International Journal of Progressive Sciences and Technologies (IJPSAT)
ISSN: 2509-0119.

Vol. 35 No. 1 October 2022, pp. 195-208

Cybersecurity in Health Systems: Challenges, And Proposals Review

Maged Naser[1], Mohamed M. Naser[2], Lamia H. Shehata[3], Thana Nassr [4]

[1] Mazahmiya Hospital, Ministry of Health, Kingdom of Saudi Arabia, Department of Ob/Gyn,

[2] King Fahd Hospital, Ministry of Health, Kingdom of Saudi, Department of Surgery, Consultant Endoscopic Surgery,

[3] Department of Radiology Care National Hospital, KSA,

[4] Software engineering, Queen's University Belfast, UK

Abstract – The new rise in network safety breaks in medical care organizations has put patients' security at a higher risk of being uncovered. In spite of this danger and the extra danger posed by such incidents to patients' safety, as well as functional and monetary dangers to medical care organizations, few studies have deliberately analysed the cyber security risks in medical care. To establish a strong starting point for medical services organizations and policymakers in better comprehension the intricacy of the issue of cyber security, this study investigates the significant sort of cyber security risks for health care organizations and makes sense of the roles of the four keys (cyber attackers, cyber defenders, developers, and end users) in cyber security. Finally, the paper studies a group of recommendations for the policymakers and health care organizations to reinforce cybersecurity in their organizations

Keywords – Cyber security, Data breach, Patient data, Security, Protection, Block chain, Cyber-attack.

I. INTRODUCTION

Propels in innovation have had various cultural advantages, including the health care sector. The ascent in the utilization of Electronic Health Records (EHR) is supposed to diminish medical care costs by working on the quality and delivery of ideal medical services administrations [1]. Perceiving these advantages.

The Health Information Technology for Economic and Clinical Health (HITECH) Act was ordered to increase the number of healthcare organizations adopting Health Information Technology (HIT) [1]. While HIT has significant advantages, incorporating medical care with innovation has increased the probability of breaches of patient records [2]. Data that is lost, taken, displaced, hacked, or imparted to informal beneficiaries is characterized as a breach; and this disturbance in data is considered a cyber-attack [3, 4]. Around 94% of healthcare organizations have encountered something like one of these kinds of cyber-attacks [5]. An expected 150 million patient health records have been penetrated somewhere in the range of 2009 and 2014 [6]. Most of the breaks during this period were the consequence of break, loss, or theft of portable computing devices [6]. A review led by McCue found that insiders as opposed to outsiders direct 70% of data fraud in organizations [7]. The richness of information's housed by medical care elements has been referred to as an essential explanation that healthcare is susceptible to high information breach and monetary risks [8].

Healthcare organizations as a rule have a high volume of sensitive data. Information's containing names, date of birth, social security number, address, and credit data are abundant in hospital and insurance records. In addition, hackers prefer focusing on healthcare organizations because healthcare information's is more valuable than information's from different industries in black market. An EHR, for example, is worth somewhere in the range of 10 and 100 times more than credit data in the black market [9].

Corresponding Author: Maged Naser

Cyber breaches add to the monetary burden for the medical services industry, which as of now goes up against high consumptions and low-net revenues in contrast with numerous different industries. As of now, the typical expense of information loss is more noteworthy for a medical services organizations contrasted with organizations in different areas [8]. The punishments and fines forced by elements like the health and Human Administrations' Office for civil rights further compound the monetary burden endured by medical care associations, in spite of the fact that they boost organizations to work on their network protection. It is assessed that data breaks will prompt $309 billion in lost income by 2019 [6].

The issue of cybersecurity goes past patients' security and the monetary burden on the industry; it likewise represents a danger to patient safety [8]. For instance, the utilization of wireless medical devices might expose patients to dangers from cybercriminals. A cybersecurity flaw in a heart device like the one as of late identified by the U.S. Branch of Country Security could be taken advantage of by cybercriminals to harm a patient [10]. Safeguards, for example, encryption, shredding documents, locking doors, and utilizing passwords, ought to be executed to restrict exposures and stay away from incidental exposures to safeguard sensitive medical care data and diminish cyberattacks [3]. Notwithstanding developing danger of cyberattacks in medical care, the research on this point is early and there are significant gaps in its literature [11].

II. Types of Cyberattacks

There have been a few endeavours to classify cybersecurity threats [12]. Every one of these studies has used an alternate set of criteria to classify cybersecurity in view of the reason, severity, scope, and legality of cyberattacks [4]. We examine the major types of cyberattacks and the motivations driving them.

1.2. Denial of Services (DoS)

The point of a DoS attack is to flood a network with traffic to disturb service and prevent users from getting to network resources [13]. This type of attack is prepared to do fundamentally slowing or shutting down the network of a health care organization. The attack on Boston children' Medical clinic in 2014 is an illustration of how "hacktivists" deployed a distributed DoS attack to disturb the network of a several organizations [14]. Notwithstanding the monetary losses connected with re-establishing systems after a DoS attack, it is especially dangerous as it can prevent health care suppliers from getting or sending crucial data during the attack.

1.3. Privilege Escalation

Privilege Escalation attacks are driven by the objective of accomplishing a more significant level of access to an organization or program; they are typically executed by taking advantage of weaknesses in a program or organization [15]. Hackers could choose to utilize the elevated access to do various things to the system, like changing a patient's visit data, consequently, compromising the patient's safety. There are two major types of Privilege Escalation attack: vertical and horizontal [16]. "Multi-layered attacks" can likewise use malware to Privilege Escalation on a system and inflict considerably more damage.

1.4. Man in The Middle (MITM) or Eavesdropping

An Eavesdropping attack is viewed as a kind of reconnaissance attack [4]. It happens when an intruder catches communication between two parties [17]. The attacker eavesdrops on the items communicated by secretly acting as an intermediary in the data exchange. The integrity of the information communicated can easily be compromised since the intruder is fit for modifying the information’s prior to transferring it to the next party or groups, unbeknownst to them. In healthcare, an eavesdropper could get access to private data and even blackmail patients. Man-in-the-Programs (MITB) attacks built on MITM attacks by working with the attack remotely. The most complex MITB attacks use Trojan malware that is fit for evading antivirus programs [18].

