Engineering Assignment Coversheet

Please note that you:

- Must keep a full copy of your submission for this assignment
- Must staple this assignment
- Must NOT use binders or plastic folders except for large assignments

Student Number(s)

992038, 1144272, 825960, 964360, 962496

Group Code (if applicable): Group 33

Assignment Title:	Addressing Cybersecurity in Healthcare Organizations from an Architectural Perspective
Subject Number:	ISYS90043
Subject Name:	Enterprise Applications & Architectures
Student Name:	Diego Aranda Villarreal, Clark Zhu, Yushi Zhao, Jiayi Xie, Xuemei Tu
Lecturer/Tutor:	Dr. Rod Dilnutt/Leila Meratian
Due Date:	16th October, 2020

For Late Assignments Only

Has an extension been granted? Yes / No (circle)

A per-day late penalty may apply if you submit this assignment after the due date/extension. Please check with your Department/coordinator for further information.

Plagiarism

Plagiarism is the act of representing as one's own original work the creative works of another, without appropriate acknowledgment of the author or source.

Collusion

Collusion is the presentation by a student of an assignment as his or her own which is in fact the result in whole or in part of unauthorised collaboration with another person or persons. Collusion involves the cooperation of two or more students in plagiarism or other forms of academic misconduct.

Both collusion and plagiarism can occur in group work. For examples of plagiarism, collusion and academic misconduct in group work please see the University's policy on Academic Honesty and Plagiarism: http://academichonesty.unimelb.edu.au/

Plagiarism and collusion constitute cheating. Disciplinary action will be taken against students who engage in plagiarism and collusion as outlined in University policy. Proven involvement in plagiarism or collusion may be recorded on my academic file in accordance with Statute 13.1.18.

STUDENT DECLARATION

Please sign below to indicate that you understand the following statements:

I declare that:

- This assignment is my own original work, except where I have appropriately cited the original source.
- This assignment has not previously been submitted for assessment in this or any other subject.

For the purposes of assessment, I give the assessor of this assignment the permission to:

- Reproduce this assignment and provide a copy to another member of staff; and
- Take steps to authenticate the assignment, including communicating a copy of this assignment to a checking service (which may retain a copy of the assignment on its database for future plagiarism checking).

Student signature …Diego, Clark, Yushi, Jiayi, Xuemei…… Date ……07/10/2020……

Table of Contents

Addressing Cybersecurity in Healthcare Organizations from an Architectural Perspective

Clark Zhu
The University of Melbourne
1144272
lezhu1@student.unimelb.edu.au

Diego Aranda Villarreal
The University of Melbourne
992038
darandavilla@student.unimelb.edu.au

Jiayi Xie
The University of Melbourne
964360
jxxie1@student.unimelb.edu.au

Xuemei Tu
The University of Melbourne
962496
xuemeit@student.unimelb.edu.au

Yushi Zhao
The University of Melbourne
825960
yushiz@student.unimelb.edu.au

Abstract

The rapid development of technology and the increased digitization of healthcare organizations have not only prompted the healthcare system more convenient and economical but have also led to more cybersecurity issues. The healthcare industry is one of the most vulnerable sectors in the world in terms of cyberattacks, resulting in the breakdown of medical devices and the compromise of patient health records. Although regulators have recognized the magnitude of the problem, research on the subject is still in its infancy. As Enterprise Architecture (EA) enables healthcare organizations to effectively integrate IT and healthcare resources, improve strategic alignment and reduce risk, this article focuses on how healthcare organizations can address cybersecurity issues from an EA perspective. First of all, it will introduce the importance of EA in healthcare organizations and the three layers based on the TOGAF framework, including Hospital Service Layer, Application and Data Layer and Technology Infrastructure Layer. Then, this article will explain the evolution of cybersecurity and the issues of cybersecurity in the healthcare industry. After that, four cases of cyber-attacks and the resulting software and device failures that harmed organizations and patients are exhibited. The internal factors leading to these issues are mainly related to the lack of cyber-security awareness and interoperability, as well as network security issues. Finally, based on these challenges, recommendations for the healthcare organization architecture will be presented.

1 Introduction

Concerns have been increasing in the past few years regarding cybersecurity threats in healthcare environments. The rise of eHealth systems for healthcare has been driven by the growing use of IoT (Internet of Things) devices, in particular, wireless sensor technologies. In this case, the aim is to enhance the monitoring, diagnosis, and treatment of patients being cared for in hospital facilities. Such applications have been progressively integrated with traditional healthcare technologies over time (Xu et al. 2014).

The current scenario for the eHealth systems may include several hospital processes that range from managing patient information, admission services, remote monitoring of patients, supervising the administration of drugs, medical equipment, and health-worker management, among others (Miorandi et al. 2012). In traditional health working environments, data management may be a mix of manual and semi-automated activities, which could result in information asymmetries among

different departments that often need to treat the same patients. The introduction of novel technologies in the hospital's ICT infrastructure has led health workers to have the opportunity to break the barriers among different levels within the Enterprise Architecture (EA), allowing workers to access data seamlessly and ubiquitously through various devices, thus improving the patient's care process (Lu & Xu 2019). However, advanced medical equipment might be subject to vulnerabilities due to their openness nature. Various malicious cyber-attacks might target the core principles of information security, namely, confidentiality, integrity, and availability (CIA) of patients and health workers' data (Whitman & Mattord 2010). Therefore, the cybersecurity issues related to these technologies need to be addressed by health organizations in a holistic manner to maintain the safety of the patients and the privacy of their data, as attackers might find patient's records to be of high value (Omoogun 2017).

