JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

A Review on Cybersecurity in healthcare information security

Gagandeep Kaur*

Assistant Professor in Computer Science,
Khalsa College (ASR) of technology &Business Studies,
Mohali-Punjab.

Abstract

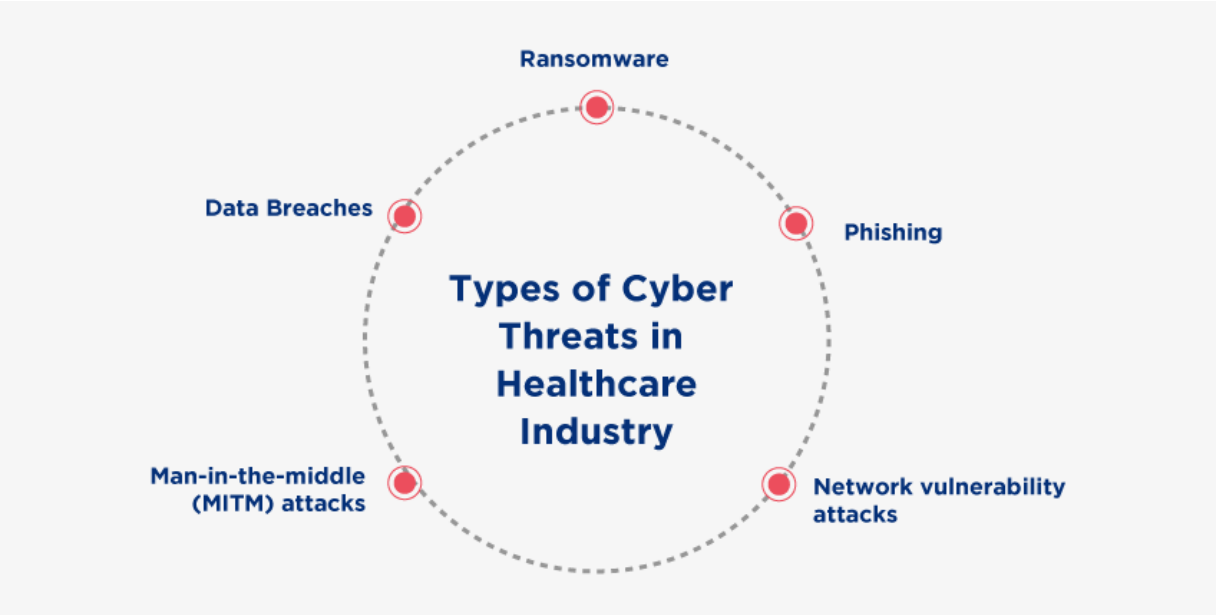
The healthcare industry lags behind other industries in protecting its data from Cyber-attacks. As health data contain sensitive personal and financial information, Cyber security incidents are a growing threat. To change this trend, it is important to develop systematic procedures for identifying suitable approaches for responding to their needs. To identify and summarize ethical, legal, and social issues related to information technology in healthcare, as exemplified by telehealth and telemedicine. To expand on prior analyses and address gaps illuminated by the COVID-19 experience. To propose future research directions. Literature was identified through searches, forward and backward citation chaining, and the author's knowledge of scholars and works in the area. EU and professional organizations' guidelines, and nineteen scholarly papers were examined and categories created to identify ethical, legal, and social issues they addressed. A synthesis matrix was developed to categorize issues addressed by each source.

Keywords: Cyber-attack, cybercrime, cybersecurity, cyber threats, health, healthcare, ransomware

1. Introduction

Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks. These cyberattacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes. Implementing effective cybersecurity measures is particularly challenging today because there are more devices than people, and attackers are becoming more innovative. Cybercrime emerged in the late 1970 with the development of computer Information Technology. Healthcare is an attractive target for cybercrime because it is a rich source of valuable data and not well protected. Cybersecurity breaches are a growing threat to the healthcare industry.

