BEST PRACTICES OF CYBERSECURITY IN THE HEALTHCARE INDUSTRIES

Mónica Cruz, Lizzette Pérez, Angel Ojeda

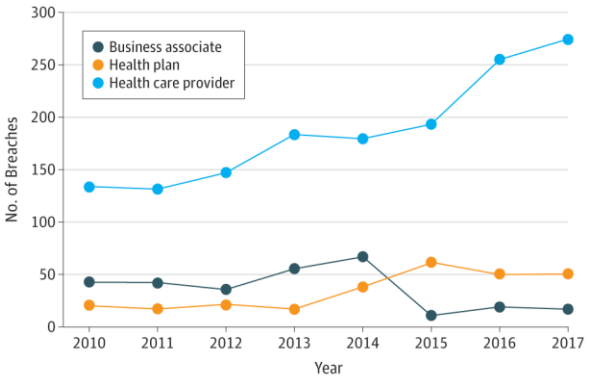
Abstract: The aim of this article is to present a literature review of what organizations in healthcare business do to protect the patients' private information, how breaches and vulnerabilities occurs, and the impact in healthcare institutions. The importance of reinforcement of information technology (IT) systems to protect it from cyberattacks. Forty-five articles related to the theme of cybersecurity, cyberattacks, healthcare institutions, HIPPA Privacy Rule, and patient's health information from 2015 to 2020 was used to write this article. Cyberattacks are easy to execute in devices that have weak IT or security systems. Healthcare institutions have the obligation to invest in strong software's to ensure the protection of patient's health information. In this article, we are going to present what healthcare institutions do to protect the patient's information to avoid the implications involving data theft and how these institutions reinforce its' IT systems to protect it from cyberattacks. How cybersecurity is affected, examples of cybersecurity threats, and the importance of preserving a patient's health information will be discussed.

Index Terms: Cyberattacks, cybersecurity, patient's health information, healthcare institutions, data theft, digital healthcare system

1 INTRODUCTION

The digital healthcare system is threatened by hackers to breach the critical infrastructure (Athinaiou, 2017). Hackers favor stealing health care records, which includes personal information like credit cards, financial, and banking records. "Stolen health care records have a longer shelf life and offer a higher payout on the black market" (Wendling, 2015). Data will breach in hospitals, doctor's offices, but the significant rate are done in the insurance companies (Sadakova, 2015). The social security numbers and credit card information can be sold in the black market or use to their benefit. Opportunities to benefit from the stolen healthcare data, such as identities, Medicaid, tax numbers, increase the value of selling this information online (Wedling, 2015). The advantage found in the health data over financial data is that social security number and date of birth cannot be changed, while economic data can be. Healthcare data used to trace other critical financial data (Kenealy, 2015). Other areas such as government, financial system, private sector have used sophisticated methods to protect their data, while the healthcare industry has been forced to embrace it quickly. The healthcare insurance business has suffered a data breach; over 80 million Americans had their personal information stolen. In 2014, data of over 1.1 million customers were exposed. Conversation from plan insurance is focused on cost and benefits; experts recommend changes to avoid breaches in the insurance company, leading to class-action lawsuits from plan members and damage to the employer's reputation. (Sadakova, 2015). A summary of breaches posted in the US Health and Human Service Office for Civil Right from 2010 to 2017, published by the Journal of the American Medical Association, where the trends in some breaches and number of records affected by business association, health plan and health care provider are shown. It states that healthcare providers are the primary source where the breaches occur (Figure 1).

The numbers below each year refer to the cumulative number of records breached up to that year. Business associate relates to entities that do not provide or reimburse health care but are given access to the Health Insurance Portability and Accountability Act (HIPAA)–protected data, generally to support physicians or health plans. A health care provider is a person or organization who furnishes, bills, or is paid for health care service; a health plan provides or pays the cost of, medical care (US Code of Federal Regulations 160.103). The four breaches of a health care clearinghouse were omitted for clarity. Retrieved by McCoy, T. H., & Perlis, R. H. (2018). Temporal trends and characteristics of reportable health data breaches, 2010-2017. Jama, 320(12), 1282-1284



Cumulative records breached, millions

Business associate	1.5	10.5	11.6	12.6	21.0	25.0	28.5	28.7
Health plan	3.6	3.7	4.0	4.1	6.2	109.1	110.0	110.4
Health care provider	0.8	5.0	6.3	12.1	14.1	20.5	32.7	37.2

***Figure 1**: Annual Breach Volume by HIPAA Entity Type*

One of the challenges that healthcare institutions face is the vulnerability of their systems. The digitalization of medical records and telemedicine using electronic equipment such as mobile phones, introduce the risk of cybersecurity vulnerabilities (Jalali, 2019). Medical personnel, such as doctors, nurses, and others, use many mobile devices, as part of his or her duties.

