in digital format and in the English language were included. Exclusion criteria were conference documents, book chapters, printed articles or academic theses and dissertations.

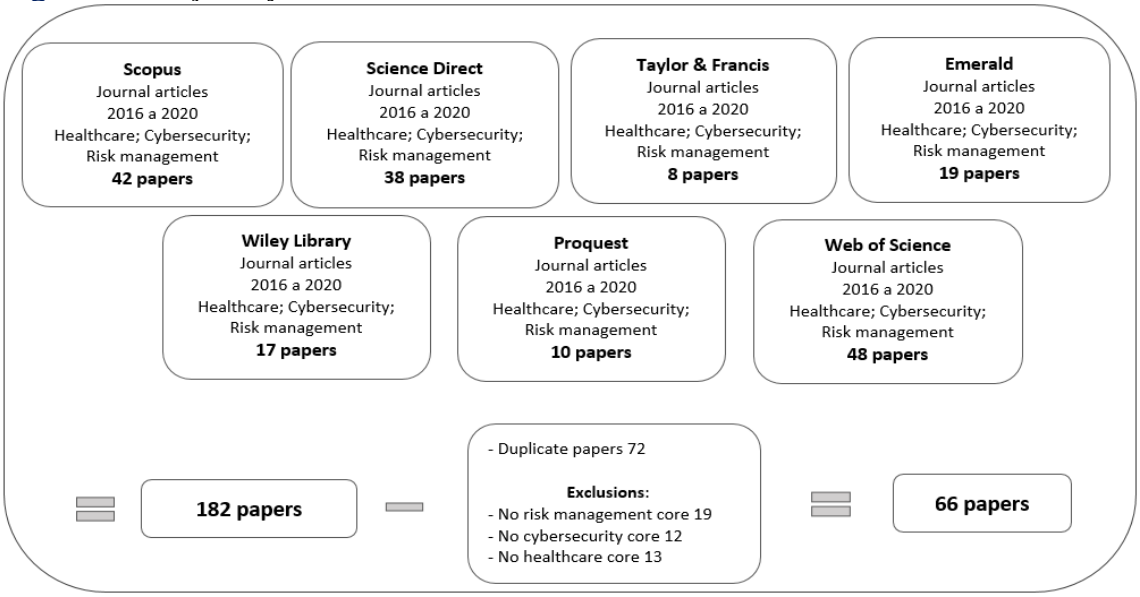
The stage three refers to **the rationale for the *corpus* of the work**. With the application of the inclusion / exclusion criteria, the time period of the published articles that would be analyzed and the selected databases, constituted the 182 articles that supported the *corpus* of this article's work.

The step four involved **the floating reading** of the 182 selected articles from the article title, abstract and introduction fields, this process allowed us to find repeated articles, as well as articles that were not relevant for the purpose of the current research. In this way, it was possible to remove from the pretensions of this research 72 repeated articles, 19 articles without connection with the theme of risk management, 12 articles without connection with the theme cybersecurity and 13 without connection with the theme of healthcare. Thus, 66 relevant articles were selected at the end of the floating reading process that are part of this work.

The step five enabled **the conception of the prepositions and objectives of this research**. In which it was possible to observe the importance of cybersecurity in the current industry 4.0. The awareness and separation of the five gaps found: a) Cybersecurity is an extremely important topic in the healthcare sector; b) Cybersecurity in the healthcare sector is neglected; c) There are no significant investments in the healthcare sector; d) The information generated by the healthcare sector is rich in content; e) There is a lack of actions protection of data in the healthcare sector. And so, offer healthcare institutions parameters to be used in the fight against cybercrime.

Figure 1 summarizes the pre-analysis processes.

Figure 1 – Trajectory of article selection



Source: The authors.

The second phase called **the exploration of selected articles** is the phase in which a vertical analysis / reading of the 66 selected articles is made.

The single step of this phase consisted of deepening the understanding and analysis of the selected texts through their exploration and codification of the selected articles, which resulted in the constitution of that article. The articles were read in full and categorized through a framework of analysis of the relationship with the proposed study theme. In this context, the record units were excerpts, citations and important ideas from the 66 selected articles. Thus, fourteen main content groups were created: cryptography, cyber physical systems, cybersecurity, malware, secure control systems, viruses, crisis management, management, plan, project management, risk management, 5G, industry 4.0, internet of thing, data processing and healthcare, which were relevant to the purpose of this work.

The third phase, called **Treatment of Results and Interpretations**, constitutes the interpretation of the selected information and grouped into a richer understanding and new knowledge that are proposed by this work. Through this phase it was possible to make all the

quantification and qualification used throughout this study as well as the synthesis and selection of the proposed results.

The next section shows in more detail the results of this methodology.