Thus, the question that this article addresses is: *How can healthcare organizations address cybersecurity issues from an EA perspective?*

2 An Architectural Perspective for Healthcare Organizations

2.1 The Importance of EA in Healthcare Organizations

Healthcare organizations have been growing in technological complexity and capabilities along with the rise of IoT developments for healthcare, thus increasing the number of structural components to be managed. Thus, a broad view of the healthcare organization is needed, and a structure that aligns IT and business views is required for managing technical and organizational components. Hence, EA can be considered as a tool that may allow the healthcare organizations to integrate their IT resources and medical services effectively, while benefiting from EA's "integration, systemic regulation, reusability, decision support, risk reduction and strategy alignment" capabilities (Ahsan, Sha & Kingston 2010; Sajid & Ahsan 2016).

2.2 A TOGAF-based EA for Healthcare Organizations' Operations

TOGAF has been widely used as an EA framework for representing highly complex business environments by adding flexibility for other frameworks to be embedded within it. Thus, each organization may be able to construct its own specific EA. One key component of TOGAF is the Architecture Development Method, with which the healthcare organization can start a process for aligning IT and business needs in a cyclical manner. Thus, all stakeholders can hold a common understanding of the components once the process is finished. Moreover, the Foundation Architecture aspect allows the healthcare organization to represent their as-is architecture as a base for building their to-be architecture in the future (The Open Group 2001; Sajid & Ahsan 2016).

A TOGAF-based EA for the healthcare organization is provided by Ahsan, Sha, and Kingston (2010), where they used Archimate, a graphical description language for visualizing TOGAF components and their interactions. As seen in Figure 1, the healthcare organization as-is architecture can be represented by three layers, each layer supporting the above functionalities: Hospital Service Layer, Application and Data Layer, and Technology Layer.

The Hospital Service Layer focuses on the health worker-patient interaction, and also the interaction of both with the Application Layer. Firstly, this layer contains the logic and rules that define the clinical information along with its value and meaning. Secondly, it holds the patient care processes and interactions, such as admissions, diagnosis, drug management, emergency, and hospitalization care among other common services. Thirdly, it incorporates the hospital organizational structure, including roles and responsibilities, and administrative processes (Ahsan, Sha & Kingston 2010).

All services in the Hospital Service Layer are connected to the Application Layer, which contains two domains. Firstly, the data domain holds the patients' health records along with data generated from applications, such as patient profiles, and data flows from medicare devices, such as temperature, blood pressure, among others. Secondly, the application domain offers an interface for the Hospital Service Layer to interact with information systems. Valuable data may be created from applications related to patient movements, evolution, and interactions with medical staff along with aggregated data from administrative support functions (Ahsan, Sha & Kingston 2010; Velasco et al. 2016).