1.5. Cryptographic Attack

A cryptographic attack is completed fully intent on uncovering data that has been hidden; all in all, it tries to decode encrypted data [19]. Cryptography is the way of encrypting and decrypting into codes, so just the sender and planned recipient can understand it [20]. The binary coding obscured to others in light of the fact that the algorithms utilized in encrypting the data are only accessible to its creator [21].

1.6. Structured Query Language

Several sites utilize the programming language structured Question Language (SQL) to deal with their databases. Vulnerabilities in SQL might be taken advantage of by programmers to execute malicious "payloads" (harmful SQL statements) that cause the information servers to uncover data. During such a SQL infusion assault, programmers can change the data in the database, affecting the integrity, confidentiality, and accessibility of data stored on that database [22]. In 2015, weakness in variant 3.3 of Revelation Cardio Server, a central web application that manage data for hospitals, was found that could consider a SQL injection to exploit it [23].

1.7. Malicious Software

Malware or Malicious Software alludes to a group of programs that are intended to damage or compromise a computer system without the permission of the user [24]. These programs do different capabilities that incorporate altering, damaging, spying, or deleting user data. Malware is spread either actually utilizing an outer drive or through web downloads, for example, "phishing" messages. Some normal malware are worms, bots, viruses, adware, Trojans, spyware, secondary passages, ransomware, and rootkits.

1.8. Virus

A virus, the most common malware, self-spreads without the consent of the user and infects different computers [25]. Viruses are usually malicious; they perform actions like corrupting or deleting data [26]. Despite the fact that infections are self-propagating, they require user activation to exact their impact but replicate automatically [25]. The requirement for user activation is because of the fact that most of viruses are executable files connected to have host file. In 2017, a virus shut down the computer system at Erie country medical Centre in upstate New York and delayed performance as laptops must be distributed to staff so they could access backed up patient data [27].

1.9. Trojans

This piece of malicious software is designed to show up as helpful, real legitimate software [25]. One more significant component of a Trojan is that, dissimilar to viruses and worms, this sort of malware isn't self -replicating and does not need a host file [25, 28]. Trojans can give hackers a "backdoor" to permit access to an infected system [25]. The Alaska department of health and Social services was hit by a Trojan attack, and two computers were found to have malicious software that masqueraded on the appearance of legitimate applications [29]. It is conceivable that the Trojan had proactively made a backdoor through which patients' records were uncovered.

1.10. Spyware

Spyware is "a software installed on a computer without the user's knowledge and sends data about the user's computer activities over the internet" [30]. Spyware works covertly on a system and permits the attacker to monitor the target's utilization and gather individual data [31, 32]. A spyware can come as a Trojan used to carry MITM attacks. Spyware can likewise slow down computers, commonly by overworking behaviour the system [31].

1.11. Ransomware

Recently, stories of ransomware attacks have turned into an everyday title in the news [33]. A central feature of this type of malware attack is the interest for ransomware to deliver for decryption of data [33]. Ransomware, notwithstanding, can utilize one of the several different kinds of malware to hack an organization. Sporadically, as well as encrypting the victim's data, the hackers threaten to sell or expose the data to the public if the ransom is not paid. The 2017 attack on Britain's National Health Services (NHS) was facilitated with utilizing ransomware named Wanna Cry (also called Wanna Crypt). This attack hindered patient care all through the health system [34].

1.12. Phishing

The utilization of social engineering to trick individuals or organizations into either uncovering data or perform an action harmful to their computer is alluded to as phishing [35]. Phishing is more a strategy or a vector as opposed to a type of attack. It is one of the most widely recognized approaches to delivery malware [36]. Attackers generally utilize emails that divert the recipient to a website, which either gathers their data or prompts the download of malicious software. Spear phishing is a type of malicious

phishing that is directed at certain individuals or organizations [37]. New York's largest provider, Kaleida health, was breached two times in2017 utilizing the spear phishing technique and in excess of 3000 patient records were compromised [38].

1.13. Worms

Dissimilar to viruses, worms don't depend on a host file to run, self-replicate, or propagate [25]. Scattering of worms as a rule relies upon vulnerabilities in the target system or through social engineering [25]. The Wanna Cry that affected Britain's NHS is a worm by design [34].

III. Major Players in Cybersecurity

The key part in cybersecurity incorporate a large group of individuals and organizations that range from software designers to end-users [19]. These players incorporate hackers, cybersecurity professional, software developers, government regulators, and end users. Every one of these individuals assumes either a basic part in defending or endangering cybersecurity. A profound comprehension of their roles in accomplishing cybersecurity and a recognition of their limits will help healthcare organizations in better planning to prevent cyber breaches.

3.1 Cyber- attackers

Cyber-attackers comprise the principal danger to cybersecurity. Cyber-attackers are the principal reason that Cyber-attackers exists. Understanding the inspiration of the different types of cyber attackers can serve as a foundation for building strong cybersecurity protocols. A hacker is an individual that looks for to gain remote access to information's regardless of approval [39]. Nonetheless, when the endeavour is made without a malicious or criminal intent and under the suitable approval, it is alluded to as ethical hacking [40]. Subsequently, the intent and approval status decides the type of attacker. Attackers utilize one or a mix of cyberattack methods to accomplish their goals. Fischer (2016) comprehensively classified cyber attackers into hacktivists, terrorists, spies, and criminals [41]. This characterization is like Goderdzishvili's grouping of cyberattack based on legality in2010[42]. Under these two author's' characterization, cybercriminals are people that utilization a computer to carry out violations like robbery or blackmail, and their inspiration is generally money related. Hacktivists, be that as it may, are energized by nonmonetary inspirations; they participate in cyber-attacks to promote their political plan. The two studies defined cyberterrorists as people that are engaged with the purposeful interruption of computer networks. Cyber terrorists could have a place with either subnational or clandestine gatherings. Attackers engaged with undercover work are cyber spies who snoop on sensitive classified or proprietary materials having a place with one or the other government, private companies, or individuals.

