JOURNAL OF INTERNATIONAL CRISIS AND RISK COMMUNICATION RESEARCH
ISSN: 2576-0017
2024, VOL 7, NO S7

The impact of cybersecurity and its role in health care

Ebtesam Alruwaili1, Modhi Alshammari2, Mashael Mohammad Sindi3, Fayrouz Abdullah Saeed Alghamdi4, Awatef Abdu Ahyaf5, Fawziah Hamdan Alqarni6, Mohammed Ali Namshan Alkhathami7, Ohoud Jazi Alhumairan8, Ahmad Jamaan Said Alzahrani9, Saleh Atiah Ali Alghamdi9, Fahad Saeed Ateh Alzahrani9, Khaled Rajaan A Alharbi10, Eid Saud Alanazi11

1Health information technician, Second Health Cluster, Riyadh,Primary health Care Center Al-Naseem Al-Awsat Ministry of Health Riyadh, Saudi Arabia
2Health information technician,Innovation Offic ,General Directorate of Health Affairs in Riyadh Region, Ministry of Health Riyadh , Saudi Arabia
3Health informatics specialist, Maternity and children hospital makkah, Saudi Arabia.
4Health information technician, National Guard Health Affairs Western Sector Jeddah, Saudi Arabia.
5health Informatics Technician, king Abdulaziz hospital In Jeddah, Saudi Arabia.
6Health information Technician, Tabuk Health Cluster (Managing internal communication), Saudi Arabia.
7Health Information Management, Al Quwayiyah General Hospital, Saudi Arabia.
8Health information, Alsaadh PHC, Saudi Arabia.
9Health information's technician, King Fahad Hospital Albaha, Saudi Arabia.
10Health informatics, Ministry of National Guard, Saudi Arabia.
11Health informatics technician, Taima General Hospital, Saudi Arabia.

1.1 INTRODUCTION

There is no doubt that digitalization or the application of advanced information technologies plays a vital role in the functioning of healthcare institutions in the modern era (G. Gopal,2019).

However, it also brings some challenges. One of them is cybersecurity (M. Mijwil,2023). Protecting information is one of the most important tasks of healthcare organizations. (X. Liu,2022) Most use health information systems such as “electronic prescribing systems, electronic health record systems, practice management support systems, clinical decision support systems, radiological information systems, and computerized order entry systems.” Doctors", to name a few. (N. Al-Shorbaji,2022) These systems are usually connected to the Internet of Things, the Internet, etc. and have the possibility of remote access (R.T. Sutton,2020). The fact is that these technological systems simplify various tasks and help in managing healthcare processes.

With Therefore, the threat it poses to cybersecurity should not be underestimated (S. Gallina,2023). The healthcare sector is an ideal target for cyber-attacks due to its glaring cybersecurity flaws. Over the past five years, approximately 93% of medical companies have experienced a data breach, and 57% of them have had more than five incidents (Staff,2022).

According to Check Point Research, healthcare organizations around the world saw an average of 1,463 cyberattacks per week in 2022, a 74% increase compared to 2021. (A.F. Sayed,2020) Healthcare organizations in the United States face an average of 1,410 cyberattacks per week, an 86% increase from 2021 (L. Phillips,2023). From these statistics, it is clear that cyber-attacks are increasing every year. As more healthcare organizations adopt information systems, more cyber-attacks occur. The risks associated with these technologies cannot be ignored and require appropriate management measures (J. McKeon,2022).

On the other hand, the benefits of these technologies in healthcare cannot be ignored and healthcare institutions have no choice but to adopt them (M. Ibrahim,2015). It is necessary to identify the factors behind these attacks in healthcare organizations and

how to mitigate them. While this is a fact, cybercriminals are changing their tactics and adopting new attacks as technology evolves.(G. Memmi,2023)

The impact of cyberattacks on healthcare is often significant. The loss may involve financial, personal or organizational documents, which can be used for many purposes. Health Information System (HIS) adoption has become important in the rapidly growing healthcare environment to improve patient care, process efficiency, and innovation in healthcare.(S. Malhotra,2023)

Aside from the potential benefits, their adoption varies widely, with challenges related to the perceived cybersecurity risks posed by these systems. Due to the highly sensitive nature of medical information, healthcare is a prime target for cyberattacks, and concerns about data breaches, privacy, and system vulnerabilities prevent healthcare facilities from fully adopting a healthcare information system. This study seeks to fill this important gap and understand the role of perceived cybersecurity threats in the adoption of healthcare information systems, while identifying key drivers for improving healthcare system security, patient trust, and medical care in general.