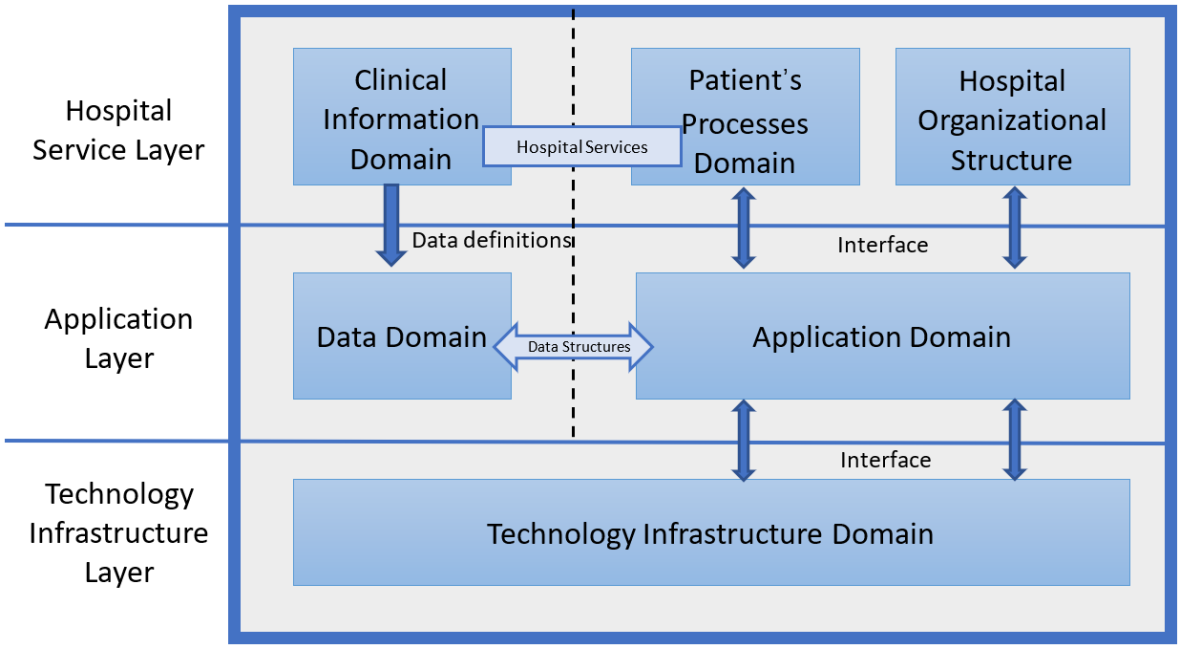

Figure 1: As-is Healthcare Organization Architecture

The Technology Layer acts as the technological infrastructure that supports the Application Layer. This layer defines how technical components interact and how they should be deployed for maintaining interoperability among medical devices and information systems. Moreover, it includes traditional infrastructure such as network systems, workstations, and physical access control, alongside traditional medical equipment to capture data from patients. Furthermore, it can include advanced IoT-based technologies, such as wearable and mobile-based devices (Ahsan, Sha & Kingston 2010; Islam et al. 2015).

3 Cybersecurity landscape in healthcare

3.1 Evolution of Cybersecurity

Cybersecurity emerged by the end of the 1970s, and it refers to the collection of organizations, resources, processes, and structures that can protect the information systems linked to the company's network from physical damage, leakage of information, and other related incidents that might put the company's interests at risk (Craigen et al. 2014).

The expansion of cyberspace has been growing to an extent where cybersecurity measures might not be sufficient to face multidimensional and highly complex cyber-attacks. Nowadays, as companies have been increasingly relying on IoT and cloud computing technologies to store and manage high

volumes of data, the probability and impact of cyber-attacks have also incremented to a considerable degree (Cabaj et al. 2018). For instance, an advanced cyber-espionage malware called Red October targeted worldwide diplomatic and governmental agencies for five years, and it was captured by 2013 (Taddeo 2017). By 2017, Equifax suffered from a data leakage that affected nearly 147 million customers, which made the company lose around $250 million US dollars (Kuhn 2018). Thus, the need for cybersecurity has been increasing due to the high impact on individuals and organizations.

3.2 Cybersecurity in the Healthcare Industry

In recent years, advanced technologies have been increasingly integrated into the healthcare sector, resulting in healthcare systems with improved flexibility, accessibility, and cost-effectiveness (Yang et al. 2011). However, since the cybersecurity measures in the healthcare sector might not be as mature as others, it has become one of the most targeted industries in the global cyber-attack scenario. The frequency of data breaches in the healthcare industry has been on the rise since 2010, where around 94% of healthcare organizations have been victims of cyberattacks and an estimated 150 million patients' health records having been compromised (Williams & Woodward 2015; Berger 2016).

The digitalization trend has led many healthcare organizations to store medical records and wearable health devices data in the cloud. This interconnection of numerous devices might raise several cybersecurity issues. Furthermore, the abundance of the data generated by medical care processes and devices is considered to be a key vulnerability for numerous data breaches. Healthcare organizations often have a wealth of sensitive data, including names, dates of birth, insurance numbers, credit cards, and even past medical records. Whether used for extortion or trafficking, this data may be more valuable than that from other industries (Argaw et al. 2020; Bhuyan et al. 2020).

Cybersecurity issues have caused severe financial and reputational damage to healthcare organizations, such as extortion software that might bring down the system and delay urgent care (Bhuyan et al. 2020). Unfortunately, while the bank card or mobile phone information can be changed, health data cannot (Offner et al. 2020). Therefore, patients' confidentiality is at risk when private data is compromised and corrupted (Coventry & Branley 2018).

As incident reports have been notified more and more, academia has acknowledged the magnitude and urgency of the problem. However, research on this topic is still in its infancy. Cybersecurity protection is not just a technical issue; the broader healthcare environment requires a comprehensive healthcare system architecture coordinated across the three layers of healthcare service delivery, application, and technology infrastructure (Williams & Woodward 2015).

4 Cases of Study

As digitization transforms into a pervasive technology in the healthcare industry, hackers are exploring and attempting various approaches to benefit from the artefacts of digitization. In 2019, the Michigan-based Brookside ENT and Hearing Center experienced a Ransomware attack where their computers were shut down and would not turn on. As a result of refusing to pay the ransom of $6,500 to the hackers, their whole system’s files were erased, and the practice had to shut down as they lost all the necessary data to operate (Hepp 2019).

While ransomware attacks leverage loopholes of applications, the medical devices might also be threatened by cyber-attacks. In October 2016, a major eHealth device maker Animas warned that their OneTouch insulin pump was susceptible to hacking (Mello 2016). According to Ratliff, an electrical engineer at HIS Markit, reverse-engineering the unencrypted protocol on the insulin pump

was not a difficult task. The consequence of an attack on the insulin pump could be physical damage to the diabetic patients due to overdose (Finkle 2016).