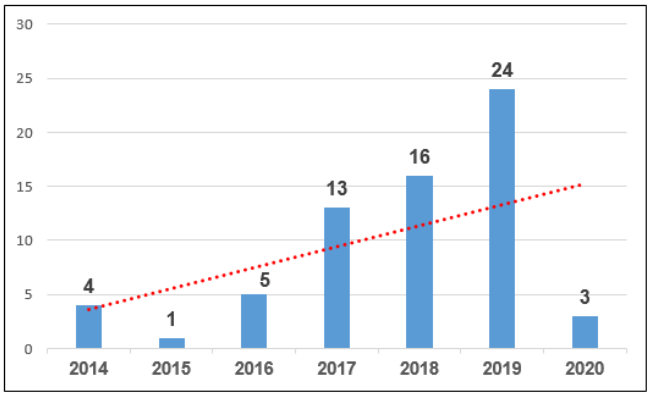
4 Results and analysis

This section of the article presents the main results of the analysis of the constructed base. The results include the frequency and the respective content related to the authors, keywords, and journals.

4.1 Literature measurement

Figure 2 evidences the evolution of publications about the investigated topic in the last seven years. The blue dotted line indicates the evolution of articles, which were included in the portfolio presented in the current study. Only 10 articles on the investigated topic were published from 2014 to 2016, whereas 56 articles were published from 2017 to 2020.

Figure 2 – Evolution of the publications



Source: The authors.

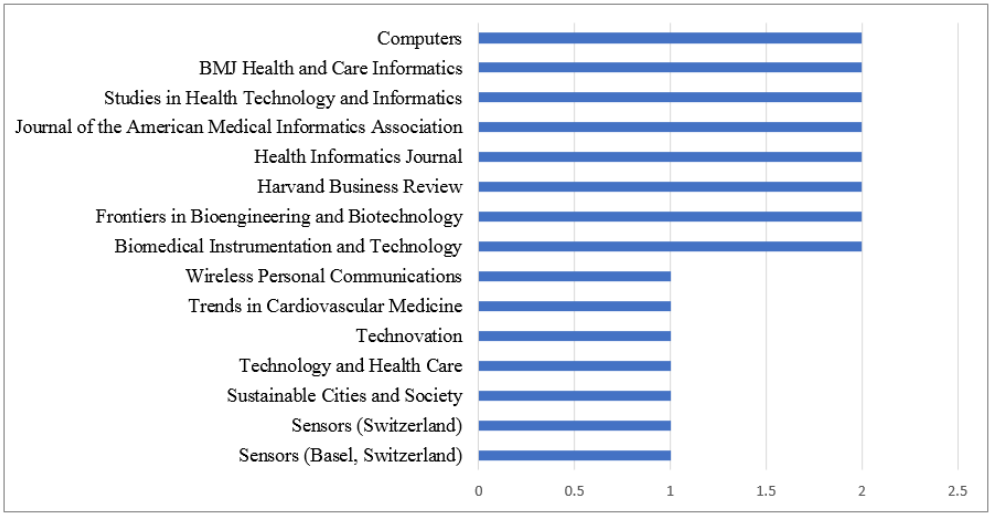
Another analysis has shown that the frequency of keyword citations in the articles allows a first reading of the themes in a given area (Thomé, Scavarda, Scavarda & Thomé, 2016). The three most frequent keywords of the 294 ones used in the articles included in the current study were cybersecurity (30 times), security (five times), and privacy (five times). Figure 3 depicts the connection between the keywords and the portfolio of articles. For analysis of this figure was using the software VOSViewer (Van Eck & Waltman, 2010).

Figure 3 – Map of occurrence network between words

Source: The authors.

Finally, Figure 4 indicates the most active journals associated with the investigated topic in the last seven years. “Studies in Health Technology and Informatics” and “Frontier in Bioengineering and Biotechnology” were the most active journals on the subject.

Figure 4 – Representativeness in scientific journals



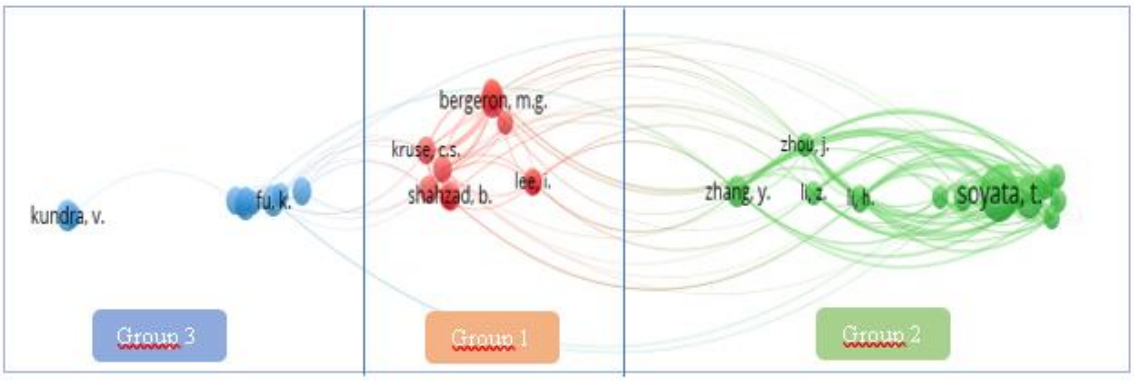
Source: The authors

There was also prevalence 64% of articles published with the collaboration of more than one research institution to the detriment of published articles produced by a single institution.