- *Mónica Cruz is currently pursuing a doctoral degree program in management in Universidad Ana G. Mendez in Puerto Rico, USA. Mónica Cruz has participated as speaker in local conferences. E-mail: mcruz428@email.uagm.edu*
- *Lizzette Pérez is currently pursuing a doctoral degree program in management in Universidad Ana G. Mendez in Puerto Rico, USA. Lizzette Pérez has participated as speaker in local conferences. E-mail: lperez535@email.uagm.edu*
- *Dr. Angel Ojeda is an associate professor of information systems at the Universidad Ana G. Mendez in Puerto Rico, USA. Dr. Ojeda has published articles in peer-reviewed journals on the topics of: Big Data, Data Warehouse, Social Media, Artificial Intelligence. Has participated as a speaker in international conferences in the Dominican Republic, Poland, USA, and Puerto Rico. Email: aojeda5@uagm.edu*

These devices are one of the more natural ways that hackers have access to the databases of these institutions. These personnel have the responsibility to protect organizations, and one big concern of this protection is cybersecurity (Howard, Harris, 2019). In 2019, a healthcare provider in a hospital in Georgia, USA, had an attack that exposed more than 278,016 individual records (Raja, A; 2015). A primary goal of the Privacy Rule is to assure that individuals' health information is adequately protected while allowing the flow of health information needed to provide and promote high-quality health care and to protect the public's health and wellbeing. To protect patient's information in healthcare institutions, in 1996, the United States Department of Health and Human Services ("HHS") issued the Privacy Rule to implement the requirement of the Health Insurance Portability and Accountability Act ("HIPAA"). The rule strikes a balance that permits important uses of information while protecting the privacy of people who seek care and healing. Large companies can have up to 100 attacks in its' IT systems in a year. Of these 100 attacks, one-third of these attacks end in "success" for the cybercriminals (Schaeffer, Brown, Graessle, Salzsieder, 2017). The primary guide to protecting healthcare information is the HIPAA law. Still, additional to this law, organizations have had an obligation to create other guides and policies to preserve systems of the cyberattacks. Kim (2017) wrote about the concern of the seriousness of cyberattacks and what some governments were doing about the cyber-attack problem and what they have been doing to strengthen cybersecurity. Within these concerns is the high cost of solving these cybersecurity problems. For example, in 2015, President Barack Obama recognized this seriousness and motivated CEOS, IT professionals, and others to act about this matter. With this initiative, President Obama's administration took the issue of cybersecurity protection seriously by implementing the 13636 Executive Order (The National Institute of Standards and Technology) and the Cybersecurity National Action Plan (CNAP). These aimed to maximize the cybersecurity policies to a more effective response to cyberattacks. Kim (2017) also mentioned some statistical information about cybercrimes. For example, the cost of cybercrime committed globally was 100 billion dollars; there are more than 1.6 billion social network users worldwide, with more than 64% of internet users accessing social media services online. Social media is the most vulnerable means of cyberattacks. One out of ten social media users are victims of cyberattacks, and the numbers are on the rise. From 2016 to 2019, global cybercrime costs are expected to increase, reaching US 2.1 trillion dollars substantially. The US government spent US 14 billion dollars on cybersecurity in 2016 with plans to spend 19 billion dollars in 2017.