The main objectives of this paper is to present a structured framework of an eventual empirical research for linking Cyber Security improvement actions in healthcare systems to their strategic improvement needs. The structured framework is based on Quality Function Deployment (QFD), a generic, multi-purpose planning framework. The paper does not attempt to contribute to existing theories of cyber security or Quality Function Deployment.



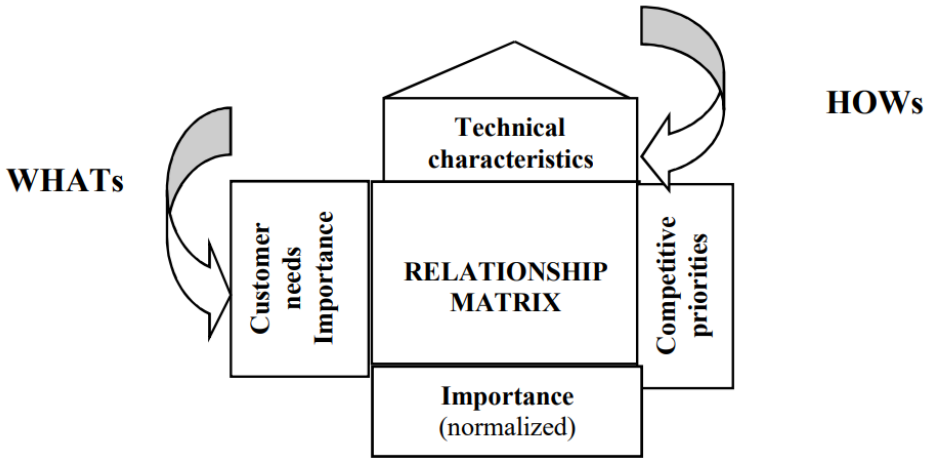
Cyberattacks and Security Issues in the Healthcare Sector

2. Quality Function Deployment

Quality Function Deployment (QFD) is a process and set of tools used to effectively define customer requirements and convert them into detailed engineering specifications and plans to produce the products that fulfil those requirements. QFD is used to translate customer requirements (or VOC) into measurable design targets and drive them from the assembly level down through the sub-assembly, component and production process levels. QFD methodology provides a defined set of matrices utilized to facilitate this progression.

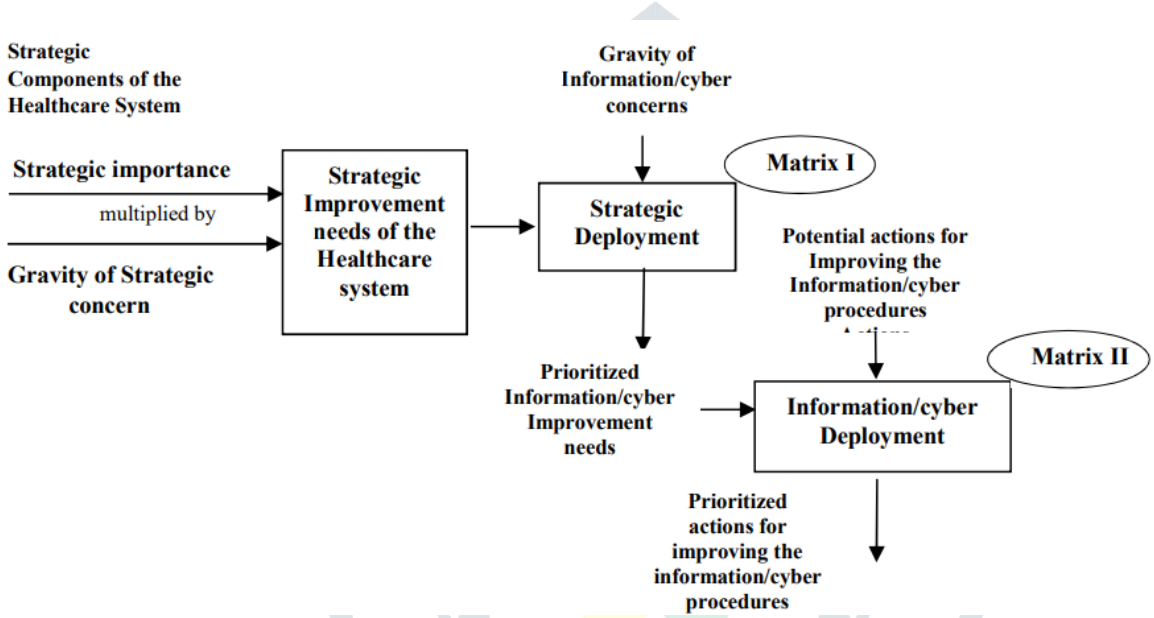
QFD was first developed in Japan by Yoji Akao in the late 1960s while working for Mitsubishi's shipyard. It was later adopted by other companies including Toyota and its supply chain. In the early 1980s, QFD was introduced in the United States mainly by the big three automotive companies and a few electronics manufacturers. Acceptance and growth of the use of QFD in the US was initially rather slow but has since gained popularity and is currently being used in manufacturing, healthcare and service organizations. The QFD methodology is implemented through sequential matrices The first and best documented matrix which translates the customer requirements expressed in his/her own words into measurable product technical characteristics is called **'The House of Quality'.**