Further to the security weaknesses in hardware and applications, people might also be the common target that hackers rely on to open the backdoor by Phishing attacks. In early October 2013, one of the computers in University of Washington Medicine in Seattle were taken control of by hackers due to an employee opening an email attachment that contained malware. The data stored in the computer was patient information including patient names, medical record numbers, and dates of service. The incident was identified and handled by the organization and reported to the FBI in the next day (Donohue 2013).

Internal security deficiency can often be the root cause of the cyber-security issue. In March 2019, a California-based company that develops HER software configured its fax servers unencrypted without a password (Whittaker 2019). Consequently, as the company heavily relied on fax transmission to share patient files to other providers and pharmacies, anyone could read the transmitted faxes containing medical records, doctor's notes, prescription details, and critical personal information of patients (Whittaker 2019).

4.1 Financial Incentive for Cyber-attacks

In March 2019, there was averagely one data breach reported in healthcare each day (HIPAA Journal 2019). There might be a wide range of impacts on the healthcare organization, including financial loss, business shutting down, and eroded trust towards patients (Symantec Corporation 2014).

The illegal financial benefits that could be extracted from systems, and sensitive data that helps open backdoors of more people and organizations might be the major factors leading to the cyber-attacks. According to a report issued by the Institute for Critical Infrastructure Technology (2016), after the data breach at the University of Pittsburgh Medical Center in 2015, the Personal Identifiable Information was traded and used in the black market to fake income taxes for employees to collect their returns. Additionally, the stolen Private Health Information was then combined with the personal information breached in the Office of Personnel Management to perform more targeted attacks with social engineering skills (ICIT p6).

5 Cyber-attacks Impacts in Healthcare Organizations

The high complexity of technological devices within the health organization architecture and the openness characteristic of IoT and wireless medical devices have raised concerns regarding the CIA of health data (Lu & Xu 2019; Liveri et al. 2015).

As health organizations incorporate advanced technological assets into their critical infrastructure, they might increase the probability of information security incidents. This can be related to the massive volume of valuable data, the lack of interoperability between technologies, the poor security awareness of health workers, and the inadequate implementation of security controls. These are major security challenges for health organizations to keep their architectural layers and patients safe from a wide range of risks (Liveri et al. 2015).

In order to categorize the cyber-attacks implications on health care organizations and their critical technological assets, Liveri et al. (2015) proposed an analysis that classifies the various threats, vulnerabilities, and risks which are important for these institutions given the increasing introduction of pervasive systems.

Threats can be related to objects or entities that represent a current danger to the health organization's IT assets (Whitman & Mattord 2010). "Malicious actions" are referred to as external agent cyberattacks. "Human errors" are related to IT asset misconfigurations, unauthorized access, and non-compliant behavior by stakeholders. Other threats may come from internal software, hardware, and network "System failures," flaws by third party's dependencies as "Supply chain failure" and unexpected "Natural phenomena" (Liveri et al. 2015).

Vulnerabilities can be referred to as the weaknesses that threat entities or objects might exploit to conduct cyber-attacks on the health organization's IT assets (Whitman & Mattord 2010). From the technical side, a high level of wireless interconnections, a high dispersion of devices around the physical domain, a lack of threat-avoidance based design for applications, a high homogeneity and long lifespan of equipment, and a lack of prevention and detection capabilities are considered as main threats. From an organizational perspective, the rise of IoT devices has brought threats to policies and standards for authentication and authorization, and IT asset configuration. Moreover, there might be poor training for managing incidents and unaware medical staff bypassing security measures (Liveri et al. 2015).

Risks may be viewed as the negative impacts on healthcare organizations resulting from the exploitation of their IT assets' vulnerabilities by threat entities or objects (Whitman & Mattord 2010). Risks can be closely related to transgressions of the CIA triad, compliance and network violations, and interoperability issues due to poor standardization. Moreover, as incidents might end up putting the patient's safety at risk, reputational damage and financial loss might also occur (Liveri et al. 2015).

A summary of the threats, vulnerabilities, and risks evaluation is provided below (Table 1), according to Ahsan, Shah & Kingston (2010), healthcare organization architecture, where the three layers are contrasted with Liveri et al. (2015) assessment.

Table 1: Cyber-attacks impacts in healthcare organization enterprise architecture

		Threats	**Vulnerabilities**	**Risks**
Healthcare Organization Layers	**Service Layer**	Human errors Insider threats	High dependence on IoT to work Lack of technological expertise Poor security incident training Security measures being bypassed Poor authorization/authentication measures	Reputational damage Patient's safety risks Compliance and trust violations Financial loss
	Application and Data Layer	Supply chain failure Malicious actions	Lack of security-based design Lack of prevention and detection capabilities	Patient's data loss Patient's data integrity violation Confidentiality violation Unauthorized access
	Technology Infrastructure Layer	Natural phenomena System failures	Wireless interconnectivity Dispersion of devices Homogeneity of devices Long life span of infrastructure Poor standards for configuration	Network security violations Loss of availability of systems Lack of interoperability Lack of standardization

6 Discussion on Cybersecurity Challenges for Healthcare Organizations

The reasoning from Section 5 raises three key concerns to be further analyzed. The following challenges might affect the three layers of the healthcare organization architecture directly or indirectly.