4.2 Network analysis

The map presenting the network of authors co-citing the authors cited in the articles is shown in Figure 5. The minimum co-citation of five per author was used. This connection was determined based on the number of times the authors were cited together, which means that they have assessed similar subjects or related fields, thus generating citations from other researchers in the same articles. The current study has found the prevalence of three co-citation groups. For network analysis was used the software VOSViewer (Van Eck & Waltman, 2010).

Figure 5 – Co-citation of authors in the database - with indication of cluster



Source: The authors.

The link between authors represents citations in the same article in this article portfolio. The intensity of the line connecting two authors corresponds to the intensity of the relationship. Appendix 1 shows the class of article-author grouping. Intensity values show the intensity of relationships in the set of articles.

The eight most relevant articles analyzed in the current study had at least five citations. There was the relevant concentration of articles associated with institutions such as: Chul De Quebec Research Center (Canada); National University of Modern Languages (Islamabad - Pakistan); Texas State University (United States); Albany University (United States); Howard University (Usa); Beth Israel Medical Deaconess Medical Center (United States); Partners Healthcare (United States), and University of Connecticut (United States).

Researchers in **Group 1** agreed that cybersecurity is of paramount importance for the healthcare field. Cybersecurity is becoming an increasingly important component for the infrastructure of health services, whose recent attacks have had negative impacts on their operations. Such impacts have resulted in information loss, cancellation of consultations and clinical procedures, and high monetary cost as well as have generated a negative image of these institutions (Al-Muhtadi, Shahzad, Saleem, Jameel, & Orgun, 2019; Bissonnette & Bergeron, 2017; Kruse et al., 2017).

The researchers in **Group 2** agree that as information generated in the health area is rich in content, the sale of this information has generated billions of dollars in recent years on the dark web. The extracted information allows access to prescription drugs, extortion, opening bank accounts, loans, or passports (Coventry & Branley, 2018; Good et al., 2005; Habibzadeh, Nussbaum, Anjomshoa, Kantarci & Soyata, 2019; Wethington et al., 2018).

Researchers in **Group 3** agreed that cybersecurity is neglected in the healthcare field. The industry is not prepared to deal with the reality of today's cyber threats; it only deals with cybersecurity issues after the system is compromised. Finally, all three groups agreed on the need to set clear terms with minimum cybersecurity items or requirements for the sector as well as pointed out the need to develop risk management plans (Gordon et al., 2019).

4.3 Cybersecurity requirements and best practices

According to Coventry and Branley (2018) and Martin et al. (2017), cyber resilience is a holistic view of cyber risk, which analyzes organizations' culture, employees, processes, and technology, among others. Several factors were identified to help to improve the situation through minimum cybersecurity items based on this viewpoint.

According to the literature in the field, minimum cybersecurity items enable the healthcare sector to improve the resilience and cybersecurity of medical devices. Table 3 represents the minimum-security items necessary to assure the safety of medical devices in the healthcare sector in the current era of interconnectivity and IoT.

Table 3 – Minimum requirements for medical device security

Requirement	Authors
All medical devices must be properly inventoried, containing what type of information the device stores	(Blanke & McGrady, 2016; Coronado & Wong, 2014)
All devices must be password protected, with screen savers and automatic log offs after a predetermined period.	(Blanke & McGrady, 2016; Mostfa Kamal, Abd Ali, Alani & Abdulmajed, 2016)
All devices must contain strong passwords, with a combination of eight characters and digits. These passwords must be changed every six months.	(Blanke & McGrady, 2016; Mostfa Kamal et al., 2016)
All portable devices must encrypt data. All keys used for encryption and decryption must be previously approved to meet complexity requirements.	(Blanke & McGrady, 2016; Braga, Dahab, Antunes, Laranjeiro & Vieira, 2019; Coronado & Wong, 2014; Kharraz, Robertson & Kirda, 2018; Natsiavas et al., 2018)
All portable devices must contain remote cleaning and geographic location tracking.	(Blanke & McGrady, 2016)
All devices must have lock enabled after three failed login attempts.	(Abraham et al., 2019; Blanke & McGrady, 2016; Busdicker & Upendra, 2017; Kharraz et al., 2018; Priestman, Anstis, Sebire, Sridharan & Sebire, 2019)
All devices must have their operating systems, software, and antivirus updated as new releases and patches become available.	(Abraham et al., 2019; Blanke & McGrady, 2016; Ondiege et al., 2017; Primo, Bishop, Lannum, Cram, Nader & Boodoo, 2018)
All devices must have their data backed up on periodically backed up in a secure location on which cybersecurity experts have previously agreed.	(Abraham et al., 2019; Blanke & McGrady, 2016; Ghafir et al., 2018; Kharraz et al., 2018; Martin et al., 2017; Primo et al., 2018)

Source: The authors.

Based on the analysis, one-third of healthcare industry management sectors acquired cybersecurity solutions without having any expert guidance or technical criteria (Abraham et al., 2019). Thus, the best practices found in the literature about cybersecurity in the healthcare sector are presented in Table 4.