3.2 End Users

End users likewise assume an essential role in guaranteeing cybersecurity. End users can be either malicious or non- malicious players, and both present a particular kind of threat. End users have shown to be a "weak link in protecting organizations against some cyber-attacks strategies [43]. A study of more than 900 breaches in 2010 uncovered that insiders who are either current or previous employees were liable for coordinating 48% of all data breaches in the study, and just 10% of the occurrences were unintended [44]. Malicious insiders are considered very dangerous since they are familiar with strengths and weakness of the system [45]. Be that as it may, non- malicious end users likewise act as a gateway for cyber-attacks. For instance, spam emails that convey a cyber-threat spread only because somewhere along the system, a spammer is involving somebody's machine as a host [46]. In a review in 2013 by the SANS Organization, half of the responders consider non- malicious users the top danger to cybersecurity [47]. Regardless of whether health organizations execute the best security protocols, neglecting to prepare their workforce, for example end users, leaves them susceptible to cyber-attacks. To be completely fully capable of preventing cyber security, the organization should set up their workforce. Employee and human security testing should also be a priority [49]. It ought to be noticed that security policies set up to protect networks against cyber breaches might be a cause of nuisance for end-users. In like manner, cyber security culture in an organization requires getting the upfront investment of end-users and understanding their needs [19].

3.3 Cyber Defenders

The cyber defenders are an umbrella term that we adopt for an immense range of individuals that are effectively working to guarantee cyber security. These incorporate IT professionals (cyber security experts) and government agencies. Information technology experts that work to guarantee cybersecurity go by various titles; among the commonly used titles for them are

security engineers or architects, security analysts, IT directors, and system administrator [50]. Their essential job is in arranging and executing security efforts to guarantee that their organization is safeguarded from cyber threats [51]. The health care field is as of now confronting a lack of cyber security experts. This shortage is credited to low pay and lacklustre selecting endeavours [52].

A several government divisions are charged of protecting cyber security, for example, the department of homeland Security and department of justice are liable for capturing and charging cybercriminals, respectively [41]. Other government agencies like the national institute of standards and technology (NIST) add to the development of frameworks for guaranteeing cyber security [53]. Congress has as of late played an active role in creating regulations pointed toward mitigating cybercrimes.

3.4 Developers

Developers are fundamental to guaranteeing cyber security as it is their mistakes that cyber attackers exploit to breach systems. Malware can be easily brought into a network when there are mistakes in Developers [54, 55]. An expected 90% of security episodes occur through exploiting vulnerability in a software program [56]. For instance, the Wanna cry ransomware attack of 2017 that impacted over 99 nations exploited vulnerability in Microsoft Server Message Block (SMB) in Windows [57]. Vulnerabilities like this one are pervasive and growing in number. The National Vulnerability Data base of NIST as of now records in excess of 100,000 Common Vulnerabilities and Exposures (CVS) in its data base [58]. While a several organizations decide to invest in protecting their organizations, many breaches really happen at the application layer [59]. The obvious detach among developers and defenders also strains defenders and ultimately weakens cyber security [60]. In a study of developers by SANS in 2015, it was found that under 20% of security testing is led by the development group or quality assurance staff in an organization [60]. To strengthen the backbone of cyber security, security-risk-aware programming standards should be applied in developing software [61]. Also, the data silo that exists among developers and defenders must be broken [60].

IV. PROPOSALS

Cybersecurity issues threaten access, quality, and cost in medical services. Innovation offers confident options for every one of these objectives, yet to understand the advantages of these technologies, cybersecurity issues should be settled.

4.1. Policy Makers

1. In dealing with cyber security, policymakers face a continually developing target. For instance, when the significant utilize incentive program was first established, handheld mobile devices were a moderately minor piece of eHealth, contrasted with more recent times. Moreover, the regulatory process takes time and can be difficult to change. Thusly, policymakers will probably persistently be in a catch up mode as they attempt to develop cyber security policies. For instance, despite the fact that HIPAA regulations have been updated (for instance to deal with the issue of business associates), as technology changes, it can be expected that HIPAA will need to evolve further [62].

2. Policymakers ought to take note of that major government programs, like medical care, Medicaid, and the Veterans Health Administration (VHA) could have explicit program goals that are threatened by cyber security issues. For instance, these programs should support alternative delivery approaches using technology (for example, telemedicine). Throughout the past few years, VHA has started to make significant investments in telehealth. Thusly, policymakers should manage cyber security both according to the perspective of the threat to our society in general, and furthermore according to perspective of the threat to specific government programs.

3. Cybersecurity issues in healthcare are connected to the larger set of cyber security issues in the society. As advancements happen, policymakers might need to modify the regulatory environment to allow technological developments to be applied to healthcare. For instance, some observers accept that block chain technology offers the chance of exceptionally secure, decentralized, and longitudinal health records [63]. This technology would probably require regulatory changes. For instance, HIPAA's 1996 security, privacy, and transaction sets are not lined up with block chain technology [64].

4.2. Medical Services Organizations

1. For medical services Organizations, cyber security includes compromises. For instance, an Organization might consider upgrading privacy by expecting that a patient award approval before a specialist might get to the patient's data. In any case, that could postpone the completion of the referral. Actually quite significant cases handling staff and insurance company staff

approach a large part of the patients' data [65]. Likewise, cyber security measures might utilize significant assets. Monetary expenses are by all accounts not the only worry in such manner. There is additionally the open door cost of key IT staff. In taking into account cyber security drives, it has been proposed that governance ought to adopt the strategy that they are dealing with a "portfolio" of IT projects, and that the utilization of staff on one project will make that staff inaccessible for other projects. There is a broad writing on project portfolio management in such manner [66].