6.1 Lack of interoperability

There are several systems and applications interconnected at different layers of the infrastructure of healthcare organizations, and a lack of interoperability might affect secure data transmission between layers. A correct configuration of medical systems is key for healthcare organizations' interoperability to be effective. Thus, once hardware and software vendors release their latest versions, it is essential for healthcare organizations to keep up with the updating processes. A similar approach should be attained when acquiring new IT assets. Moreover, if misconfigurations affect the Technology Layer, that might disturb the availability and security of systems in the Application Layer, therefore, inducing the Hospital Service Layer to commit errors and menacing the quality of the service. Hence, a lack of interoperability might expose the layers to security threats (Liveri et al. 2015).

6.2 Lack of network security measures

The amount of medical equipment has been increasing greatly in the past years given the rise of IoT and mobile working environments. Although these devices can ease the health workers' job, the security of the network infrastructure might become a challenge based on the openness attributes of such devices. In addition, this has led cyber-attacks to grow in number, for which cybersecurity measures related to prevention and detection of incidents become crucial as the whole Technology Layer depends on the network. Moreover, healthcare organizations might be suffering from defective guidelines for selecting, deploying, and securing the network infrastructure, as well as constantly defending the network from cyber-attacks. As network breaches can impact the Technology Layer, availability of systems from the Application Layer might be impacted as well, thus leading to the Hospital Service Layer to have operational inefficiencies (Liveri et al. 2015).

6.3 Lack of security awareness and training

One key aspect of cybersecurity in healthcare organizations is health workers, which in some cases might open the door to threats as they might not be aware of how to detect or prevent cyber-attacks. A lack of awareness and training on cybersecurity might easily leave hospitals vulnerable to ransomware or phishing attacks, as health workers can be the easiest way for hackers to get access to networks, systems, and other IT assets. Moreover, security awareness is closely related to the interactions between Hospital Service Layer and Application Layer, as health workers constantly use medical applications for patient care processes. Malicious access to the Application Layer can be given by unaware and poorly trained medical staff, and their misuse of medical applications, thus leading the patient's data confidentiality and integrity to be at risk. Moreover, they might give access to networked medical devices, which might jeopardize the availability of systems (Mayol et al. 2016).

7 An Architectural Perspective for Building Cybersecurity for Healthcare Organizations

As stated by the challenges presented above, cybersecurity incidents might generate a chain of high-risk events throughout different layers of healthcare architecture. Therefore, a holistic approach should be considered for building cybersecurity capabilities and for promoting cybersecurity culture (Offner et al. 2020).

Several authors have proposed a cross-layered approach for improving cybersecurity in healthcare organizations by putting the focus on the technical side (Velasco et al. 2016; Islam et al. 2015; Manogaran et al. 2018). For this reason, a crosswise viewpoint can be established for defining the security requirements, so the cybersecurity technical capabilities are ensured at each layer (Offner et al. 2020). Moreover, organizational settings should be set across the architecture, which may conduct health workers' behavior towards cybersecurity awareness (Bhuyan et al. 2020). Both of these schemes can be related to "technical measures" and "organizational measures," respectively, as proposed by Mayol et al. (2016) in their recommendations for the cybersecurity and resilience of the European Union's health organizations.

Hence, we propose a cross-layered model that includes both technical and organizational perspectives coupled with the healthcare organization architecture, as shown in Figure 2 (Offner et al. 2020; Mayol et al. 2016; Sajid & Ashan 2010).