Table 4 – Best practices recommended for the healthcare industry

Best Practices	Authors
When hiring a new employee (even for part-time jobs), the employee's background should be checked	(Blanke & McGrady, 2016; Coronado & Wong, 2014; Gordon et al., 2019; Ondiege et al., 2017)
Limited access to the system should be granted based on the need for access to employees and on the roles and responsibility of the activity performed in each position.	(Blanke & McGrady, 2016; Coronado & Wong, 2014; Ondiege et al., 2017)
Users' access to databases must be restricted by linking access to information such as user's name, password, accessed information, location, and date of access.	(Abraham et al., 2019; Blanke & McGrady, 2016; Mostfa Kamal et al., 2016; Priestman et al., 2019)
Two- or three-factor authentication must be used to access the organization's system.	(Abraham et al., 2019; Blanke & McGrady, 2016; Busdicker & Upendra, 2017; Coronado & Wong, 2014; Priestman et al., 2019)
Activities should be audited and reviewed frequently, according to employees' responsibility.	(Abraham et al., 2019; Blanke & McGrady, 2016; Bojanova & Voas, 2017; Busdicker & Upendra, 2017; Coronado & Wong, 2014; Habibzadeh et al., 2019; Huang, 2014; Kuerbis & Badiei, 2017)
Records of the entire organization infrastructure must be reviewed to validate individual access and use.	(Blanke & McGrady, 2016)
Constant training must be provided to all organization employees.	(Abraham et al., 2019; Blanke & McGrady, 2016; Coronado & Wong, 2014; Gordon et al., 2019; Kruse et al., 2017; Maimó et al., 2019; Martin et al., 2017; PMI, 2017)
Employees' awareness of digital security must be constantly enabled.	(Abraham et al., 2019; Blanke & McGrady, 2016; Busdicker & Upendra, 2017; Coronado & Wong, 2014)
Access to the system and the organization of employees who leave the organization must be removed.	(Ahmed & Ahmed, 2019; Blanke & McGrady, 2016; Busdicker & Upendra, 2017; Diggans & Leproust, 2019)

Employee dismissal must be communicated; the dismissed employee must have contact with suppliers or partners disconnected.	(Ahmed & Ahmed, 2019; Blanke & McGrady, 2016; Diggans & Leproust, 2019)
Parking and all external areas of the organization must be properly lit at night.	(Blanke & McGrady, 2016)
All equipment and physical documents must be properly disposed.	(Blanke & McGrady, 2016; Busdicker & Upendra, 2017; Lebeda, Zalatoris & Scheerer, 2018)
The terminal must be locked every time the employee is absent, no matter how brief the absence is.	(Blanke & McGrady, 2016)

Source: The authors.

5 Future implications

It is evident that if cybersecurity issues in healthcare institutions are not resolved promptly, their impact on such institutions can be catastrophic and cause sociotechnical issues. In addition, given the critical nature of medical devices, and their ability to affect patients' health, the potential of cybersecurity breaches to cause damage is catastrophic since vulnerabilities identified in this segment are extremely complex.

This sector has many vulnerabilities; nowadays, financial gain is the main reason for cyber-attacks, although political motivations and the likelihood of taking lives are projected by experts as the evolution of the motivation for attacks, which is expressed in the form of cyber warfare. On the other hand, the sector has made great progress over the years, such as the Health Information Technology for Economic and Clinical Health (HITECH), the Health Insurance Portability and Accountability Act (HIPAA), the National Institute of Standards and Technology (NIST), the National Health Service (NHS) in England, the Chinese Personal Information Security Specification and, in Brazil, the General Data Protection Act (LGPD), among others.

Thus, the healthcare sector must incorporate new risk management solutions to use technological innovations in order to meet current healthcare needs in and outside hospital environments. Therefore, new paradigms such as the Internet of Medical Things (IoMT) that, for standardization purposes, was herein referred to as the Internet of Things (IoT), and the Cyber-Physical Medical Systems (MCPS) offer new solutions to monitor, diagnose, and treat patients through medical interconnections by using devices with integrated computer systems (King et al., 2018; Maimó et al., 2019; Wethington et al., 2018).

Thus, the sector expands the use of mobile health devices that work on disease prevention, monitoring, and diagnosis by using technological tools and solutions developed to improve the quality of medical care based on new technologies. Therefore, the projection of specialists is that these MCPSs will create solutions to prevent epidemics, help treat chronic

diseases, and prevent deaths within a few years as well as will bring data crossing to the analysis of the so-called big data (Bilek, Muscionico, & Amiel, 2017).

Accordingly, there are new solutions in remote care, such as telehealth, which refers to a broad concept that may include activities such as remote services, diagnostics, research, and education in the health field. There is an extremely valuable range of possibilities enabled by telehealth; it comprises telediagnosis, which makes it possible to diagnose diseases at a distance (patients and doctors in different places) and uses Information and Communication Technologies (ICTs) that allow sharing medical information to diagnose diseases (Coventry & Branley, 2018; Handler, 2018).

The importance of cybersecurity is mainly reinforced by three main actions (Okereafor & Marcelo, 2020): preventive identification of planned or active cyber-attacks against health data, systematic prevention of cyber-attacks targeting vulnerable health information systems, and prompt responses to cyber-attacks successfully executed in order to minimize their impact.