2. One worry for concluding HIT risk trade-offs is the idea of "hiding in the bell curve". An organization would rather not badly trail their peers in meeting a regulation; in any case, there is probable little to acquire by going through the cost of enormously outpacing their peers. If instead an Organization is in the middle of the peer group, it is probably not going to be the focal point of regulators or firmly disadvantages competitively [67].

3. Healthcare Organizations, similar to any Organizations, need to adopt a complete strategy to cyber security instead of an ad hoc methodology of managing dangers dependent upon the situation as they are found. The ad hoc process faces a troublesome challenge in sufficiently distinguishing and addressing to all arising security gaps. Security ought to be seen with regards to processes, and not explicit technological fixes. Concerning security issues, Schneier expressed, " If you think technology can solve your security problems, then you don’t understand the problems and you don’t understand the technology." [68].

4. One example of comprehensive approach to deal with cyber security is the CERT Resilience the Management Model [69]. With regards to this model. " resilience " is the capacity of an organization to endure an effect, proceed with operations, and return to the original condition. The model incorporates a detailed evaluation of process areas all through an organization. This comprehensive methodology incorporates laying out a governance structure over each process, and guaranteeing that planning, training, financing, and different factors are sufficient to accomplish required resilience in each process area.

5. Another methodology is risk the management. This approach implies a risk evaluation that starts with distinguishing potential risks. When each risk is recognized, the specific asset and vulnerability are determined. Next a risk evaluation is created in view of the probability of an unfriendly occasion, the effect in the event that occasion happens, and any safeguards as of now set up to lessen the impact of the occurrence. Then next step is mitigation planning, where a particular step is distinguished, an individual is made responsible, and a due date is assigned. The activity is then monitored and a reconsidered evaluation of the risk is made following the mitigation. Customarily the various ways to deal with risk management have been classified under the headings of mitigating risk, avoiding risk, transferring risk (for example through insurance) and bearing risk [70, 71]. To keep away from biased predispositions and cover-up, risk assessment can be directed through external parties.

6. The decision of chance management strategies has been impacted by the arising field of cyber insurance. Policies might be bought that cover costs related with data breaches, including "notification expenses, credit monitoring, expenses to define claims by state regulators, fines and penalties, and loss coming about because of identity theft" [72]. Vaughan and Vaughan give "rules" to assist with directing the choice about how to respond to explicit risks during the risk management process, including a "tool" that distinguishes which risks ought to be guaranteed against [73]. Notwithstanding, the medical care organizations ought to have a clear comprehension of what is covered under cyber security and under which circumstances.

7. Another choice for a comprehensive methodology is to coordinate cyber security into the strategic planning and budget process. After some time, there has been a change of the role of IT in the planning process. At first, the IT director was considered to be an "applications provider" and was not a part of the strategic planning process. Nonetheless, it has since been perceived that spending on IT was frequently conflicting with the organization's essential objectives, and subsequently efforts were made to "strategic adjust" the objectives of the organization and the IT budget. This was followed by recognition that the IT manager could be considered to be a "strategic contributor" (rather than responding to a completed plan), and be a part of the planning group that is leading the "strategic evaluation". One objective was IT fusion, which exists when there is a high level of arrangement among IT and the remainder of the organization. Expanding on this idea, Bensaou and Baron discussed the possibility of "strategic instinct" [74]. They highlight the case of Japan where IT investments will generally be made not in light of explicit objectives, but because the investment is fundamental to the long-range targets of an organization.

8. In another exhaustive methodology Cook attempts to produce a "trust framework" by making layers of protection [75]. The first layer of protection is risk management; and the subsequent layer is data assurance strategy that covers policies for security, privacy, and safety. The third layer comprises of physical safeguards, for example, workstations and devices. The fourth layer is operational safeguards, for example, training, assigning a security officer, and continuity of operation planning. Layer five

is architectural standards, managing interoperability, accessibility, and dependability. Layer six is a technology safeguard with respect to data encryption, access control, audit controls, and security against malevolent software. Layer seven is ease of use elements, for example, single sign-on. These layers are supposed to cooperate to make reliability for data security and privacy.

9. Training status and file employees is important. There is an adage in cyber security that goes "You are only as safe as your 'most vulnerable' individual". A key concern is countering efforts at social engineering. Contingent upon the conditions, other safeguards might be set up. For instance, one type of social engineering includes leaving a USB drive in a worker parking lot hoping that an employee will take it inside and try to determine what is on it. Such risks are countered by not having USB drive ports on computers. One more progressively significant area for training is the suitable and preventative utilization of handheld devices.

10. A hospital -specific methodology is recommended by the American Clinic Association (AHA), which proposes six actions to oversee cyber security risk [76]. Three of the six include planning. These are developing a reaction plan: laying out techniques, cyber security teams, and testing the reaction plans. The AHA proposes that the arrangement be "mindful" of NIST's Cyber Security System [77]. The other three activities focus around specific issues: explore all medical devices following FDA rules, take part in data sharing organizations that distinguish new risks confronting hospitals, and ensure protection covers cyber security risks [78].

11. Another potential strategy could be observing the user's ways of behaving and utilizing the identity and access the management protocols.

V. Best Practices

Considering the rising dangers presented by cyber breaches to the health care industry, cyber security ought to be viewed as a crucial shield for the endurance of any health care organization. The cyber security insurance also called digital responsibility or cyber liability insurance is an extraordinary protection offering that is intended to mitigate the financial liability that might result from harms or losses brought about by a breach. [79,80] Since not at all like traditional insurance policies, the underwriting of this policy has no standard format, healthcare organizations that try to buy such policies ought to guarantee the following:

(1) At a base, a healthcare organization ought to guarantee that their policy covers three areas: liability coverage against claims for harms from theft, loss, or unapproved disclosure of data; inclusion for liabilities from regulatory fines like those including HIPAA and HITECH; and coverage against losses from business interruption. [81]

(2) Before buying a policy, health care organizations ought to perform a comprehensive evaluation of their information technology security capabilities and need.18 This assessment ought to be a collaborative exertion of all organizational stockholders. In particular, there ought to be a representative from the legal team, IT leaders, head of security, and organization and business leaders. These will inform the organization as to the best policy that is appropriate for their organization.