1.2 Research Importance:

The study is important because it covers important challenges in integrating healthcare, technology, and security. Now more than ever, knowing the role and impact of perceived cybersecurity issues on healthcare system adoption is essential as technology revolutionizes healthcare. This study provides insights into how to improve patient data security, healthcare efficiency, provide guidance for policies and regulations, reduce costs, etc., in the healthcare industry. Ultimately, it promises to improve the healthcare sector's ability to harness the potential benefits of modern technology, while protecting the highest levels of patient safety and confidentiality.

1.3 STATEMENT OF THE PROBLEM

This research focuses on addressing the problem in Saudi Arabia of the study, which revolves around knowing phishing attacks on health care systems, knowing the role of information systems and cybersecurity on the health care department, and studying technological gaps and the extent of their significant impact on the adoption of health care information systems . Therefore, the problem of the study focuses on answering the main question, which is:

What is the impact of cyber security course in healthcare?

1.4 Research Objectives:

1-Explore the impacts of cybersecurity-related factors that affect the adoption of healthcare information systems

2- Identify if the phishing attacks and lack of skills of workers have a significant impact on the adoption of healthcare information systems

3-Identify the Benefits of cyber security on the adoption of healthcare information systems?

1.5 Research Questions :

1-What are the impacts of cybersecurity-related factors that affect the adoption of healthcare information systems?

2-Do the phishing attacks and lack of skills of workers have a significant impact on the adoption of healthcare information systems?

3. What are the Benefits of cyber security on the adoption of healthcare information systems?

1.3 Research Methodology

1.3.1 Research Design

1. The research included a descriptive analytical approach that focused on health care employees to determine the impact of cybersecurity and its role in health care in the Kingdom of Saudi Arabia.
2. And the quantitative approach will be used, which is a method to study scientific phenomena or problems by describing them scientifically and then arriving at logical explanations that have evidence and arguments that give the scientific researcher the ability to reach a solution to the problem in a way Certain, and this approach is used to arrive at results related to the study problem

1.3.2 Research Sample

1. Data will be collected by distributing the electronic questionnaire by selecting a random sample.
2. The study population was selected by the researchers in the form of a random sample. The researcher nominated that sample to apply the questionnaire by distributing it electronically via a Google Chrome link
3. Study populationThis community was collected and the questionnaire was distributed to them.
4. Study sample: A random sample was selected from a group of employees in the care department in Riyadh.

1.3.3 Data Collection Method and Instruments

The questionnaire will be used as a study tool to collect data, then it will be presented to the dissertation supervisor, approved, and transferred to the electronic version.

1.3.4 Data Analysis Procedure

After collecting data, researchers analyze it using appropriate techniques, which may include quantitative analysis (statistical methods) The researcher will use the statistical package program (SPSS) and the following methods will be used:

1- Pearson correlation coefficient to verify the validity of the study tool.
2- Cronbach's alpha coefficient to calculate internal consistency reliability.
3- Frequencies and percentages.
4- Calculating the standard deviation
5- Calculating the arithmetic mean
6- Calculation (T-test)

1.4. Research Outline

The research has been divided into several chapters that will be discussed as follows:

Chapter One: The general framework of the study.

In this chapter, we will provide an introduction to the topic, an overview of the problem of the topic, and we will define our point of view The objectives of the study, the problem of the study, and the study questions are presented, and we will address a set of questions that determine the method of solving the study problem

Chapter Two: The theoretical framework and previous studies.

In this chapter, we will discuss the previous research and find the gaps between it.

Chapter Three: Research Methodology.

The research is based on the use of a quantitative approach, as it is considered the approach that is appropriate for this study, by using a survey to evaluate the factors affecting the data, and relying on knowledge of the extent of the impact of cybersecurity and its role in health care. The data that will be collected via Google Forms will be analyzed using statistical methods.

Chapter Four: Study results and discussion.