This panorama sets the health data management scenario in the Covid-19 era and beyond. It strongly relies on health data classification, which is based on value, sensitivity to privacy and criticality to life (Okereafor & Marcelo, 2020).

Major pandemics, such as Covid-19, are associated with high contagion levels since they account for shortcomings and respiratory infections that can cause economic crises and take contaminated patients to death. Thus, there is a challenge in the capacity of health systems worldwide with the sudden lack of medical resources to serve a large number of patients, and to ensure the safety of patients and health professionals (Vecchione, Stintzing, Pentheroudakis, Douillard & Lordick, 2020).

6 Final considerations

With this study, we found that there is no 100% effective way to prevent system violations by cybercriminals, but cybersecurity should be part of management processes in healthcare organizations that should always pursue cyber resilience.

In this sense, the current study has shown that, given their vulnerabilities, health organizations are often the particular target of cyber-attacks and warned several members in the sector to protect themselves based on cybersecurity measures and new products inherent to the health market.

Data breaches deriving from these attacks represent a significant threat to the viability of healthcare organizations; damages range from financial losses to compromised patient safety.

Accordingly, we believe that this study has equally contributed to the literature of healthcare cybersecurity risk management because, besides presenting a systematic and conceptual review on the main topic, it highlighted significant gaps in the literature with an emphasis on the need to conduct further research to help better understand the risk management method applied to control cybercrimes in the healthcare sector in the context of the digital era or industry 4.0.

Thus, the current research presented contributions to risk management and control in healthcare cybersecurity systems, minimum requirements for medical device safety, best practices recommended for the healthcare industry and five gaps found in the academic literature.

This context suggests advancements in scientific research regarding the main themes presented in the current research.

Thus, in addition to advancements in scientific research on this subject, for good risk-management practices and for the adoption of the presented minimum safety items, organizations can ensure that decision-makers will be able to prepare themselves in order to provide efficient answers to the risks to which organizations are exposed and to equip themselves to reduce or even to eliminate existing and latent risks by improving the performance and effectiveness of health institutions.

Finally, keywords were a limitation of the present study, and assumingly, created a bias in it, given the detailed description of the systematic literature review carried out. However, the research, despite these limitations, provides updates to other research and broadens the spectrum of analysis and interpretation. Further qualitative and quantitative research is also recommended to better understand this theme in the healthcare context and other sectors in order to provide an even greater scientific contribution to the research field in healthcare cybersecurity and other sectors.

References

Abdelhamid, M., Kisekka, V., & Samonas, S. (2018). Mitigating e-services avoidance: the role of government cybersecurity preparedness. Information and Computer Security, 27, pp. 26-46. doi:10.1108/ICS-02-2018-0024.

Abraham, C., Chatterjee, D., & Sims, R. R. (2019). Muddling through cybersecurity: Insights from the U.S. healthcare industry. Business Horizons, v.62(n.04), pp. 539-548. doi:10.1016/j.bushor.2019.03.010.

Ahmed, A. A., & Ahmed, W. A. (2019). An Effective Multifactor Authentication Mechanism Based on Combiners of Hash Function over Internet of Things. Sensors, 19 n.17. doi:10.3390/s19173663.

Alcantara, D. P., & Martens, M. L. (2018). Technology Roadmapping (TRM): a systematic review of the literature focusing on models. Technological Forecasting and Social Change, pp. 127-138. doi:doi.org/10.1016/j.techfore.2018.08.014.

Alexander, B., Haseeb, S., & Baranchuk, A. (2019). Are implanted electronic devices hackable? Trends in Cardiovascular Medicine, pp. 476-480. doi:10.1016/j.tcm.2018.11.011.

Al-Muhtadi, J., Shahzad, B., Saleem, K., Jameel, W., & Orgun, M. A. (2019). Cybersecurity and privacy issues for socially integrated mobile healthcare applications operating in a multi-cloud environment. Health Informatics Journal, 25, 315-329. doi:10.1177/1460458217706184.

Askar, A. J. (2019). Healthcare management system and cybersecurity. International Journal of Recent Technology and Engineering, 237-248.

Baaziz, A.; Quoniam, l. (2013). How to use big data technologies to optimize operations in upstream petroleum industry. International Journal of Innovation, v. 1 n.1, p. 19-25. doi 10.5585/iji.v1i1.4.

Berger, K. M., & Schneck, P. A. (2019). National and transnational security implications of asymmetric access to and use of biological data. Frontiers in Bioengineering and Biotechnology, 7. doi:10.3389/fbioe.2019.00021.

Bilek, A. M., Muscionico, D., & Amiel, C. (2017). A primer on the regulation and development of M-Health products. Regulatory Rapporteur, https://www.scopus.com/record/display.uri?eid=2s2.085032879397&origin=inward&txGid=408ced46814b35c8bd8454243cf24e2d.

Bissonnette, L., & Bergeron, M. G. (2017). Portable devices and mobile instruments for infectious diseases point-of-care testing. Expert Review of Molecular Diagnostics, 471-494. doi:10.1080/14737159.2017.1310619.