The House of Quality is presented in the figure below. The matrix inputs (the house's western wall) are the customer needs, the WHATs and their respective numerical importance to the customer. They are translated into the HOWs (the house's ceiling), which represent the measurable product technical characteristics, or specifications. The relationship between each technical characteristic and each customer need are the core of the matrix and show how well each technical characteristic expresses the related customer need. The typical relationship strengths are weak, strong and very strong and they are all positive. The triangle (the house's roof) describes the relationships between the technical characteristics. Some are positively related, while others are negatively related and are used as trade-off. The translated values (the matrix output) represent the calculated importance of the technical characteristics. As mentioned above, the output of matrix I becomes the input of matrix II. This sequential approach continues from matrix to matrix.



3. The conceptual QFD model of a healthcare system

We adapt the QFD technique to describe propagation of the improvement needs of a healthcare system from the strategic level to the action level.



we evaluate the strategic improvement needs of a healthcare system by multiplying the importance of each strategic component by the gravity of its concerns. The higher the importance of a strategic component and the higher the gravity of the concern related to its realization, the higher is its improvement need. This measure is a vector version of the ‘importance-performance matrix as a determinant of improvement priority'. However, the set of strategic components representing the competitive advantages of the healthcare systems are different from the competitive advantages of a manufacturing enterprise in and cannot be measured on universal scales such as time, quality and cost. The strategic competitive advantages of a healthcare system are related to the safety/satisfaction of patients, the quality of the medical team, the technological level of the medical facilities and eventually to financial management and marketing.

MATRIX 1 Strategic Deployment

	Input 2 Gravity of information /cyber concerns		
Input 1 Strategic Improvement needs of the Healthcare System			
		$r_{1k,i}$	
Output	**Prioritized information/cyber improvement needs**		

MATRIX II Information/cyber Deployment

	Input 2 Potential actions for improving information / cyber procedures		
Input 1 Prioritized Information/cyber Improvement needs			
		$r_{1k,i}$	
Output	**Prioritized information/cyber improvement needs**		

4. A proposed empirical study: the necessary data and its analysis

The above conceptual model can be used to design and perform an interview based empirical study. At least say a sample of 20 healthcare organizations (hospitals) have to be investigated. In each organization, at least 7-8 employees should be interviewed.

We first define a set of k, k=1, 2…, s basic strategic competitive advantages of a healthcare system.

- Safety and satisfaction of patients
- Quality of medical team
- Technology level of the medical facilities
- Financial Management
- Marketing

Some examples of information/cyber concerns

- Infringement of information
- Lack of physical security
- Denying access to systems and files
- Employees lack of awareness
- Operational malfunctions and warnings

Some examples of potential actions for improving information/cyber procedures

- Encryption and data/ information protection
- Permission, identification and access control
- External protection
- Human resources and employees training
- Physical and environmental protection

Matrix II, with hypothetical data from the above examples, is presented.