2 LITERATURE REVIEW

CYBERATTACKS

Cyberattacks begin with elemental things, such as when someone clicks to a link. Also, it occurs with the use of infected devices (portable drives, disks, etc.). When someone clicks to a relationship, it can appear one of the following: virus, worm, or Trojan. A virus infects software and reproduces copies of itself when the software is opened. The worm infects software and spreads copies without the user acting. Trojan appears to be secure software but contains malware that acts when downloaded and opened (Conaty-Buck, 2017). Conaty-Buck (2017) mentioned some ways of cyberattacks, these are: ransomware, rootkits, keystroke, and adware. Ransomware is malware that keeps users from accessing their system or device or encrypts files until a fee (ramson) has been paid. Ransomware presents critical risks to both individuals and business organizations, hence the need to craft plans to tackle ransomware assaults. It is a type of malicious software that blocks access to the victim's data or threatens to publish or delete it unless a ransom amount is paid. Some simple ransomwares may lock the system in a way that is not difficult for a knowledgeable person to reverse. Still, others are more advanced and encrypt the victim's files and make them inaccessible, thereby demanding a ransom payment to decrypt them (Mago, Madyira, 2017). An example of ransomware is the case of CryptoLuck; that was an interesting case study. In this case, the payload comes in three parts, which are contained in a self-extracting archive: a legitimate Google updates executable GoogleUpdater.exe, a legitimate accompanying configuration file crp.cfg, and a malicious DLL file goodate.dll (Nieuwenhuizen, 2017). Rootkits hide malware from antivirus detections and removal programs. An example of a rootkit occurs over the past 25 years; countless rootkits have left their mark on cybersecurity. A few of them were legitimate, like the ones Sony launched in 2005 to improve copy protection for audio CDs, or a similar one, released by Lenovo in 2015 to install indelible software on its new laptops. Most rootkits, however, were developed by unknown hackers to compromise their victims' computers and obtain their personal information from them for their own, especially financial gain (Moes, 2020). Keystroke logger programs record user keystrokes to help cyber thieves acquire passwords. Exist two types of keystroke loggers, hardware, and software keyloggers. Michrandi Nasution et al., (2014) mentioned that keyloggers are used for the benefit of positive and negative examples. Positive benefits of keyloggers, among others, are, monitor the activities of employees or parental control children at home, and gather evidence of criminal activity. The negative examples of keyloggers can be used to steal identities, passwords, PINs, credit card numbers, or other confidential data secretly. Conaty- Buck (2017) mentioned that adware produces a code that automatically downloads malware. Occurs when the user receives an offer to remove the malware, but it is a program to activate the malware. One example of adware is when Google removed over 210 applications from the Play Store after checkpoint researchers discovered that they were infected with the same malware "SimBad" based on the abundance of infected simulator games, the code hid in a bogus ad-serving platform and created a back door that could install rogue apps, direct users to scam websites and show other apps in stores. Check Point believes the apps' developers were tricked into using the platform (Fingas, 2019). For data breaches, healthcare organizations pay high prices. This occurs because the violations of unsecured health information effect 500 or more individuals who must be publicly reported on the Office for Civil Rights (ORC). Also, each state establishes additional penalties for HIPAA violations. These penalties for noncompliance are based on the level of negligence, and federal fines can fluctuate from $100 to $50,000 per violation, with penalties of $1.5 to $5.5 million. To avoid these issues, healthcare organizations have had an obligation to design training programs for their employees to prevent cyberattacks. Other things these organizations do to educate them was telling the importance of password security, data encryption,

and patient education (Conaty Buck, 2017). Cyberattacks in health institutions are more susceptible due to the transfer of patient information in a variety of areas. For example, patient information for surgery must be shared in several regions (pharmacies, health insurance companies, the admission area of the hospital, or surgery centers). If IT systems are weak in some of these areas, data theft and cyberattacks could occur. (Howard, Harris, 2019).

CYBERSECURITY THREATS

Cybersecurity is a shared responsibility between people, processes, and technology to protect digital data and technology investments. Hackers found ways to defeat cybersecurity's barriers. Healthcare organization increasingly transmits electronic data through a mobile device, cloud base applications, medical devices, and other technologies infrastructure. Occasionally, organizations deploy technologies without cybersecurity safeguards or used with no protection, allowing hackers to attack it. Cyberattacks occurred during a period in were individuals use unsecured internet connection (Healthcare & Public Health Sector Coordinating Councils, 2015) There are many ways in which hackers can breakdown the system that causes breaches. Scientific communities recognize the weakness areas to unsecure the information. Strong focus in health IT systems without attention on security, creating a vulnerability to the cyberattacks (Ronquillo et al., 2018). The hacking incident and electronic medical record (EMR) breached on confidentiality health information was summarized by Ronquillo (2018), which shows breaches occur by media type and categories (Table 2).