In this part of the research results and discussion, a questionnaire will be distributed, and after taking the results, they will be analyzed and included. Chapter Five: Conclusion and recommendations. In this final chapter, a set of recommendations will be presented based on the results of the study: The impact of cybersecurity and its role in health care. We conclude by summarizing the main ideas and their implications for future research and practical applications.

CHAPTER II: LITERATURE REVIEW

2.1 LITERATURE REVIEW

The ever-increasing technological revolution has been at the heart of improving healthcare services around the world. This technology has led to the implementation of important health information systems for organizational stakeholders, healthcare providers, and patients. This is because it links the system to complex process management functions, such as health care costs, electronic record keeping, and automation of critical care information. In other words, many devices are being used in hospitals via the Internet of Things (IoT) to disseminate healthcare delivery standards (Liu, X.,2019) . Critics argue that these developments can be seen as inheriting many benefits. However, health information systems, software and networks also carry a series of threats and all kinds of risks, such as hacking. To date, cyberattacks have primarily focused on financial institutions with the goal of breaching security encryption to steal funds or cause other damage. However, dynamic changes have occurred that make the healthcare environment a potential target (Demigha,2016). First, healthcare organizations have a sensitive infrastructure that contains important records needed for various functions, such as health history and research. Referring to the research conducted by (Rajendra,2014), attackers have increased their attacks against US health organizations and the statistics are expected to grow significantly. According to published reports, most healthcare organizations experience at least one system attack within a twelve-month period. Additionally, system integrity was compromised at half of these organizations, resulting in the disclosure of critical medical and patient information. In addition, some healthcare organizations participate in research activities and thus act as host laboratories. Due to the circumstances of piracy, there is a possibility of loss of intellectual property and research work which requires a significant investment of time and resources. In the worst cases, this type of exposure can harm unsuspecting patients when medical formulations are stolen and used in clinical trials. Cybersecurity, positive factors affecting data in the field of health care: It is worth noting that cybersecurity is the practice of securing computer systems and networks against unauthorized access, by mitigating information risks and vulnerabilities, and thus this practice has become an essential part of maintaining the safety of companies, institutions, and individual users.

In healthcare Cybersecurity includes a set of measures, such as firewalls, anti-virus programs, and encryption techniques to defend against electronic threats. The primary goal is to maintain the integrity, confidentiality, and availability of information while reducing the risks associated with cybersecurity, the most prominent of which are the following:

2.1.1- Protection of personal data

The protection provided by cybersecurity is not limited to the data of institutions and companies only; It also includes the personal data of sick employees, as cybersecurity can also protect data from internal threats, whether accidental or with malicious intent,

and ensure that employees can access the Internet and use it at work without threats of data breaches.

2.1.2- Enhancing productivity

Cyber attacks and crimes lead to data breaches, which affect workflow, networks and performance, so productivity is negatively affected and the affected company goes out of business. Therefore, one of the most prominent benefits of cybersecurity is enhancing the productivity of individuals and companies, through scanning viruses, improving firewalls, and automated backups, in addition to educating employees about email phishing, fraud, suspicious links, and all other suspicious activities.

2.1.3- Strengthening the cyber situation

Cybersecurity provides companies with comprehensive digital protection, which gives employees the flexibility, security, and freedom to access the Internet. This strategy enables companies to act and respond during and after a cyberattack.

2.1.4- Improving data management

Organizations continuously monitor their data by implementing cybersecurity strategies, ensuring that data security regulations are implemented optimally. 2.1.5- Increase workforce education

Cybersecurity strategies include educating employees and workers in institutions and companies about potential risks such as ransomware, spyware, data breaches, and other aspects of the organization's daily operations.

When educating the employee about these risks; He will be more aware before clicking on malicious links or suspicious files and will also be able to know the right action if anything goes wrong.

2.1.6- Protecting websites

The majority of companies and institutions rely on websites, so the downtime of these websites leads to loss of revenue, loss of transactions and communications, and deterioration of patient confidence. Therefore, implementing a cybersecurity process ensures that those sites are protected from unexpected damage and hence long-term data access.

Electronic attacks also include hacking into bank accounts or using malware to steal credit card numbers, making purchases in the victim's name, and then accumulating debts on him. Thus, cybersecurity provides the necessary protection for identity from theft.