(3) They ought to likewise can bargain for a fair and thorough arrangement that doesn't leaves gaps that expose them to liabilities. [79] For example, a healthcare organization ought to guarantee that their strategy covers ransomware attacks since not all policies cover such events. Organizations ought to likewise guarantee the utilization of correct terminology in drafting the underwriting. [79]

(4) Since third-party contractors are generally liable for 41% of the breaches in health care organizations, it would be judicious to guarantee that the policy covers events that include third-parties were necessary. [82]

Policymakers likewise play a significant role to play in further developing cyber security protection in health care. The expense of cyber security insurance payments might preclude smaller, low-resourced healthcare organizations, including rural and safety-net hospitals, from having the option to manage the cost of it. These organizations could be compelled to close in light of a cyber-breach, leaving their former patient population with substantially more restricted access to care. Such bankruptcies could worsen the health disparities that as of now exist among these populations. [83] Moreover, policymakers ought to advance cyber security protection since it very well may be utilized as a tool for further developing cyber security that protects valuable patient data. This is on the grounds that insurance companies can offer lower charges for hospitals as an incentive for meeting specific security requirements. [84] Considering the possible net positive effects of cyber security insurance on the society, policymakers ought to empower its adoption through dynamic and robust policies.

A beginning stage for policymakers will be the improvement of health care area explicit cyber security regulatory principles. While several guidelines exist for the regulation of cyber security in general like the national institute of standards and technology (NIST 800-53), international organizations for standardization (ISO27001), and centre for Web security (CIS) critical controls, there are no regulatory standards specific for the health sector that consider its unique needs. [85] Such healthcare explicit regulatory standards could further develop cyber security practices across organizations. The standards could likewise advance the entry of new insurance organizations into the health care cyber security protection marketplace, and support price competition, where there is right now a shortage of such companies.12 price competition may at last prompt a diminishing in price competition premiums.

It is essential to take note of that price competition protection ought to be just be a part and not the sole way to deal with relieving the risk of cyberattacks. This is on the grounds that even the most robust insurance policy won't cover or repay for the damage in reputation an organization experiences after a cyber-breach. Furthermore, cyber security insurance may not cover losses including legitimacy classified data and fall in stock prices because of a breach. [86,87] In this manner, these policies ought not be viewed as a long term solution for security concerns. Besides, overreliance on cyber security protection could likewise put organizations at more risks of cyber breaches since they don't bear the monetary responsibility from such occurrences, a term alluded to as moral hazard. [88] It is additionally essential to take note of that since the ideas of cyber security and its insurance are generally new, potential dangers are dynamic and changing daily. [90] Consequently, best practices will undoubtedly keep developing with evolving dangers. [89]

Notwithstanding cyber security, health care organizations ought to likewise think about the accompanying risk management strategies:

Health care organizations ought to be proactive not reactive to cyber threats or cyberattacks. For example, health care organizations ought to plan and direct efficient educational training programs for employees and other end users to assist them with being more mindful of cyber security issues. [91,92]

(1) Collaborations and sharing of data about best practices on cyber security with other organizations in the health care sector, or with similar firms, ought to be encouraged. [91,92]

(2) Adoption of new and imaginative techniques for safeguarding individual health records. For example, the execution of block chain innovation based systems through which health care suppliers, payers, and patients could share information on a decentralized network that are hard to breach. [93]

(3) The extreme objective of cyber security ought to be to fortify resilience. Resilience healthcare systems will find reasonable ways to work on their security and safeguard their organizations and won't rely entirely upon cyber security insurance. [85]

(4) Maintaining secure and up to date backup data to keep away from long-lasting loss in the case of a cyberattack is necessary. [94] In this process, unique thought ought to be sent to where the backup data are stored. [94]

(5) Since there are deficiencies of health care cyber security experts, health organizations ought to pursue attracting, retaining and training cyber security staff. [2]

VI. Conclusion

Data breach is a rising danger to health care organizations. Several factors add to this danger, among these elements is the richness and complexity of data health care organizations manage. Such breaches likewise present serious malicious results to these organizations that incorporates however are not restricted to monetary losses and dangers to patient security. Because of the high prevalence and adverse consequence of this danger, health care organizations are progressively adopting cyber security as a mitigation strategy. In any case, this sector actually lags behind other basic businesses. For those that have adopted the cyber security insurance policies, complains of underinsurance abound. To accomplish ideal adoption of cyber security insurance and further develop the insurance utility for health care organizations, these organizations really must perceive the extent of possible risk from breaches they face, and the best practices in choosing a policy that mitigates them. Policymakers likewise play a role in extending and improving the availability and affordability of such insurances by designing regulatory standards for cyber security that are specific for health care.

GLOSSARY

Cryptographic an attack carried out with the intention of attack revealing information that has been concealed.

Cyber-attack The act of intentionally disrupting data information.

Data breach This is when information is lost, stolen, displaced, hacked, or communicated to unofficial recipients.

Denial-of-Services an attack that aims to flood a network (DoS) with traffic in order to disrupt service and prevent users from accessing network resources.

Malicious Software group of programs that are designed to or Malware harm or compromise a computer system without the permission of the user.