	Breaches, *n* (%)	Records affected, *n* (%)
Hacking-related breaches by media type		
Portable electronic device or laptop	1 (0.3)	1911 (0.0)
Desktop, email, or EMR	106 (29.2)	1984418 (1.5)
Network server	192 (52.9)	119590428 (91.5)
Multiple types	48 (13.2)	8822024 (6.7)
Other/unknown	16 (4.4)	303597 (0.2)
EMR-related breaches by breach category		
Theft	21 (16.4)	146496 (3.0)
Unauthorized access or disclosure	66 (51.6)	377088 (7.7)
Hacking or IT incident	34 (26.6)	4240218 (87.1)
Multiple categories	5 (3.9)	102614 (2.1)
Other/unknown	2 (1.6)	1504 (0.0)

Abbreviations: **EMR: electronic medical record; IT: information technology**

***Figure 2**: Breakdown of hacking and EMR-related breaches*

Current health critical infrastructure is threatened by cyberattacks, targeted a physical aspect, with the objective of monitor, disrupt, destroy, and degrade, operations of the infrastructure (Athinaiou, 2017). A cyber threat not only challenges the services of the architecture, also the integrity of research environments and the consequences of working with identifiable and personal health information. Compliance is not the same thing as security. Security is a breach when rules are not adequately implemented (Perakslis,2016). All new services in the healthcare industry required personal information to receive services. Providing personal information to outside entities leads to losing control over the confidentiality of their data. The reliance creates a potential significant data breach if the healthcare organization that received the information does not apply adequate security measurements to protect the privacy of the data (Mariani,2015). Interconnection introduces vulnerabilities (possible breaches) to the healthcare systems. A growing concern of cybersecurity within the healthcare has resulted in a lack of medical information confidentiality (Kruse,2017) and the integrity of the data (Ross,2016). The interconnectivity provides numerous potential getaways to access remotely personal information, where previously paper records have been safeguarded in hospitals (only this accessible via to breach). Today the access due to the interconnection ended in more valuable resources for potential attacks. Previously, misplaced private document information or stolen laptop exposes the data for potential breaches. Today this information is electronically available on numerous networks, which has the potential of the offense to affect millions of people (Kam, 2015). Healthcare organizations are still using a legacy system allowing hackers and malware to easily avoid detection, the nature of the device's software may not be able to allow healthcare IT teams to access the internal software depending in the manufacture to build and maintain security (National Audit Office, Investigation, 2017).

PATIENT'S HEALTH INFORMATION

For Strauss (2015), each day, protecting patient information is becoming more meritorious, but, in some cases, are exceptions. Sometimes patient's reports must be shared to receive health care services. Also, it can be skipped when needed to safeguard the patient's health. When disaster relief situations occur, the entities involved have the authority to decide or inform how is the patient's health status. For example, The American Red Cross, public health authorities, and designated governmental agencies can have that authority. Also, when the patient is verbally disabled, entities can share the patient's health information if they believe if realizing this is in the best interest of them. Although the HIPAA Privacy Rule allows several exceptions to PHI, there are things not allowed. For example, protected patient information may not be disclosed on social and television media unless there is written authorization from the patient (Strauss, 2015). Another way to protect the PHI is, for example, when this information is used to make medical investigations, it is essential to eliminate the sensitive information of the patients before public availability of this investigation for external investigators and others. To protect patient's health information, investigators only use the relevant information. To do their research, they de-identify those files, which means that these researchers extract from the files of these patients just the information that is relevant to their studies. In this way, they maintain the confidentiality of the full archives of these patients elsewhere (Yang, Garibaldi, 2015). Patient's health information must be protected at all time. How organizations work with this matter is an enormous challenge. In many cases, even if patients sign a consent to protect their identities, this information may be shared with other organizations for medical equipment billing, or medicinal purposes. Also, in research for testing new drugs and treatments. For this purpose, it is unrealistic to obtain another consent when this information for research purposes in the medical area has no exceptions (Choi et al., 2015). Choi et al. (2015) mentioned that there are several methods to protect patient's health information if it is impossible to obtain consent of the patients participating in medical studies. For example, the institutional review boards (IRB's) intervention, but for its' interventions exists a lot of steps to take. These steps are: the research involves no more than minimal risk to the subjects; the waiver or alteration will not adversely affect the rights and welfare of the issues; the study could not practicably be carried out without the waiver or modification; and, whenever

appropriate, the subjects will be provided with additional pertinent information after participation. Another method to protect patient's health information to be used in secondary clinical data is anonymized the potential prospects for studies. With this exercise, researchers used the medical or clinical knowledge of the patients, but their names would not be disclosed.