2.1.7- Compliance with regulations

Companies and organizations' compliance with cybersecurity standards and regulations protects them from legal problems and potential fines.

2.1.8- Ensuring the security of remote work

Implementing cybersecurity measures has become essential as remote work has become increasingly common in recent years, as it ensures safe access to and use of organizational resources, maintaining productivity while reducing risks associated with remote work environments.

To benefit from cybersecurity, skills in it can be enhanced by enrolling in the training courses provided by the Bakkah platform in the cybersecurity analysis course.

Cybersecurity: Negative factors affecting data in the healthcare field Main threats against the health sector: Viruses: This type of threat is considered a form of malware that encrypts all data on electronic devices (cell phones, computers, etc.) and prevents the owner from accessing 1-Insider Threat: An insider threat is defined as a threat specific to employees or individuals allowed to access sensitive data and information,

which may lead to damage to the system by disabling, revealing, or changing information.

3- DDoS attacks:.

Email phishing: Due to lack of awareness of phishing scams by health practitioners, many of them fall into the trap of these attacks. Phishing messages may usually contain a download link or file that leads to the installation of malicious viruses, ransomware, or installation of keyboard trackers that can track every keystroke the user makes.

2.2 Software Solution for Healthcare Cybercrime

Some of the software used in preventing cyber-attacks include but not limited to email encryption software and firewall software. Email encryption software such as Virtue and Symantec Desktop Email encryption are used to protect hospital emails and thereby thwarting manin-the-middle attacks and other phishing-based attacks. Besides Open DNS and other DNS filtering software, hospital have referred to tools such as SSL and contracted security companies such as COMODO to secure the connection and communication over application and data layers. Breach Trends in healthcare and other sectors based on the chart below and considering a wider timeline to understand the trend, it suffices to conclude that data breaches worsened in 2016 and 2017 in the medical/healthcare industry.

From: The Impact of Cybersecurity on Healthcare

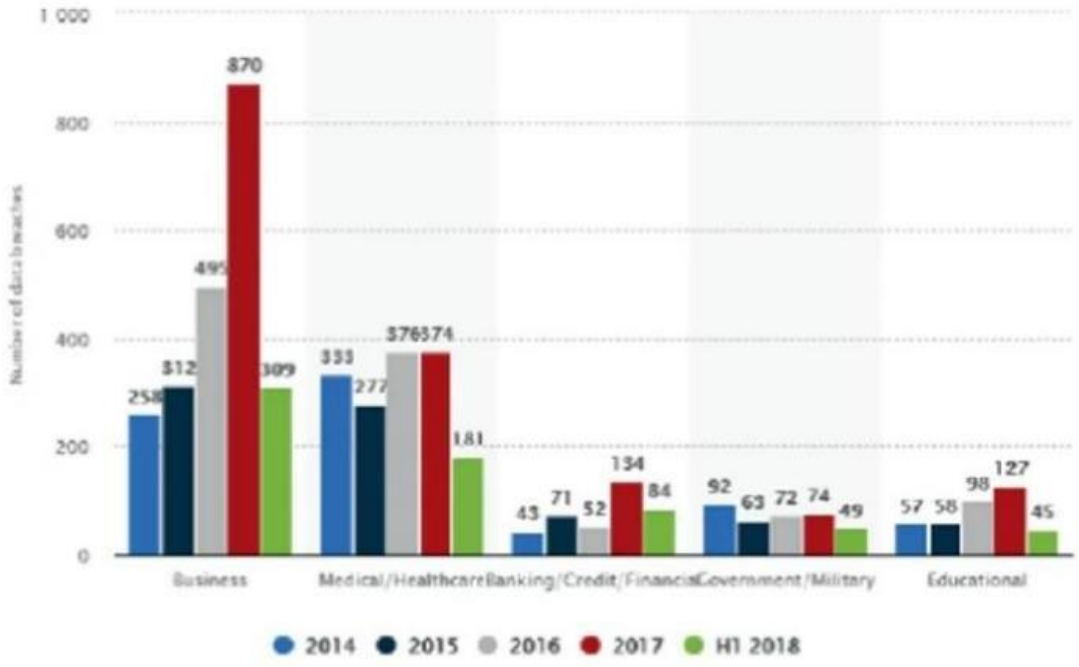

Fig. 1: Data breaches from 2014 to 2018

As per the chart of Fig. 1, a majority of the data breaches affected the businesses (608), followed by healthcare organizations in the first half of 2018. However, it is imperative to note that about 67 cyberattacks that occurred in May 2017 were related to WannaCry and they targeted and affected healthcare organizations among others. As per the chart, businesses were the most affected in 2017 with an overall 870 data breaches. During the same year, healthcare organizations endured 374 attacks while the banking industry