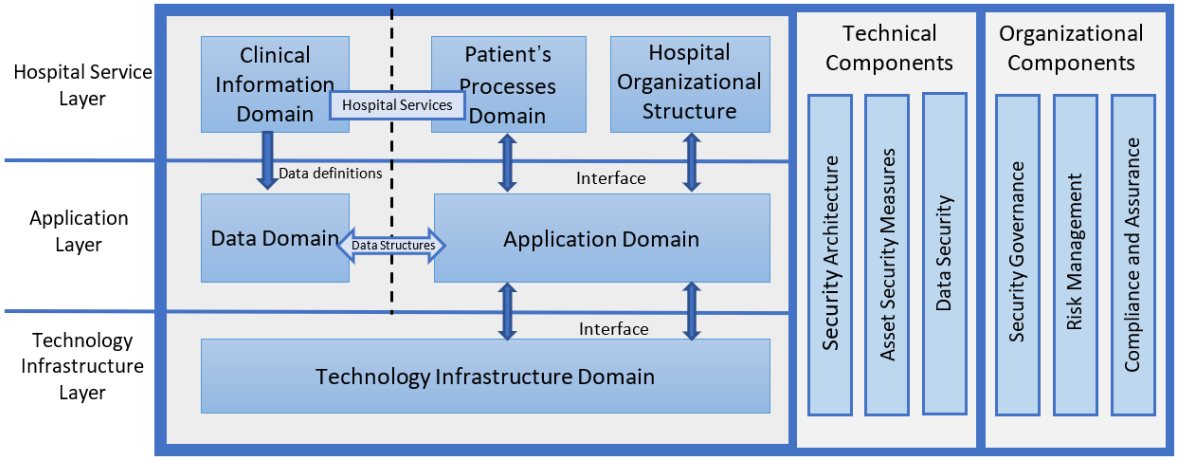

Figure 2: Cross-layered Healthcare Organization Architecture for Cybersecurity

7.1 Technical Best Practices

The technical view may be crucial for the healthcare organization to define technical security capabilities across the whole architecture, and also for providing the Hospital Service Layer with complete, correct, and timely information (Offner et al. 2020). Firstly, with regards to the “security architecture," intrusion detection and prevention systems are needed to manage potential incidents, along with firewalls and malware protection to defend the network. Moreover, the use of periodic backups becomes essential to recover from ransomware or medical device hacking attacks. Secondly, IT assets need to be protected by periodically installing patches and updates of systems, and also by enforcing the controls for accessing systems and technology infrastructure. Moreover, a strict policy for asset configuration would be required to maintain the interoperability among medical devices. Thirdly, in regard to the security of data, encryption is considered indispensable to handle the confidentiality of data and also the levels of authority for the stakeholders to use applications (Mayol et al. 2016).

7.2 Organizational Best Practices

The organizational perspective may be key for cyber-security awareness to be leveraged by the organization across all of its layers. Thus, stakeholders can be aligned towards a common cybersecurity culture where potential attacks such as phishing or ransomware may be prevented. (Offner et al. 2020). Firstly, in relation to “security governance," a clear definition of roles and

responsibilities related to security should be set and aligned with the patient's safety, so the Hospital Service Layer is aligned to the technical layers. Moreover, policies and procedures related to security should be established to conduct the behavior of health workers, and also for setting the necessary training and awareness programs to enforce it. Secondly, in regard to “risk management," the identification of threats, vulnerabilities, and risks should be periodically conducted according to a risk management plan. Furthermore, a contingency plan is to be in place when the healthcare organization is under attack, such that key stakeholders are contacted expeditiously to recover the system’s operations. Thirdly, with respect to “compliance and assurance”, standards should be adopted to comply with industry security best practices, and also procurement of technology should be strictly ruled through policies and contracts with technology suppliers (Mayol et al. 2016).

Conclusion

While the pervasive digitized technology has gained popularity in the healthcare industry, it has also largely increased the complexity of its IT landscape. Meanwhile, the healthcare industry is suffering from various cybersecurity threats more frequently than other sectors of economy (Ponemon Institute LLC 2016). We performed our analysis of the healthcare organization from an architectural view, and we identified three major gaps in the current healthcare organization architecture which are: insufficient cybersecurity awareness among people, lack of interoperability among systems and devices, and unsound network security configuration. The contribution of this paper is that we provided an improved architectural solution to address the cybersecurity issues in the current healthcare industry. We recommended a holistic cross-layered architectural solution comprising technical and organizational components. By following these guidelines, healthcare organizations can build cybersecurity capabilities and resilience into the current architecture comprehensively.

References

Ahsan, K, Shah, H & Kingston, P 2010, 'Healthcare Modelling through Enterprise Architecture: A Hospital Case', *2010 Seventh International Conference on Information Technology: New Generations, Information Technology: New Generations (ITNG), 2010 Seventh International Conference on,* pp. 460–465, viewed 5 October 2020, <https://search.ebscohost.com/login.aspx?direct=true&AuthType=sso&db=edseee&AN=edseee.5501732&site=eds-live&scope=site>.

Argaw, ST, Troncoso-Pastoriza, JR, Lacey, D, Florin, M-V, Calcavecchia, F, Anderson, D, Burleson, W, Vogel, J-M, O, LC, Eshaya-Chauvin, B & Flahault, A 2020, 'Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks', *BMC Medical Informatics and Decision Making*, vol. 20, no. 1, viewed 5 October 2020, <https://search.ebscohost.com/login.aspx?direct=true&AuthType=sso&db=edssjs&AN=edssjs.F5FA43DF&site=eds-live&scope=site>.

Berger, DW 2016, 'Breach Report 2015: protected health information (PHI)', *Redspin*.

Bhuyan, SS, Kabir, UY, Escareno, JM, Ector, K, Palakodeti, S, Wyant, D, Kumar, S, Levy, M, Kedia, S, Dasgupta, D & Dobalian, A 2020, 'Transforming Healthcare Cybersecurity from Reactive to Proactive: Current Status and Future Recommendations', *Journal of Medical Systems*, vol. 44, no. 5, viewed 5 October 2020, <https://search.ebscohost.com/login.aspx?direct=true&AuthType=sso&db=edssjs&AN=edssjs.D801E245&site=eds-live&scope=site>.

Cabaj, K, Domingos, D, Kotulski, Z & Respício, A 2018, 'Cybersecurity education: Evolution of the discipline and analysis of master programs', *Computers & Security*, vol. 75, pp. 24–35, viewed 5 October 2020, <https://search.ebscohost.com/login.aspx?direct=true&AuthType=sso&db=edselp&AN=S0167404818300373&site=eds-live&scope=site>.