MITIGATION PRACTICES

"According to a study from IBM Security and the Ponemon Institute, the cost of a data breach for health care organizations rose from $380 per breached record in 2017 to $408 per record in 2018." (Healthcare & Public Health Sector Coordinating Councils, 2015). Cyber-attacks interrupt healthcare's capacity to provide life-changing and life-saving capabilities. These cyberattacks occur through an unsecured internet connection. Organizations deploy technologies without proper protection, making them a target for hackers. Therefore, organizations should invest in technology and the protection of digital data. Effective cybersecurity should be shared between the individual (physicians, nurses, etc.), organizations, and machine learning (Healthcare & Public Health Sector Coordinating Councils, 2015). To reduce extensive areas of cybersecurity vulnerabilities, one can start at the individual level, by creating, updating, and protecting strong passwords. Then, at the organizational level, institutions must implement user authentication, data encryption, and frequent updates in software (Ronquillo, 2018). They are defining cybersecurity duties for employees, software up-dated procedure, virtual local area network (VLAN), use of de-authentication, data breach plan in place, cloud computing, and training employers (Kruse, 2016) support better controls for cybersecurity. Hospitals must pursue their cybersecurity efforts with their organizational objectives. Organizations must work with the criticality of "human factors" such as employee awareness, perceptions, and values in security management. Especially organizations designed for healthcare will help hospitals achieve a comprehensive and adequate security posture, as well as identify appropriate security controls to meet all compliance requirements (Mariani, 2015). Regulatory requirements will help ensure security measures and policies (Doherty & Fulford, 2006). Cybersecurity must be part of the risk management process, and cyber resilience must be ensured. Cyber resilience is a holistic view of cyber risk, which looks at the culture, people, and procedures, as well as technology (PWC Insurance, 2020). Factors identified to improve cybersecurity are maintaining basic cyber-hygiene and secure backups, which are essential to maintain resilience, to be able to recover quickly from possible attacks, to keep software up to date, and to ensure security patches are in place. Maintained confidentiality can be achieved through the anonymization of data, removing patient identification when it is used for research purposes, limiting access to online patient information. Investing and reinforcing in systems and processes to support secure data transfer (e.g., e-mail encryption and protection of online data) is required (N.C.S. Centre, 2016). Cybersecurity should be part of patient care culture, and insecure processes must be replaced (Levin, 2006). Culture change must be implemented from top to bottom; the metrics implemented should be applied through the Care Quality Commission (Martin, 2017) to ensure active engagement. The effectiveness of security culture has the potential that employees act in the effect of a 'human firewall' helping to protect electronic assets. Other precautions include staff not logging-in as a domain administrator, no sharing of login credentials or password, training staff to communicate the risks involved by the lack or lax security behaviors, and how security can be reached without exposing patient care (Martin, 2017). Under cybersecurity, there are activities, processes, and capabilities were the information, and communications systems contain protection from damages, unauthorized use, modification, or misuse utilization (Tschider, 2017). This requires a healthy cybersecurity practice, organizational process, and continued management supervision. In the cybersecurity field, the control process, administrative process, and procedures regulating human behavior, technical controls, computer mechanisms manage control, need to be implemented to complete cybersecurity programs (Northcutt, 2016). The cybersecurity field's objective is to protect the confidentiality, integrity, and private information (Craigen, et.al, 2014). Another area that should be carefully researched is the mobile social media application, which overwhelms the information-sharing perspective. Nevertheless, the advantage of this application is unprecedented. The privacy of the information is compromised. Healthcare applications are being developed for mobile devices, which is of great concern due to the sensitive information it contains (Al-Muhtadi, 2019). Mobile healthcare application is vulnerable to the attacks, exposing a threat to the data secured. The healthcare data vulnerability in association with the social network required double security as a person in social network security is more frivolous to reach (Delerue, He, 2012). Developing correct use of social media and security policies, routine monitoring of social media sites and internet activity, using the educational and training program, archiving social media content, and developing incident social media and response planning is critical (Delerue, He, 2012). Healthcare data is of interest to phishers and intruders; the availability of social media invites to an invasion. The integration of social media with physical infrastructure presents a viable solution for ensuring privacy and securing data (Al-Muhtabi, 2019). Evolution in devices used for social media indicates a change in consumer preferences in contemporary mobile technology, but choices on these devices are not articulate. Options for devices should take into consideration the technology know-how of end-users, local health systems, nature of the intervention, and availability of resources needed to support technology. This becomes more relevant as these solutions are targeted to community health workers and patients to promote self-control and health promotion in communities (Bassi, 2018). The Health Insurance Portability and Accountability act of 1996 (HIPAA) implemented safeguards to ensure protection from cybercriminals. Within these protections, one can find physical and technical safeguards. Physical safeguards incorporate workstation security, devices, and media control, and facilitate access control. Professional protection includes a unique user identification number, automatic logoff, emergency access procedure, encryption, and decryption (Kruse, 2017). The implementation of healthcare technologies is a process that requires planning and consistency. Organizations are finding a large amount of money for integration, but not enough on software updates (Kruse, 2017). Organizations within the healthcare sector must consider incorporating security into their organizational culture. Executives in charge of the data