Blanke, S. J., & McGrady, E. (2016). When it comes to securing patient health information from breaches, your best medicine is a dose of prevention: A cybersecurity risk assessment checklist. Journal of healthcare risk management, 14-24. doi:10.1002/jhrm.21230.

Bojanova, I., & Voas, J. (2017). Trusting the Internet of Things. IT Professional, 19 n.5, 16-19. doi:10.1109/MITP.2017.3680956.

Braga, A., Dahab, R., Antunes, N., Laranjeiro, N., & Vieira, M. (2019). Understanding How to Use Static Analysis Tools for Detecting Cryptography Misuse in Software. IEEE TRANSACTIONS ON RELIABILITY, 1384-1403. doi: 10.1109/TR.2019.2937214.

Brody, R. G., Chang, H. U., & Schoenberg, E. S. (2018). Malware at its worst: death and destruction. International Journal of Accounting & Information Management. doi:10.1108/ijaim.2011.36619caa.003.

Burns, L. R., DeGraaff, R. A., Danzon, P. M., Kimberly, J. R., Kissick, W. L., & Pauly, M. V. (2011). The Wharton School Study of the Health Care Value Chain. San Francisco CA: John Wilet and Sons.

Busdicker, M., & Upendra, P. (2017). The role of healthcare technology management in facilitating medical device cybersecurity. Biomedical Instrumentation and Technology, 19-25. doi:10.2345/0899-8205-51.s6.19.

Coronado, A. J., & Wong, T. L. (2014). Healthcare cybersecurity risk management: Keys to an effective plan. Biomedical Instrumentation and Technology, 48, 26-30. doi:10.2345/0899-8205-48.s1.26.

Coveney, P. V., Dougherty, E. R., & Highfield, R. R. (2016). Big data need big theory too. Philosophical Transactions Of The Royal Society A-Mathematical Physical And Engineering Sciences, 374. doi:10.1098/rsta.2016.0153.

Coventry, L., & Branley, D. (2018). Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. Maturitas, 48-52. doi:10.1016/j.maturitas.2018.04.008.

Cleland-Huang, J. (2014). How well do you know your personae non gratae? IEEE Software, 31, 28-31. doi:10.1109/MS.2014.85.

Dandage, R., Mantha, S. S., & Rane, S. B. (2018). Ranking the risk categories in international projects using the TOPSIS method. International Journal of Managing Projects in Business, 11, 317-331. doi:10.1108/IJMPB-06-2017-0070.

Diggans, J., & Leproust, E. (2019). Next steps for access to safe, secure DNA synthesis. Frontiers in Bioengineering and Biotechnology, 7. doi:10.3389/fbioe.2019.00086.

Elizabeth, M. J., Jobin, J., & Dona, J. (2019). A fog based security model for electronic medical records in the cloud database. International Journal of Innovative Technology and Exploring Engineering, 8 n.7, pp. 2552-2560.

Frontoni, E., Mancini, A., Bald, M., Paolanti, M., Moccia, S., Zingaretti, P., . . . Misericordia, P. (2019). Sharing health data among general practitioners: The Nu.Sa. project. International Journal of Medical Informatics, 129, pp. 267-274. doi:10.1016/j.ijmedinf.2019.05.016.

Ghafir, I., Prenosil, V., Hammoudeh, M., Baker, T., Jabbar, S., Khalid, S., & Jaf, S. (2018). BotDet: A System for Real Time Botnet Command and Control Traffic Detection. IEEE Access, 38947-38958. doi:10.1109/ACCESS.2018.2846740.

Ghafur, S., Grass, E., Jennings, N., & Darzi, A. (2019). The challenges of cybersecurity in health care: the UK National Health Service as a case study. The Lancet Digital Health, 1 n.1, pp. 10-12. doi:10.1016/S2589-7500(19)30005-6.

Good, N., Dhamija, R., Grossklags, J., Thaw, D., Aronowitz, S., Mulligan, D., & Konstan , J. (2005). Stopping spyware at the gate: A user study of privacy, notice and spyware. ACM International Conference Proceeding Series. doi:10.1145/1073001.1073006.

Gordon, W. J., Stern, A. D., Landman, A. B., & Kramer, D. B. (2019). Evaluation of a mandatory phishing training program for high-risk employees at a US healthcare system. Journal of the American Medical Informatics Association, 547-552. doi:10.1093/jamia/ocz005.

Goncharov, E., Kruglov, K., & Dashchenko, Y. (2019). Five ICS cybersecurity myths based on Kaspersky Lab ICS CERT experience. At-Automatisierungstechnik, 67, pp. 372-382. doi:10.1515/auto-2019-0016.

Grimes, S., & Wirth, A. (2017). Holding the Line: Events that Shaped Healthcare Cybersecurity. Biomedical instrumentation & technology. doi:10.2345/0899-8205-51.s6.30.

Habibzadeh, H., Nussbaum, B. H., Anjomshoa, F., Kantarci, B., & Soyata, T. (2019). A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities. Sustainable Cities and Society, 50. doi:10.1016/j.scs.2019.101660.

Handler, I. (2018). Data Sharing Defined-Really! Computer, 36-42. doi:10.1109/MC.2018.1451659.