The symbol √means high impact of a specific improvement action on a specific concern

Cybersecurity in Healthcare and Its Importance

IT security in healthcare constantly deals with evolving cyber threats that could endanger patient safety. It is urged that hospital C-suite executives and senior management avoid viewing cybersecurity as a purely technical issue that only their IT departments can tackle. Instead, it is essential to include cybersecurity in the hospital's present enterprise, risk management, governance, and business continuity structures as a top strategic priority for patient safety and enterprise risk. Following the Healthcare Stakeholders

- Patients
- C-Suite
- Workforce Members
- Vendors/Market Suppliers

5. Cyberattacks Against Medical Devices

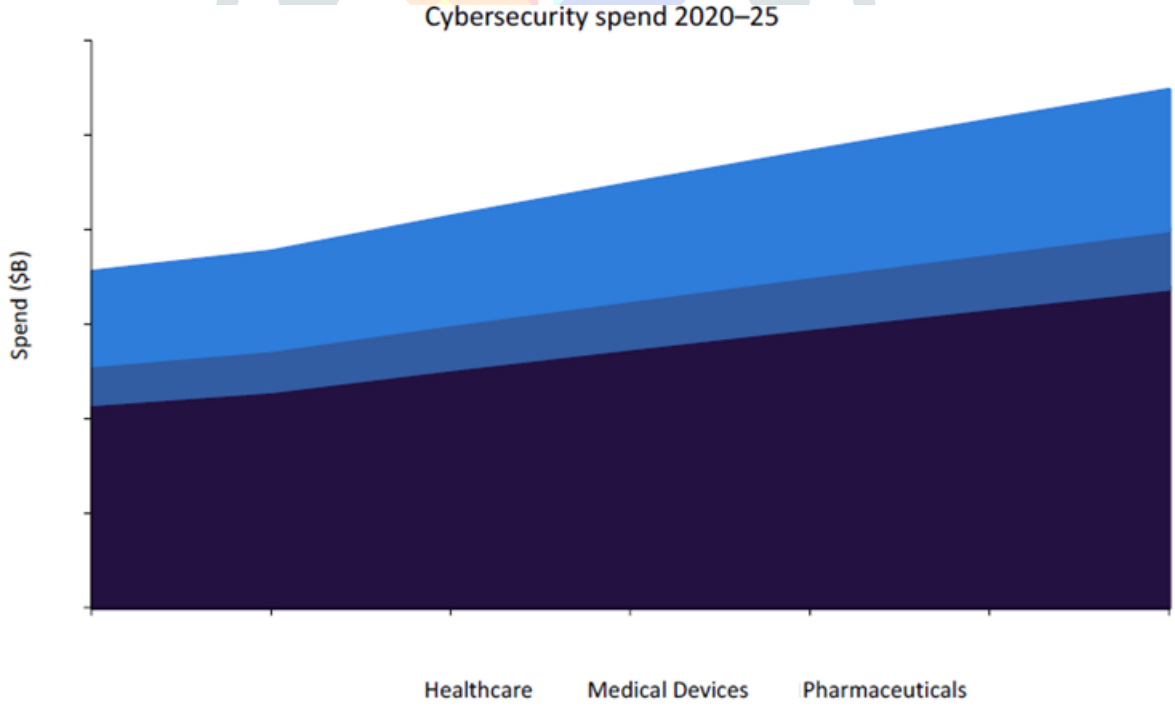
Healthcare IT experts find it particularly difficult to maintain security because of the enormous number of linked medical equipment, many of which have different specifications and come from different manufacturers. Even though medical devices don't necessarily include a lot of patient data, they can serve as easy access points for hackers to servers containing a lot of data. The healthcare cybersecurity market must prioritize keeping these entry points securely and up to date to reduce the costs and harm brought on by unauthorized access.