information and technology need to conceive a mechanism to enforce stronger passwords and overcoming weak passwords. Passwords should use upper- and lower-case letters, combine letters in conjunction with numbers and special characters, require frequent changes, depending upon the sensitivity of the data, and avoid common words. A periodic review of the system access and institute of two-factor authentication criteria for remote access (Mariani, 2015). The cyberattacks consequences can be up to disruption of an operation to loss of sensitive data, lawsuits, loss reputation, regulatory inquires and penalties, bankruptcy, and business closure. Being aware of a strategy that understands the impacts of cybersecurity risk is critical to approach cyber resilience preparedness. Upper management must engage the immersion on strategy significance (Rothrock, 2017). Senior management needs to be on top and hands-on to learn about the organization's vulnerabilities and defense mechanism to participate in security review discussion, as well as be proactive in serving on different security governance committees. Managing cybersecurity risk is a balance between security and resilience (Abraham, 2019).

3 METHODOLOGY

This article was created from the review of literature of forty-five articles related to the theme of cybersecurity, cyberattack, healthcare institutions, HIPPA Privacy Rule (2000), and patient's health information from 2015 to 2020.

4 LIMITATIONS

This review was limited to journal articles focused on United States cybersecurity regulations laws targeted towards healthcare. Reports about cybersecurity, cyberattacks, and healthcare threats are the core of this study. A primary focus was the USA environment for private healthcare information, regulation, and cyber threats. Much of the work on cybersecurity and healthcare is operational and administrative, not academic (Jalali, 2019). A large amount of laws targeting healthcare in cybersecurity have been created and developed. Nevertheless, problems arise continually, which requires the government to continue growing and modifying regulation laws. Broader research could be done on future research. Broader refers to focus on other countries besides the United States. Cyberattacks and cybersecurity is a global problem. In the face of increasing the numbers of cybersecurity incidents, we should focus more on their current management of these incidents, how to prevent these (or at least decrease its' frequency), and the aftermath of the incidents. Future reviews could focus on how healthcare organizations and agencies are investing in reinforcing employee's education and training of cybersecurity for the protection of a patient's personal and private information.

5 CONCLUSIONS

It is increasingly imperative to protect the identity of patients to maintain their trust in hospitals and healthcare institutions. For this reason, it is indispensable and essential that these healthcare institutions invest in more robust information technology (IT) systems. In this way, they would avoid having to pay large sums of money if they become victims of cybercrimes. The measures implemented must be increasingly more robust because identity theft in healthcare institutions, medical and clinical services are economically more lucrative.

Healthcare institutions must implement more excellent controls on the use of mobile devices in their employees. Much of the access to information technology (IT) systems in these institutions to commit cybercrimes, sometimes, is through cell phones and other mobile devices. Cell phone companies, who are the owners of these devices, do not have good security controls to prevent these acts, making them extremely vulnerable and easy to be hacked. With the implementation of more reliable information technology (IT) systems, these healthcare institutions have higher profits because they do not have to make significant investments in restorations, demands, and other expenses related to cyber-attacks. With superior information technology (IT) systems, the chances of cyber-attacks happen are minimal, resulting in excellent benefits for these medical and clinical institutions. The complexity of healthcare cyberattacks continue growing, protect the private information, and management data, become critical. Strategy, technology, process, people, and environment become key issues for further controls. The integration between security and corporate culture, manage by people, will lead the future. Government agencies, intelligent technology, and determination of upper-level management, all together drive the future cyberculture to support the necessary steps to protect the privacy of information for the healthcare business.