Man in the Middle A reconnaissance attack in which an

(MITM) or Eavesdropping	intruder intercepts communication between two parties. The attacker eavesdrops on the contents communicated by secretly acting as an intermediary in the information exchange.
Phishing	The use of social engineering to trick individuals or organizations into either divulging information or perform an activity harmful to their computer.
Privilege escalation	Attacks driven by the goal of achieving a higher level of access to a network or program; they are usually executed by exploiting vulnerabilities in a program or network.
Spyware	A software that is installed on a computer without the user's knowledge and transmits information about the user's computer activities over the Internet.
SQL Injections Exploit	Attack that exploit vulnerabilities in SQL to execute malicious "payloads" (harmful SQL statements) that make the data servers divulge information.
Trojans	A type of malware designed to appear as useful, legitimate software.
Virus	A common malware that self-propagates without the permission of the user and infects other computers.
Worms	A type of malware that does not rely on a host file to run, self-replicate, or propagate.

CONFLICT OF INTEREST

All authors declare no conflicts of interest.

AUTHORS CONTRIBUTION

Authors have equally participated and shared every item of the work.

REFERENCES

[1] Rajkomar, Alvin, et al. "Scalable and accurate deep learning with electronic health records." *NPJ digital medicine* 1.1 (2018): 1-10.

[2] Bhuyan, Soumitra Sudip, et al. "Transforming healthcare cybersecurity from reactive to proactive: current status and future recommendations." *Journal of medical systems* 44.5 (2020): 1-9.

[3] Karasz, Hilary N., Amy Eiden, and Sharon Bogan. "Text messaging to communicate with public health audiences: how the HIPAA Security Rule affects practice." *American journal of public health* 103.4 (2013): 617-622.

[4] Uma, M., and Ganapathi Padmavathi. "A Survey on Various Cyber Attacks and their Classification." *Int. J. Netw. Secur.* 15.5 (2013): 390-396.

[5] Filkins, Barbara. "Health care cyber threat report: Widespread compromises detected, compliance nightmare on horizon." *SANS Institute* 42 (2014).

[6] Berger, D. W. "Breach Report 2015: Protected health information (PHI). Red spin." (2016).

[7] McCue, Andy. "Beware the insider security threat." *CIO Jury* (2008).

[8] Perakslis, Eric D., and Martin Stanley. "A cybersecurity primer for translational research." *Science translational medicine* 8.322 (2016): 322ps2-322ps2.

[9] Akpan, Nsikan. "Has health care hacking become an epidemic." *PBS News hour* (2016).

[10] Smith, McKay, and Garrett Mulrain. "Equi-failure: The national security implications of the equifax hack and a critical proposal for reform." *J. Nat'l Sec. L. & Pol'y* 9 (2017): 549. Jalali, Mohammad S., et al. "Health care and cybersecurity: bibliometric analysis of the literature." *Journal of medical Internet research* 21.2 (2019): e12644.

[11] Jouini, Mouna, Latifa Ben Arfa Rabai, and Anis Ben Aissa. "Classification of security threats in information systems." *Procedia Computer Science* 32 (2014): 489-496.

[12] Arora, Arushi, Summit Kumar Yadav, and Kavita Sharma. "Denial-of-service (dos) attack and botnet: Network analysis, research tactics, and mitigation." *Research Anthology on Combating Denial-of-Service Attacks*. IGI Global, 2021. 49-73.

[13] Nigrin, Daniel J. "When 'Hacktivists' Target Your Hospital." *New England journal of medicine* 371.5 (2014): 393-395.

[14] Song, Chengyu, et al. "Enforcing Kernel Security Invariants with Data Flow Integrity." *NDSS*. 2016.

[15] Piscitelli, Ann-Marie. *Overcoming Learning Anxiety in Workplace Learning: A Study of Best Practices and Training Accommodations that Improve Workplace Learning*. Diss. University of Arkansas, 2021.

[16] Xiao, Liang, et al. "IoT security techniques based on machine learning: How do IoT devices use AI to enhance security?" *IEEE Signal Processing Magazine* 35.5 (2018): 41-49.

[17] Cain, Chris. "Analysing Man-in-the-Browser (MITB) attacks." *dated Dec* (2014).

[18] Langer, Steve G. "Cyber-security issues in healthcare information technology." *Journal of digital imaging* 30.1 (2017): 117-125.

[19] Merello, Marcelo, and Kailash Bhatia. "From the Reflex Hammer to Molecular Biology: Do Clinical Descriptions Still Play a Role in Our Neurological Decision Making? Jorge Luis Borges and the Analytic Language of Wilkins." *Movement Disorders Clinical Practice* 1.1 (2014): 1.

[20] Cho, Adrian. "Quantum spy games." (2014): 482-483.

[21] Williams, Patricia AH, and Andrew J. Woodward. "Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem." *Medical Devices (Auckland, NZ)* 8 (2015): 305.

[22] Blowers, Misty, et al. "The future internet of things and security of its control systems." *arXiv preprint arXiv:1610.01953* (2016). King, Christopher, Jonathan Chu, and Andrew Mellinger. *Emerging technology domains risk survey*. CARNEGIE-MELLON UNIV PITTSBURGH PA PITTSBURGH United States, 2015.

[23] Federal Trade Commission. "Consumer Information; Malware." (2015).

[24] Kraken, Johanna. "Analysis of malware-the Morris Worm." (2019).

[25] Virus. (n.d.). In Merriam-Webster's dictionary.

[26] Terry, Nicolas P. "Appification, AI, and healthcare's new iron triangle." *J. Health Care L. & Pol'y* 20 (2017): 117.

[27] Sainju, Arpan Man, and Travis Atkison. "An experimental analysis of Windows log events triggered by malware." *Proceedings of the Southeast Conference*. 2017.

[28] Kandasamy, Kamalanathan, et al. "Digital Healthcare-Cyberattacks in Asian Organizations: An Analysis of Vulnerabilities, Risks, NIST Perspectives, and Recommendations." *IEEE Access* 10 (2022): 12345-12364. Spyware. (n.d.). In Merriam-Webster's dictionary.

[29] OPERATIONS, US-CERT. "UNITED STATES COMPUTER EMERGENCY READINESS TEAM (US-CERT)."