Huang, J. C. (2014). How well do you know your personae non gratae? IEEE Software, 31, 28-31. doi:10.1109/MS.2014.85.

ISO/IEC 27001 (2013) Information technology - Security techniques — Information security management systems — Requirements. [S.l.]. https://www.iso.org/standard/54534.html.

ISO31000 (2018). Risk management - Principles and guidelines. [S.l.]. https://www.iso.org/standard/65694.html.

Jalali, M. S., Russell, B., Razak, S., & Gordon, W. J. (2019). EARS to cyber incidents in health care. Journal of the American Medical Informatics Association, 26, 81-90. doi:10.1093/jamia/ocy148.

Kabir, U. Y., Ezekekwu, E., Bhuyan, S. S., Mahmood, A., & Dobalian, A. (2020). Trends and best practices in health care cybersecurity insurance policy. Journal of Healthcare Risk Management, pp. 1-5. doi:10.1002/jhrm.21414.

Kessler, S. R., Pindek, S., Kleinman, G., Andel, S. A., & Spector, P. E. (2019). Information security climate and the assessment of information security risk among healthcare employees. Health informatics Journal. doi:10.1177/1460458219832048.

Kharraz, A., Robertson , W., & Kirda, E. (2018). Protecting against Ransomware: A New Line of Research or Restating Classic Ideas? IEEE Security and Privacy, 16, 103-107. doi:10.1109/MSP.2018.2701165.

King, F., Klonoff, D. C., Kerr, D., Hu, J., Lyles, C., Quinn, C., . . . Gabbay, R. (2018). Digital Diabetes Congress 2018. Journal of Diabetes Science and Technology, 1231-1238. doi:10.1177/1932296818805632.

Koppel, R., & Kuziemsky, C. (2019). Healthcare data are remarkably vulnerable to hacking: Connected healthcare delivery increases the risks. Studies in Health Technology and Informatics, 218-222. doi:10.3233/978-1-61499-951-5-218.

Kruse, C. S., Frederick , B., Jacobson , T., & Monticone , K. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends. Technology and Health Care, 25, 1-10. doi:10.3233/THC-161263.

Kuerbis, B., & Badiei, F. (2017). Mapping the cybersecurity institutional landscape. Australian Catholic University, 19, 466-492. doi:10.1108/DPRG-05-2017-0024.

Kure, H. I., Islam, S., & Razzaque, M. A. (2018). An integrated cyber security risk management approach for a cyber-physical system. Applied Sciences (Switzerland). doi:10.3390/app8060898.

Lebeda, F. J., Zalatoris, J. J., & Scheerer, J. B. (2018). Government Cloud Computing Policies: Potential Opportunities for Advancing Military Biomedical Research. MILITARY MEDICINE, 183, 438-447. doi:10.1093/milmed/usx114.

Lechler, T., & Wetzel, S. (2017). Conceptualizing the silent risk of inadvertent information leakages. Computers and Electrical Engineering, 67-75. doi:10.1016/j.compeleceng.2016.12.020.

Leung, K., Clark, C., Sakal, M., Friesen, M., & Strudwick, G. (2019). Patient and family member readiness, needs, and perceptions of a mental health patient portal: A mixed methods study. Studies in Health Technology and Informatics, 266-270. doi:10.3233/978-1-61499-951-5-266.

Loi, M., Christen, M., Kleine, N., & Weber, K. (2019). Cybersecurity in health –disentangling value tensions. Journal of Information, Communication and Ethics in Society, 229-245. doi:10.1108/JICES-12-2018-0095.

Maimó, L. F., Celdrán, A. H., Gómez, Á. L., Clemente, F. J., Weimer, J., & Lee, I. (2019). Intelligent and dynamic ransomware spread detection and mitigation in integrated clinical environments. Sensors (Switzerland). doi:10.3390/s19051114.

Martin, G., Martin , P., Hankin , C., Darzi , A., & Kinross , J. (2017). Cybersecurity and healthcare: How safe are we? BMJ (Online). doi:10.1136/bmj.j3179.

Mostfa Kamal, S. U., Abd Ali, R. J., Alani, H. K., & Abdulmajed, E. S. (2016). Survey and brief history on malware in network security case study: Viruses, worms and bots. ARPN Journal of Engineering and Applied Sciences, 683-698.

Natsiavas, P., Rasmussen, J., Voss-Knude, M., Votis, K., Coppolino, L., Cano, I., . . . Nalin, M. (2018). Comprehensive user requirements engineering methodology for secure and

interoperable health data exchange. BMC Medical Informatics and Decision Making, 18 n.1. doi:10.1186/s12911-018-0664-0.

Okereafor, K., & Marcelo, A. (2020). Addressing Cybersecurity Challenges Of Health Data In The Covid-19 Pandemic. International Journal in IT & Engineering (IJITE), 8 n.6, pp. 1-12. Fonte: http://ijmr.net.in.

Ondiege, B., Clarke, M., & Mapp, G. (2017). Exploring a new security framework for remote patient monitoring devices. Computers, 6 n.1. doi:10.3390/computers6010011.