REFERENCES

[1] Abraham, C., Chatterjee, D., et.al. (2019). Muddling through cybersecurity: Insights from the US healthcare industry. Business horizons, 62(4), 539-548.

[2] Al-Muhtadi, J., Shahzad, B., et.al. (2019). Cybersecurity and privacy issues for socially integrated mobile healthcare applications operating in a multi-cloud environment. Health informatics journal, 25(2), 315-329.

[3] Athinaiou, M. (2017). "Cyber security risk management for health-based critical infrastructures," 2017 11th International Conference on Research Challenges in Information Science (RCIS), Brighton, 2017, pp. 402-407

[4] Bassi, A., John, O., et.al. (2018). Current status and future directions of mHealth interventions for health system strengthening in India: systematic review. JMIR mHealth and uHealth, 6(10), e11440.

[5] Choi et al. (2015), Establishing the role of honest broker: bridging the gap between protecting personal health data and clinical research efficiency. PeerJ 3:e1506; DOI 10.7717/peerj.1506.

[6] Conaty-Buck, S. (2017). Cybersecurity and healthcare records. American Nurse Today, 12(9), p. 62-65.

[7] Craigen, D., et.al. (2014). Defining Cybersecurity. Tech Innovation MGMT, 13(15).

[8] Delerue, H., He, W. (2012). A review of social media security risks and mitigation techniques. J. Syst. Inform.Tech. 14, p.171-180.

[9] Doherty, N., & Fulford, H. (2006). Aligning the information security policy with the strategic information systems plan. Computers & Security, 25, 55-63.

[10] Fingas, J. (2019). 'SimBad' android adware was downloaded nearly 150 million times. Engadget, New York. Retrieved from https://search-proquest-