[30] Lennon, Elizabeth. *ITL Updated Glossary of Key Information Security Terms*. No. ITL Bulletin June 2013 (Withdrawn). National Institute of Standards and Technology, 2013.

[31] Sharma, Rohit, and Mona Purohit. "Emerging Cyber Threats and the Challenges Associated with them." *International Research Journal of Engineering and Technology (IRJET)* 5.02 (2018).

[32] Ehrenfeld, Jesse M. "Wannacry, cybersecurity and health information technology: A time to act." *Journal of medical systems* 41.7 (2017): 1-1.

[33] Baker, Yolanda S., Rajeev Agrawal, and Sambit Bhattacharya. "Analyzing security threats as reported by the united states computer emergency readiness team (US-CERT)." *2013 IEEE International Conference on Intelligence and Security Informatics*. IEEE, 2013.

[34] Hummel, Richard. "Securing against the most common vectors of cyber-attacks." *SANS Institute* (2017): 1-31.

[35] Burns, A. J., M. Eric Johnson, and Deanna D. Caputo. "Spear phishing in a barrel: Insights from a targeted phishing campaign." *Journal of Organizational Computing and Electronic Commerce* 29.1 (2019): 24-39.

[36] Davis, J. "Hackers breach New York's largest provider with phishing attacks." (2017).

[37] Vogel, Sara, et al. "Languages, literacies and literate programming: can we use the latest theories on how bilingual people learn to help us teach computational literacies?" *Computer Science Education* 30.4 (2020): 420-443.

[38] Sunyaev, Ali. "Emerging technologies." *Internet Computing*. Springer, Cham, 2020. 373-406.

[39] Fischer, Eric A. *The Help America Vote Act and Election Administration: Overview and Selected Issues for the 2016 Election*. Congressional Research Service, 2016.

[40] Goderdzishvili, N. "Legal Assessment of Cyber Attacks on Georgia." *Data Exchange Agency Ministry of Justice of Georgia* (2010).

[41] Rhee, Hyeun-Suk, Cheongtag Kim, and Young U. Ryu. "Self-efficacy in information security: Its influence on end users' information security practice behavior." *Computers & security* 28.8 (2009): 816-826.

[42] Baker, Wade, et al. *Data Breach: Investigations Report, a study conducted by the Verizon RISK Team with co-operation from the US Secret Service and the Dutch High-Tech Crime Unit*. Technical report, Verizon, New Jersey, 2010.

[43] Wirth, Axel. "The economics of cybersecurity." *Biomedical instrumentation & technology* 51. s6 (2017): 52-59.

[44] Camp, L. Jean. "Reconceptualising the role of security user." *Daedalus* 140.4 (2011): 93-107.

[45] Filkins, Barbara. "New Threats Drive Improved Practices: State of Cybersecurity in Health Care Organizations." *SANS Institute* (2014).

[46] Cadwell, Zoe. "Pointing the Finger: Applying Extreme Environment Finger-mark Development to Forensic Archaeology." (2020).

[47] Evans, Mark, et al. "Human behaviour as an aspect of cybersecurity assurance." *Security and Communication Networks* 9.17 (2016): 4667-4679.

[48] Pescatore, John, and Gal Shpantzer. "Securing the internet of things survey." *SANS Institute* (2014): 1-22.

[49] Jarocki, Samuel, and Houssain Kettani. "Examining the efficacy of commercial cyber security certifications for information security analysts." *2019 4th International Conference on Information Systems Engineering (ICISE)*. IEEE, 2019.

[50] Conn, Joseph. "Low pay hinders healthcare's hunt for cyber cops." *Modern healthcare* 47.4 (2017): 23.

[51] Cybersecurity, Critical Infrastructure. "Framework for improving critical infrastructure cybersecurity." *URL: https://nvlpubs. nist. gov/nistpubs/CSWP/NIST. CSWP* 4162018 (2018).

[52] Zorabedian, J. "How malware works: Anatomy of drive-by download web attack." (2014).

[53] Rowe, Dale C., Barry M. Lunt, and Joseph J. Ekstrom. "The role of cyber-security in information technology education." *Proceedings of the 2011 conference on Information technology education*. 2011.

[54] Moteff, John, and Paul Parfomak. "Critical infrastructure and key assets: definition and identification." Library of Congress Washington DC Congressional Research Service, 2004.

[55] Bhuyan, Soumitra Sudip, et al. "Transforming healthcare cybersecurity from reactive to proactive: current status and future recommendations." *Journal of medical systems* 44.5 (2020): 1-9.

[56] DiPatrizio, Nicholas V., et al. "Endocannabinoid signal in the gut controls dietary fat intake." *Proceedings of the National Academy of Sciences* 108.31 (2011): 12904-12908.

[57] Morgan, Steve. "Is poor software development the biggest cyber threat." *htt ps://www. csoonline. com/article/297885* 8 (2015).

[58] Bird, Jim, Eric Johnson, and Frank Kim. "State of Application Security: Closing the Gap." *SANS survey, SANS Institute Reading Room* (2015).

[59] Teto, Joel Kamdem, Ruth Bearden, and Dan Chia-Tien Lo. "The impact of defensive programming on i/o cybersecurity attacks." *Proceedings of the Southeast Conference*. 2017.

[60] Fenton, Susan H., and Sue Biedermann. *Introduction to healthcare informatics*. AHiMA, American Health Information Management Association, 2014.

[61] Miliard, Mike. "How does blockchain actually work for healthcare." *Healthcare IT News April* 13 (2018): 2017.

[62] Miliard, Mike. "Block chain faces tough roadblocks in healthcare." *Healthcare IT News April* 13 (2018): 2017.

[63] Bhuyan, Soumitra Sudip, et al. "Too Much or Too Little? How Much Control Should Patients Have Over EHR Data?" *Journal of medical systems* 40.7 (2016): 1-4.

[64] Schwalbe, Kathy, and Dan Furlong. *Healthcare project management*. Minneapolis: Schwalbe Publishing, 2013.