Pesapane, F., Volonté, C., Codari, M., & Sardanelli, F. (2018). Artificial intelligence as a medical device in radiology: ethical and regulatory issues in Europe and the United States. Insights into Imaging. doi:10.1007/s13244-018-0645-y.

PMI, P. M. (2017). Project Management Body of Knowledge -PMBOK. Global Standard.

Priestman, W., Anstis, T., Sebire, I. G., Sridharan, S., & Sebire, N. J. (2019). Phishing in healthcare organisations: threats, mitigation and approaches. BMJ Health & Care Informatics, 26, e100031. doi:10.1136/bmjhci-2019-100031.

Primo, H., Bishop, M., Lannum, L., Cram, D., Nader, A., & Boodoo, R. (2018). 10 Steps to Strategically Build and Implement your Enterprise Imaging System: HIMSS-SIIM Collaborative White Paper. Journal of Digital Imaging, 32, 535-543. doi:10.1007/s10278-019-00236-w.

Silva F., J. C., Braga, C. S., & Reboucas, S. M. (2016). Perception of the brazilian manufacturing industry about the main barriers to innovation. International journal of innovation, v. 5 n.1, p. 114-131, 2016. doi 10.5585/iji.v5i1.114.

Shneiderman, B., & Plaisant, C. (2015). Sharpening analytic focus to cope with big data volume and variety. IEEE Computer Graphics and Applications. doi:10.1109/MCG.2015.64.

Stern, A. D., Gordon, W. J., Landman, A. B., & Kramer, D. B. (2019). Cybersecurity features of digital medical devices: An analysis of FDA product summaries. BMJ Open, 9 n.6. doi:10.1136/bmjopen-2018-025374.

Swede, M. J., Scovetta, V., & Eugene-Colin, M. (2019). Protecting patient data is the new scope of practice: A recommended cybersecurity curricula for healthcare students to prepare for this challenge. Journal of Allied Health, 48 n.2, pp. 148-155. doi:PubMed ID: 31167018.

Thomé, A. M., Scavarda, L. F., Scavarda, A., & Thomé, F. E. (2016). Similarities and contrasts of complexity, uncertainty, risks, and. International Journal of Project Management, 1328-1346. doi:10.1016/j.ijproman.2015.10.012.

Van Eck, N. J., & Waltman, L. (2010). Software survey: VOSviewer, a computer program for bibliometric mapping. Scientometrics 84, 523–538. Scientometrics. doi:10.1007/s11192-009-0146-3.

Vecchione, L., Stintzing, S., Pentheroudakis, G., Douillard, J.-Y., & Lordick, F. (2020). ESMO management and treatment adapted recommendations in the COVID-19 era: colorectal cancer. Esmo Open. doi:10.1136/esmoopen-2020-000826.

Ward, s., & Chapman, C. (2008). Stakeholders and uncertainty management in projects. Construction Management and Economics, 26, 563-577. doi:10.1080/01446190801998708.

Wethington, E., Eccleston, C., Gooberman-Hill, R., Schofield, P. A., Bacon, E., Dombrowski, W., . . . Reid, M. C. (2018). Establishing a Research Agenda on Mobile Health Technologies and Later-Life Pain Using an Evidence-Based Consensus Workshop Approach. Journal of Pain, 1416-1423. doi:10.1016/j.jpain.2018.06.006.

Wiltz, C. (07 de April de 2014). Medical Device and Diagnostic Industry. Fonte: MD+DI Qmed: https://www.mddionline.com/report-healthcare-cybersecurity-appalling-legislation-not-enough.

World Economic Forum. (Janeiro de 2017). The Global Risks Report 2017. Fonte: World Economic Forum: https://www.weforum.org/reports/the-global-risks-report-2017.

Zhang, X., Tan, Y.-a., Xue, Y., Zhang, Q., Li, Y., Zhang, C., & Zheng, J. (2017). Cryptographic key protection against FROST for mobile devices. Cluster Comput, 2393-2402. doi:10.1007/s10586-016-0721-3.

Appendix 1 – Group of co-citation authors

Author	Citation	Power Link	Group
Perritt jr., H.I	10	900	1
Bergeron, M.(	8	168	1
Bamberger, K.	6	564	1
Bissonnette, I	6	138	1
Shahzad, B.	6	72	1
Kruse, C.S.	5	82	1
Lee, I.	5	50	1
Williams, P.A	5	38	1
Woodward, A.	5	66	1
Harter, P.J.	28	2016	2
Soyata, T.	21	965	2
Walker D. Holle	19	1539	2
Kantarci, B.	12	672	2
Coglianese, C	11	979	2
Thaw, D.	11	979	2
Zhang, Y.	7	223	2
Habibzadeh, M	6	372	2
Reid, M.C.	6	24	2
Reiss, D.R.	6	564	2
Kocabas, O.	5	261	2
Li, H.	5	273	2
Li, Z.	5	146	2
Zhou, J.	5	160	2
Fu, K.	7	34	3
Kramer, D.B	7	34	3
Kundra, V.	7	14	3
Gordon, W.J	5	18	3
Mansfield-Devir	5	16	3
Baxter, L.G.	5	475	3