com.librarylogin.suagm.edu/docview/2191158618?rfr_id=info%3Axri%2Fsid%3Aprimo&accountid=28867#
[11] Healthcare & Public Health Sector Coordinating Councils (2015). Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients. U.S. Department of Health and Human Services. Office of the Assistant Secretary for Preparedness and Response. Retrieved from https://www.phe.gov/Preparedness/planning/405d/Pages/default.aspx
[12] Howard, D., Harris, C. (2019). Cybersecurity: What leaders must know (Discussion). American Association for Physician Leadership. Physician Leadership Journal, Vol.6(4), p.49-53.
[13] Jalali, M. S., Razak, S., et.al. (2019). Health care and cybersecurity: bibliometric analysis of the literature. Journal of medical Internet research, 21(2), e12644.
[14] Kam, R. (2015) The human risk factor of a healthcare data breach - Community Blog, Heal. IT Exch. Retrieved from: https://searchhealthit.techtarget.com/healthitexchange/CommunityBlog/the-humanrisk-factor-of-a-healthcare-data-breach/ (accessed May 12, 2020).
[15] Kenealy, B. (2015, March 30). Health claims data tempts hackers; Rethink needed on sector's cyber security. Business Insurance, 49(7), 0017. Retrieved from https://link-gale-com.librarylogin.suagm.edu/apps/doc/A407953413/AONE?u=turabo&sid=AONE&xid=cd50bc95
[16] Kim, J.E. (2016). Implications of cybersecurity on organizations and Obama administration's counter measures. Diplomatic Courier, p. 20-25.
[17] Kruse, C.S., Frederick, B., et.al. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends. Technology and health care: official journal of the European Society for Engineering and Medicine, 25 1, 1-10.
[18] Levin, D.Z., Christmann, P. (2006). Institutionalism, learning, and patterns of decoupling: The case of total quality management.
[19] Mago, M., Madyira, F. (2018) "Ransomware Software: Case of WannaCry," International Research Journal of Advanced Engineering and Science, 3(1), pp. 258-261.
[20] Mariani, D. M. R., & Mohammed, S. (2015). Cybersecurity challenges and compliance issues within the US healthcare sector. International Journal of Business and Social Research, 5(02).
[21] Martin, G., Martin, P., et.al. (2017). Cybersecurity and healthcare: how safe are we? BMJ 358: j3179, p. 2-4 doi: 10.1136/bmj.j31
[22] McCoy, T. H., & Perlis, R. H. (2018). Temporal trends and characteristics of reportable health data breaches, 2010-2017. Jama, 320(12), 1282-1284.
[23] Michrandi Nasution, S., et.al. (2014). Integration of Kleptoware as Keyboard Keylogger for Input Recorder Using Teensy USB Development Board. Retrieved from https://ieeexplore-ieee-org.librarylogin.suagm.edu/stamp/stamp.jsp?tp=&arnumber=7065954
[24] Moes, T. (2020). ¿Qué es un rootkit? https://softwarelab.org/es/que-es-un-rootkit/
[25] National Audit Office, Investigation: WannaCry cyber-attack and the NHS, 2017. Retrieved from: https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyberattack-and-the-NHS-Summary.pdf (accessed May, 12, 2020).
[26] N.C.S. Centre, 10 Steps to Cybersecurity, 2016.
[27] Nieuwenhuizen, D. (2017). A behavioural-based approach to ransomware detection. MWR Labs Whitepaper. Retrieved from: https://labs.f-secure.com/assets/resourceFiles/mwri-behavioural-ransomware-detection-2017-04-5.pdf
[28] Nguyen-Duy, J. (2018). The Cybersecurity Regulations Healthcare, Financial Services, and Retail Industries Must Know About. Interconnecting Business & Cybersecurity. Retrieved from: https://www.csoonline.com/article/3298962/the-cybersecurity-regulations-healthcare-financial-services-and-retail-industries-must-know-about.htmlt
[29] Northcutt, S. (2016). Security Controls. SANS Tech Inst., http://www.sans.edu/research/security-laboratory/article/security-controls.
[30] Office for Civil Rights (2000). Summary of the HIPAA Privacy Rule. U.S. Department of Health and Human Services. Retrieved from https://www.hhs.gov/sites/default/files/privacysummary.pdf
[31] Perakslis, E. D., & Stanley, M. (2016). A cybersecurity primer for translational research. Science translational medicine, 8(322), 322ps2-322ps2.
[32] PWC Insurance, Insurance 2020 & beyond, 2015. www.pwc.com/insurance (accessed May 7 2020)
[33] Raja, A. (2019, May 20). Healthcare Cybersecurity in 2019: Lessons We've Learned. Atlantic.net. Retrieved from: https://www.atlantic.net/hipaa-compliant-hosting/healthcare-cybersecurity-in-2019-lessons-weve-learned/
[34] Ross, R. S., L. Feldman, G.A. Witte, Rethinking Security through Systems Security Engineering, ITL Bull. - December 2016. (2016). https://www.nist.gov/publications/rethinking-securitythrough-systems-security-engineering (accessed May 12, 2020).
[35] Ronquillo, J. G., Winterholler, E., et.al. (2018). Health IT, hacking, and cybersecurity: national trends in data breaches of protected health information. JAMIA Open, 1(1), 15-19.
[36] Rothrock, R. A., Kaplan, J., & Van der Oord, E. (2017, November 16). The board's role in managing cybersecurity risks. MIT Sloan Management Review
[37] Sadakova, Y. (2015, June). Ask your insurance provider about cyber security. Benefits Canada, 39(6), S16. Retrieved from https://link-gale-com.librarylogin.suagm.edu/apps/doc/A422529102/AONE?u=turabo&sid=AONE&xid=7bd108bf
[38] Schaeffer, T., Brown, B., et.al. (2017). Cybersecurity: Common Risks. Strategic Finance, p. 54-61.
[39] Strauss, L. (2015). Protected Health Information in an Emergency. Journal of Health Care Compliance, p.59-60, 68.
[40] Tschider, C. A. (2017). Enhancing cybersecurity for the digital health marketplace. Annals Health L., 26, 1
[41] Wendling, P. (2015, May). Cyber thieves exploiting health care security gaps. OB GYN News, 50(5), 29. Retrieved from https://link-gale-

com.librarylogin.suagm.edu/apps/doc/A417310151/AONE?u=turabo&sid=AONE&xid=2e62cac0

[42] Yang, H., & Garibaldi, J. M. (2015). Automatic detection of protected health information from clinic narratives. Journal of biomedical informatics, 58, S30-S38.