5.1 Cybersecurity in Healthcare – Industry Analysis

The healthcare market size was $4.59 billion in 2020. Cybersecurity in the healthcare industry is forecast to grow at around 8% between 2020 and 2025. Cybersecurity in medical devices and cybersecurity in pharmaceuticals, both are forecast to grow at a CAGR of about 7% during the same period.

The cybersecurity in healthcare thematic research report also covers:

- Mergers and acquisitions
- Hiring trends
- Social media trends
- Timeline



Matrix II Information/cyber deployment *(hypothetical)*

Input 1 Prioritized Information/ Cyber Improvement needs	**Input 2** Potential actions for improving information/cyber procedures	Encryption and data /information protection	Permission, identification and access control	External protection	Human Resources and Employees training	Physical and environmental protection
Infringement of information		√	√			
Lack of physical security						
Denying access to systems and files		√	√			
Employees lack of awareness					√	
Malfunctions and warns						
Output		**Prioritized** actions for improving Information /cyber procedures				

6.Concluding remarks

- QFD a product-oriented quality design technique has been applied in an innovative way to improve information/cyber procedures in healthcare systems.
- To measure the strategic improvement needs of a healthcare system a vector version of the 'importance performance matrix as a determinant of improvement priority', developed by Slack was used.
- A set of basic strategic competitive advantages in a healthcare system has been proposed.

7. Conclusions and Future Works: The healthcare industry is a prime target for medical information theft as it lags behind other leading industries in securing vital data. It is imperative that time and funding is invested in maintaining and ensuring the protection of healthcare technology and the confidentially of patient information from unauthorized access. In the future, this model will be evaluated using the same data with a different model developed by other researchers to prove it is valid and accurate. The model can be used to evaluate existing hospitals and improved to ensure it gives optimal results

References

[1] L. Coventry, D. Branley, Cybersecurity in healthcare: A narrative view of trends, threats and ways forward, Maturitas, 113 (2018) 48-52.

[2] C. S. Kruse, B. Frederick, T. Jacobson, D. K. Monticone, Cybersecurity in healthcare: A systematic review of modern threats and trends, Technology and Health Care, 25 (2017) 1-10.

[3] M. Hagland, With the ransom crisis, the landscape of data security shifts in healthcare. Healthcare information 33 (2016) 41-47.

[4] M. S. Jalali, J. P. Kaiser, Cybersecurity in Hospitals: A systematic, organizational perspective, Journal of Medical Internet Research 20 (2018) Doi: 10.2196/10059.

[5] Y. Akao, Quality Function Deployment: Integrating Customer Requirements into Product Design, Cambridge, Ma: Productivity Press (1990). 286 Miryam Barad / Procedia Manufacturing 39 (2019) 279–286 8 Miryam Barad / Procedia Manufacturing 00 (2019) 000–000.

[6] J. Bossert, Quality Function Deployment – A practitioner's approach, Milwaukee WI: ASQC Quality Press (1991).

[7] R. King, Designing Products and Services that customer wants, Portland OR: Productivity Pres (1995).

[8] L. K. Chan, M. L. Wu, Quality Function Deployment: A literature review. European Journal of Operations Research 143 (2002) 463-497.

[9] J. R. Hauser, D. Clausing, The House of Quality, Harvard Business Review 66 (1988) 1-27.

[10] M. Barad, D. Gien, linking improvement models to manufacturing strategies, International Journal of Production Research 39 (2001) 2675-2695.

[11] J. Pfeffer, Producing sustainable competitive advantage through the effective management of people, Academy Management Executive 9 (1995) 55-69.

[12] J. C. Flanagan, The critical incident technique, Psychological Bulletin 51 (1954) 327-358.

[13] N. Slack, The Importance – Performance Matrix as a determinant of Improvement Priority, International Journal of Operations and Production Management, 14 (1994) 59-75.

[14] C. M. Garcia, Strategies and performance in hospitals, Health Policy 67 (2004) 1-13.

[15] T. J. Douglas, understanding competitive advantage in the general hospital industry: evaluating strategic competence, Strategic Management Journal, 24 (2003) 334-347