had 134, the government/military had 74, and education sector had 127. The number of attacks is on the rise with several cases reported in the US over the past months. For instance, in August, about 417,000 patient records of Augusta University were reported breach and massive amount of sensitive information. On September 13, 2018, the Fetal Diagnostic Institute also suffered a ransomware attack during which 40,800 patient records were breached. Finally, it is critical to emphasize that about 4.93 million patient records were exposed in 2017, and over 980,136 records had been exposed by June 2018. Given the sensitivity of personal information and their growing value in the underground world, it is increasingly becoming important to embark on cybersecurity and enforce security control protocols that will protect both the hospital and the patients. Apparently, patient information sold as full profile leads to identity theft and criminals use such as information to claim insurance repayments. Depending on the geographical location of the affected organizations, the authority or agency concerned with thwarting cybercrime through enforcement of standards tend to differ. In the US, for example, it is Health Insurance Portability and Accountability Act (HIPAA) requires healthcare organizations to protect patient data and uphold the privacy of the patients. The importance of cyber security is hinged on the nature of the information lost and intention of perpetrators. Besides degraded reputation, the victim organizations have only worked towards securing their systems to ensure that such attacks do not occur. Fortunately, most of the organizations have good and updated disaster recovery plan as well as business continuation option. Bouncing back from a cyberattack is not an easy feat but with proper contingency and disaster recovery plan, the affected organizations have been able to embark on isolated recovery and restoration of the affected systems.

Studies:

2.1.1 Cybersecurity in Health Care

Most of us are aware of cyber-threats — if not because of personal experience, then thanks to a barrage of news stories. We've read that many of our banks, credit-card companies, and favorite retailers have been hacked and that tens of millions of con-sumers had their personal finan-cial information stolen during the 2013 holiday season. In addition, last year brought stories of suc-cessfulcyberintrusion at the Food and Drug Administration (FDA) and of the theft of the designs of major U.S. military weapons systems by foreign governments. Health care data and infrastruc-ture are at least as vulnerable as most financial and military data. beyond the pecuniary, regulatory, and reputational risks associated with data and identity theft lie even graver threats to health care infrastructure and patient safety. In a recent study, a whopping 94% of health care institutions reported having been victims of cyberattacks.1 To date, cybercrime against health care has manifest-ed as four specific threats: data loss, monetary theft, attacks on medical devices, and attacks on infrastructure In a recent study, a whopping 94% of health care institutions reported having been victims of cyberattacks.1 To date, cybercrime against health care has manifested as four specific threats: data loss, monetary theft, attacks on medical devices, and attacks on infrastructure.(Eric D. 2014).

2.1.2 Healthcare Challenges in the Era of Cybersecurity

As a result of the extensive integration of technology into the healthcare system, cybersecurity incidents have become an increasing challenge for the healthcare industry. Recent examples include WannaCry, a nontargetedransomware attack on more than 150 countries worldwide that temporarily crippled parts of the National Health Service in the United Kingdom, and the 2016 ransomware attack on Los Angeles's Hollywood Presbyterian Medical Center. The attacks cost millions of dollars

in lost revenue and fines, as well as significant reputational damage. Efforts are needed to devise tools that.allow experts to more accurately quantify the actual impact of such events on both individual patients and healthcare systems as a whole. While the United States has robust disaster preparedness and response systems integrated throughout the healthcare and government sectors, the rapidly evolving cybersecurity threat against healthcare entities is outpacing existing countermeasures and challenges in the "all-hazards" disaster preparedness paradigm. Further epidemiologic research of clinical cybersecurity attacks and their effects on patient care and clinical outcomes is necessary to prevent and mitigate future attacks(Jeff Tully, Jordan, James P. Phillips, Patrick O'Connor, and Christian Dameff,2020).