Coventry, L & Branley, D 2018, 'Cybersecurity in healthcare: A narrative review of trends, threats and ways forward', *Maturitas*, vol. 113, pp. 48–52, viewed 5 October 2020, <https://search.ebscohost.com/login.aspx?direct=true&AuthType=sso&db=edselp&AN=S0378512218301658&site=eds-live&scope=site>.

Craigen, D, Diakun-Thibault, N & Purse, R 2014, 'Defining cybersecurity', *Technology Innovation Management Review*, vol. 4, no. 10, viewed 5 October 2020, <https://timreview.ca/article/835>.

Donohue, B 2013, 'University of Washington Medicine Spills Patient Data', *Threat Post*, viewed 5 October 2020, <https://threatpost.com/university-of-washington-medicine-spills-patient-data/103060/>.

Drees, J 2019, 'Michigan medical practice to close after refusing to pay ransom to hackers', *Becker's Healthcare*, viewed 5 October 2020, <https://www.beckershospitalreview.com/cybersecurity/michigan-medical-practice-to-close-after-refusing-to-pay-ransom-to-hackers.html>.

ENISA ─ European Union Agency for Network and Information Security, Dimitra Liveri, Anna Sarri & Christina Skouloudi 2015, 'Security and resilience in eHealth: Security challenges and risks', viewed 5 October 2020, <https://search.ebscohost.com/login.aspx?direct=true&AuthType=sso&db=edseub&AN=edseub.TP.04.15.824.EN.N&site=eds-live&scope=site>.

ENISA 2016, 'Smart hospitals', *Heraklion*, viewed 5 October 2020, <https://www.enisa.europa.eu/publications/cyber-security-and-resilience-for-smart-hospitals>.

Finkle, J 2016, 'J&J warns diabetic patients: Insulin pump vulnerable to hacking', *Reuters*, viewed 5 October 2020, <https://www.reuters.com/article/us-johnson-johnson-cyber-insulin-pumps-e-idUSKCN12411L>.

John, P & Mello, JR 2016, 'Insulin Pump Susceptible to Hacking', *TechNewsWorld*, viewed 5 October 2020, <https://www.technewsworld.com/story/83969.html>.

Hacking Healthcare IT in 2016 2016, Institute for Critical Infrastructure Technology, viewed 5 October 2020, <https://icitech.org/wp-content/uploads/2016/01/ICIT-Brief-Hacking-Healthcare-IT-in-2016.pdf>.

Hepp, B 2019, 'Hackers held patient files at a Battle Creek doctor's office for ransom. The office didn't pay. It closed', *Battle Creek Enquirer*, viewed 5 October 2020, <https://www.battlecreekenquirer.com/story/news/local/2019/08/22/ransomware-attack-john-bizon-william-scalf-medical-practice/2062806001/>.

HIPAA Journal 2019, 'March 2019 Healthcare Data Breach Report', viewed 5 October 2020, <https://www.hipaajournal.com/march-2019-healthcare-data-breach-report/>.

Islam, SMR, Kwak, D, Kabir, MH, Hossain, M & Kwak, K-S 2015, 'The Internet of Things for Health Care: A Comprehensive Survey', *IEEE ACCESS*, vol. 3, pp. 678–708, viewed 5 October 2020, <https://search.ebscohost.com/login.aspx?direct=true&AuthType=sso&db=edswsc&AN=000371388200050&site=eds-live&scope=site>.

Kuhn, ML 2018, '147 Million Social Security Numbers for Sale: Developing Data Protection Legislation after Mass Cybersecurity Breaches', *Iowa Law Review*, vol. 104, no. 1, pp. 417–446, viewed 5 October 2020, <https://search.ebscohost.com/login.aspx?direct=true&AuthType=sso&db=edshol&AN=edshol.hein.journals.ilr104.14&site=eds-live&scope=site>.

Lu, Y & Xu, LD n.d., 'Internet of Things (IoT) Cybersecurity Research: A Review of Current Research Topics', *IEEE INTERNET OF THINGS JOURNAL*, vol. 6, no. 2, pp. 2103–2115, viewed 5 October 2020, <https://search.ebscohost.com/login.aspx?direct=true&AuthType=sso&db=edswsc&AN=000467564700076&site=eds-live&scope=site>.

Manogaran, G, Varatharajan, R, Lopez, D, Kumar, PM, Sundarasekar, R & Thota, C 2018, 'A new architecture of Internet of Things and big data ecosystem for secured smart healthcare monitoring and alerting system', *Future Generation Computer Systems*, vol. 82, pp. 375–387, viewed 5 October 2020, <https://search.ebscohost.com/login.aspx?direct=true&AuthType=sso&db=edselp&AN=S0167739X17305149&site=eds-live&scope=site>.

Miorandi, D, Sicari, S, De Pellegrini, F & Chlamtac, I 2012, 'Internet of things: Vision, applications and research challenges', *Ad Hoc Networks*, vol. 10, no. 7, pp. 1497–1516, viewed 5 October 2020, <https://search.ebscohost.com/login.aspx?direct=true&AuthType=sso&db=edselp&AN=S1570870512000674&site=eds-live&scope=site>.