[65] Bhuyan, Soumitra Sudip, et al. "Transforming healthcare cybersecurity from reactive to proactive: current status and future recommendations." *Journal of medical systems* 44.5 (2020): 1-9.

[66] Schneier, Bruce. *Click here to kill everybody: Security and survival in a hyper-connected world*. WW Norton & Company, 2018.

[67] Caralli, Richard A., Julia H. Allen, and David W. White. *CERT resilience management model: A maturity model for managing operational resilience*. Addison-Wesley Professional, 2010.

[68] Bhuyan, Soumitra Sudip, et al. "Too Much or Too Little? How Much Control Should Patients Have Over EHR Data?" *Journal of medical systems* 40.7 (2016): 1-4.

[69] Egenhoefer, Rachel Beth, ed. *Routledge Handbook of Sustainable Design*. London: Routledge, 2017.

[70] Carroll, R., and G. Norris. "Chapter 1 enterprise risk management in healthcare-the basics in Roberta Carroll (Editor) risk management handbook for health care organizations." (2011).

[71] Kim, Chang Yeon, and Kyungho Lee. "Risk management to cryptocurrency exchange and investors guidelines to prevent potential threats." *2018 international conference on platform technology and service (PlatCon)*. IEEE, 2018.

[72] Vaughan, Emmett J., and Therese M. Vaughan. *Essentials of insurance: A risk management perspective*. Wiley, 1995.

[73] Bensaou, M., and Michael Earl. "The right mind-set for managing information technology." *Harvard Business Review* 76.5 (1998): 119-130.

[74] Baker, Dixie B. "Trustworthy systems for safe and private healthcare." *in Essentials of nursing informatics* (2015).

[75] Middleton, Alyssa Ashlyn. "Pediatric oncology social work job analysis." (2022).

[76] ALDhanhani, Mohamed Jumah. "Review of Cyber Security on Oil and Gas Industry in United Arab Emirates: Analysis on the Effectiveness of the National Institute of Standards and Technology's (NIST) Cybersecurity Framework." *Turkish Journal of Computer and Mathematics Education (TURCOMAT)* 12.11 (2021): 714-720.

[77] Raghavan, Aarthi, Mehmet Akif Demircioglu, and Araz Taeihagh. "Public health innovation through cloud adoption: a comparative analysis of drivers and barriers in Japan, South Korea, and Singapore." *International Journal of Environmental Research and Public Health* 18.1 (2021): 334.

[78] Kabir, Umar Yusuf, et al. "Trends and best practices in health care cybersecurity insurance policy." *Journal of healthcare risk management* 40.2 (2020): 10-14.

[79] DAVIS, JOHNNIE R. *Healthcare Entities and Data Breach Threat Indicators and Deterrence: A Quantitative Study*. Diss. Northcentral University, 2022.

[80] Kim, Lee. "Cybersecurity: Ensuring Confidentiality, Integrity, and Availability of Information." *Nursing Informatics*. Springer, Cham, 2022.

[81]

[82] Carter, Barry E., Allen S. Weiner, and Duncan B. Hollis. *International Law: [Connected eBook with Study Center]*. Aspen Publishing, 2018. Tschider, Charlotte A. "Enhancing cybersecurity for the digital health marketplace." *Annals Health L.* 26 (2017): 1.

[83] Carter, Barry E., Allen S. Weiner, and Duncan B. Hollis. *International Law: [Connected eBook with Study Center]*. Aspen Publishing, 2018.

[84] Mkanta, William N., et al. "A 3-State Analysis of Black–White Disparities in Diabetes Hospitalizations Among Medicaid Beneficiaries." *Health Services Research and Managerial Epidemiology* 5 (2018): 2333392818783513

[85] Coventry, Lynne, and Dawn Branley. "Cybersecurity in healthcare: A narrative review of trends, threats and ways forward." *Maturitas* 113 (2018): 48-52.

[86] Martin, Guy, et al. "Cybersecurity and healthcare: how safe are we?" *Bmj* 358 (2017).

[87] Biener, Christian, Martin Eling, and Jan Hendrik Wirfs. "Insurability of cyber risk: An empirical analysis." *The Geneva Papers on Risk and Insurance-Issues and Practice* 40.1 (2015): 131-158. Perakslis, Eric D., and Martin Stanley. "A cybersecurity primer for translational research." *Science translational medicine* 8.322 (2016): 322ps2-322ps2.

[88] Gatzlaff, Kevin M., and Kathleen A. McCullough. "Implications of privacy breaches for insurers." *Journal of Insurance Regulation* 31 (2012).

[89] Shackelford, Scott J. "Should your firm invest in cyber risk insurance?" *Business Horizons* 55.4 (2012): 349-356.

[90] Coventry, Lynne, and Dawn Branley. "Cybersecurity in healthcare: A narrative review of trends, threats and ways forward." *Maturitas* 113 (2018): 48-52.

[91] Friedman, Sam, and Adam Thomas. "Demystifying cyber insurance coverage: Clearing obstacles in a problematic but promising growth market." *A report by the Deloitte Center for Financial Services* (2017).

[92] Astani, Marzie, and Kathryn J. Ready. "Trends and preventive strategies for mitigating cybersecurity breaches in organizations." *Issues in Information Systems* 17.2 (2016).

[93] Bordoff, Samantha, Quan Chen, and Zheng Yan. "Cyber-attacks, contributing factors, and tackling strategies: the current status of the science of cybersecurity." *International Journal of Cyber Behaviour, Psychology and Learning (IJCBPL)* 7.4 (2017): 68-82.

[94] Ivan, Drew. "Moving toward a block chain-based method for the secure storage of patient records." *ONC/NIST Use of Block chain for Healthcare and Research Workshop. Gaithersburg, Maryland, United States: ONC/NIST*. sn, 2016.

[95] Krisby, Ryan M. "Health care held ransom: Modifications to data breach security & the future of health care privacy protection." *Health Matrix* 28 (2018): 365.