2.1.3 The Impact of Cybersecurity on Healthcare

The advancement of technology in recent times has posed a number of serious threats to the integrity of the systems, networks, and programs utilized in different fields such as Healthcare organizations. Such threats have compounded with the development of cybersecurity, a move which involves protecting the systems from imminent threats that materialize in the form of digital attacks. Inadvertently, cybersecurity has become an important aspect of digital protection from ill-intentioned people who exploit the vulnerability of systems. This paper addresses the impact of cybersecurity in healthcare organizations. While on it, the paper will also present the various types of security threats in the industry and utilizing AES (Advanced Encryption Standard) as a protective measure for health-based organizations(Kohei Arai,2021)

2.4 Conclusion

The document highlights some of the important impacts of cybersecurity on health. However, this article shows that this is an area lacking scientific research. Therefore, more research is needed to help health find more sustainable ways to defend itself. The reason healthcare organizations are easy targets is because of outdated IT defenses.

References:

[1] G. Gopal, C. Suter-Crazzolara, L. Toldo, W. Eberhardt, Digital transformation in healthcare – architectures of present and future information technologies, Clin. Chem. Lab. Med. 57 (3) (Feb. 2019) 328– 335, https://doi.org/10.1515/cclm-2018-0658.

[2] N. Al-Shorbaji, Improving healthcare access through digital health: the use of information and communication technologies, in: Healthcare Access, Intech Open, 2022.

[3] M. Mijwil, M. Aljanabi, A.H. Ali, ChatGPT: exploring the role of cybersecurity in the protection of medical information, Mesopotamian J. Cyber Secur. (Feb. 2023) 18–21, https://doi.org/10.58496/MJCS/2023/004.

[4] X. Liu, et al., Cyber security threats: a never-ending challenge for ecommerce, Front. Psychol. 13 (Oct) (2022), https://doi.org/10.3389/fpsyg.2022.927398.

[5] R.T. Sutton, D. Pincock, D.C. Baumgart, D.C. Sadowski, R.N. Fedorak, K.I. Kroeker, An overview of clinical decision support systems: benefits, risks, and strategies for success, npj Digit. Med. 3 (1) (Feb. 2020) 17, https://doi.org/10.1038/s41746-020-0221-y.

[6] A.F. Sayed, M.K. Shahid, S.F. Ahmad, Adoption of Mobile Payment Application and its Impact on Business, 2020, pp. 253–269.

[7] S. Gallina, Preparing Europe for future health threats and crises: the European Health Union, Euro Surveill. 28 (5) (Feb. 2023), https://doi.org/10.2807/1560-7917.ES.2023.28.5.2300066.

[8] Staff, "Cybersecurity in Healthcare, BreachQuest, 2022. https://www.breachquest.com/industry/healthcare/.

[9] L. Phillips, Healthcare Cybersecurity in 2023: Hive's Shutdown Is Good News but Cyberattacks Are Only Getting Worse, InsiderIntelligiece, 2023.
[10] J. McKeon, As API Adoption in Healthcare Skyrockets, Cybersecurity Risks Follow, Helathitsecuity, Jan. 2022.
[11] M. Ibrahim, M.K. Shahid, Impact of risk and ethics on adoption of mobile banking in Pakistan, J. Econ. Sustain. Dev. 6 (7) (2015) 175– 188.
[12] G. Memmi, Cyber attacks in healthcare: why they matter and how to defend against them, Br. J. Healthc. Manag. 29 (1) (Jan. 2023) 8– 11, https://doi.org/10.12968/bjhc.2022.0134.
[13] S. Malhotra, Cyberattacks Hold up India's Push for Digitisation of Health, BMJ, Feb. 2023, p. p263, https://doi.org/10.1136/bmj.p263.
[14] Liu, X., et al.: Evaluation of secure messaging applications for a health care system: a case study. Appl. Clin. Inform. 10(1), 140–150 (2019)
[15] Demigha, S.: Mining knowledge of the patient record: the Bayesian classification to predict and detect anomalies in breast cancer. Electron. J. Knowl. Manag. 14(3), 128–139 (2016)
[16] Rajendra, M.: A VHDL implementation of the advanced encryption standard-Rijndael algorithm. MSc. dissertation, University of South Florida, Tampa (FL) (2014