Offner, KL, Sitnikova, E, Joiner, K & MacIntyre, CR 2020, 'Towards understanding cybersecurity capability in Australian healthcare organisations: a systematic review of recent trends, threats and mitigation', *Intelligence and National Security*, vol. 35, no. 4, pp. 556-585, viewed 5 October 2020, <https://www.tandfonline.com/doi/pdf/10.1080/02684527.2020.1752459?needAccess=true>.

Omoogun, M, Seeam, P, Ramsurrun, V, Bellekens, X & Seeam, A 2017, 'When eHealth meets the internet of things: Pervasive security and privacy challenges', *In 2017 International Conference on Cyber Security And Protection Of Digital Services (Cyber Security), IEEE,* pp. 1-7, viewed 5 October 2020, <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8074857>.

Ponemon Institute LLC 2016, 'Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data Sponsored by ID Experts Independently conducted by Ponemon Institute LLC', *In Ponemon Institute LLC*, viewed 5 October 2020, <https://www.ponemon.org/local/upload/file/Sixth%20Annual%20Patient%20Privacy%20%26%20Data%20Security%20Report%20FINAL%206.pdf>.

Sajid, M & Ahsan, K 2016, 'Role of Enterprise Architecture in Healthcare Organizations and Knowledge-Based Medical Diagnosis System', *JISTEM - Journal of Information Systems and Technology Management*, vol. 13, no. 2, pp. 181–192, viewed 5 October 2020, <https://search.ebscohost.com/login.aspx?direct=true&AuthType=sso&db=edssci&AN=edssci.S1807.17752016000200181&site=eds-live&scope=site>.

Schencker, L 2019, 'Hospitals' spending lags on digital security', *The Chicago Tribune*, viewed 5 October 2020, <https://www.courier-tribune.com/news/20190311/hospitals8217-spending-lags-on-digital-security>.

Symantec Corporation 2014, 'INTERNET SECURITY THREAT REPORT 2014', *Trends*, vol. 19, viewed 5 October 2020, <https://docs.broadcom.com/doc/istr-14-april-volume-19-en>.

Taddeo, M 2017, 'Deterrence by Norms to Stop Interstate Cyber Attacks', *Minds and Machines: Journal for Artificial Intelligence, Philosophy, and Cognitive Science*, vol. 27, no. 3, pp. 387–392, viewed 5 October 2020, <https://search.ebscohost.com/login.aspx?direct=true&AuthType=sso&db=phl&AN=PHL2361272&site=eds-live&scope=site>.

The Open Group 2011, 'Introduction to the Architecture Development Method (ADM)', viewed 5 October 2020, <http://www.opengroup.org/public/arch/p2/p2_intro.htm#:~:text=The%20TOGAF%20Architecture%20Development%20Method,assets%20available%20to%20the%20organization>.

Velasco, CA, Mohamad, Y & Ackermann, P 2016, 'Architecture of a Web of Things eHealth framework for the support of users with chronic diseases', *ACM International Conference Proceeding Series*, p. 47, viewed 5 October 2020, <https://search.ebscohost.com/login.aspx?direct=true&AuthType=sso&db=edb&AN=122591405&site=eds-live&scope=site>.

Whitman, ME & Mattord, HJ 2016, *Principles of information security*, Fifth Edition., Cengage Learning, viewed 5 October 2020, <https://search.ebscohost.com/login.aspx?direct=true&AuthType=sso&db=cat00006a&AN=melb.b5781440&site=eds-live&scope=site>.

Whittaker, Z 2019, 'A huge trove of medical records and prescriptions found exposed', *TechCrunch*, viewed 5 October 2020, <https://techcrunch.com/2019/03/17/medical-health-data-leak/>.

Williams PAH & Woodward AJ 2015, 'Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem', *Medical Devices: Evidence and Research*, vol. 2015, no. default, pp. 305–316, viewed 5 October 2020, <https://search.ebscohost.com/login.aspx?direct=true&AuthType=sso&db=edsdoj&AN=edsdoj.2f3acca2d3eb4043a25a0d84c559c05d&site=eds-live&scope=site>.

Xu, B, Xu, L, Cai, H, Jiang, L, Luo, Y & Gu, Y 2017, 'The design of an m-Health monitoring system based on a cloud computing platform', *Enterprise Information Systems*, vol. 11, no. 1, pp. 17-36, viewed 5 October 2020, <https://www.tandfonline.com/doi/ref/10.1080/17517575.2015.1053416?scroll=top>.

Yang, Y, Littler, T, Sezer, S, McLaughlin, K & Wang, HF 2011, 'Impact of cyber-security issues on Smart Grid', *2011 2nd IEEE PES International Conference and Exhibition on Innovative Smart Grid Technologies,*

Innovative Smart Grid Technologies (ISGT Europe), 2011 2nd IEEE PES International Conference and Exhibition on, pp. 1–7, viewed 5 October 2020, <https://search.ebscohost.com/login.aspx?direct=true&AuthType=sso&db=edseee&AN=edseee.6162722&site=eds-live&scope=site>.