International Journal of Scientific Research and Engineering Development-– Volume 5 Issue 1, Jan-Feb 2022

Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

Cyber security Risks in Health Care Industry

Mr. A Dhanu Saswanth[1], Dr.V Kavitha[2]

[1](Sri Ramakrishna Engineering College, Coimbatore, Tamil Nadu, India.
Email: saswanthsasu@gmail.com)

[2] (PG and Research Department of Computer Appications, Coimbatore, Tamil Nadu, India.
Email: kavithahicas@gmail.com)

----------**********----------

Abstract:

Cyber attacks are an increasing threat across all critical infrastructure sectors. For the health sector, cyber attacks are especially concerning because these attacks can directly threaten not just the security of our systems and information but also the health and safety of American patients. Globally, everything under constant cyber attack in the health sector, and no organization can escape that reality. The study said that the medical impact can be severe such as 58% of malware attack victims are small businesses, in 2017, cyber-attacks cost small and medium-sized businesses an average of $2.2 million, 60% of small businesses go out of business within six months of an attack as well as 90% of small businesses do not use any data protection at all for company and customer information.

Keywords **— Cyber Security, Cyber Crime, Mobile Network**

----------**********----------

I. INTRODUCTION

Cyber security threats are estimated to cost the world US $6 trillion a year by 2021, and the number of attacks has increased five-fold after COVID-19. Although there is substantial literature on the threats technological vulnerabilities have on the health care industry, less research exists on how pandemics like COVID-19 are opportunistic for cybercriminals. Through this article outlines why cyber attacks have been particularly problematic during COVID-19 and ways that health care industries can better protect patient data. The Office for Civil Rights has loosened enforcement of the Health Insurance Portability and Accountability Act, which, although useful in using new platforms like Zoom, has also loosened physical and technical safeguards to cyber attacks. This is especially problematic given that 90% of health care providers had already encountered data breaches. Companies must implement well-defined software upgrade procedures, should use secure networks like virtual local area networks, and conduct regular penetration tests of their systems. By understanding factors that make individuals, health care organizations, and employers more susceptible to cyber attacks.

As society has become increasingly technology dependent, it has also become increasingly vulnerable to cybercrime. Cyber security threats are expected to cost the world US $6 trillion a year by 2021, doubling from US $3 trillion dollars in 2015. This is particularly concerning for the health care industry, as cyber attacks are the leading cause of health security breaches. Since 2016, the health care industry has been the victim of more cyber security attacks than even the financial industry. Although there is substantial literature on the threats technological

vulnerabilities have on the health care industry, less research exists on how pandemics like COVID-19 are opportunistic for cybercriminals. In this paper, we provide a review of the literature on cyber security issues surrounding health care and discuss possible solutions to mitigate data breaches.

One of the primary reasons cybercriminals thrive during pandemics is because heightened emotional states like fear make victims more susceptible to falling for scams. According to the World Health Organization (WHO), the number of cyber attacks launched has increased five-fold during the COVID-19 pandemic. A similar phenomenon was seen in 2005 after Hurricane Katrina, where thousands of fraudulent websites appeared soliciting fake donations and offering false government relief. Cybercriminals often pretend to be credited and trusted organizations like the WHO and, therefore, exploit individual feelings of vulnerability in the uncertain times of a pandemic.

Additionally, health care organizations become prime targets during health crises. The use of telemedicine has proven vital to helping many patients during pandemics such as the COVID-19 crisis, especially as traditional in-person visits have become increasingly inaccessible. For example, New York University saw a 4330% increase in non urgent virtual visits after the outbreak of COVID-19. The Office for Civil Rights has loosened enforcement of the Health Insurance Portability and Accountability Act (HIPAA), which, although useful in opening up new platforms for care like Zoom, Skype, and FaceTime, has loosened physical and technical safeguards to cyber attacks. This is especially problematic given that 90% of health care providers had already encountered data breaches in the past with these safeguards. There is also a significant positive correlation between workload and the probability a health care worker will open a phishing email, which is particularly problematic in that, during pandemics, workloads can be at an all-time high.

Another potential problem for health care systems is the outbreak of ransom-motivated attacks. For example, the University of California, San Francisco (UCSF) was hacked by the cybercrime group "Netwalker," who demanded payment in exchange for not releasing confidential information. Out of fear of the consequences of this information's release, UCSF paid the group US $1.14 million. The same group also took over the Champaign Urbana Public Health District website. Similarly, the Hollywood Presbyterian Medical Center in Los Angeles paid US $17,000 to get a decryption key to regain access to their hospital system. Although they regained access, they lost 10 days of revenue and likely took a hit to their reputation. Unfortunately, however, complying with the demands of the cybercriminal may in fact be the most cost-effective solution, as a successful cyber attack costs an average of US $3.7 million to recover from. Additionally, failure to comply can pose a serious threat to patient safety.

Access to patient records is a gold mine for cybercriminals, as they often contain information like date of birth, insurance and health provider information, as well as genetic and health data—information that cannot be easily altered, unlike the case of a credit card being stolen. This information is particularly lucrative for hackers because a patient's health information can be sold for 10-20 times more than the amount for credit card information or even their social security number on the dark web.

Leak of this information can also compromise the physician-patient relationship. For instance, electronic medical record breaches could make patients less likely to disclose more private aspects of their medical history, which has the potential to impact their quality of care. Furthermore, the longer a health care provider's network is down, the longer those health care workers lack access to information critical to a patient's care, like comorbidities, blood type, and allergies, in times of crisis. The cost both financially and in terms of reputation and patient

safety can cripple already strained hospital operations.

One additional avenue of attack presents itself as a result of the increase in the number of health care workers working from home during a pandemic like COVID-19. In the attempt to transition employees to a work-from-home setup as quickly as possible, many employers fail to consider the potential security threats these new setups create. For instance, in the hospital or office, employees may be using secure internal computer systems and updated computers, but at home, the same employees could be using insecure or outdated devices that are more vulnerable to attack. Although many hospitals opted to use the Zoom platform because they view it as HIPAA-compliant, easy for both providers and patients to use, and cost-effective with medical videoconferencing accounts costing only US $200 a month, hacking of Zoom meetings has been a significant threat. Services like Zoom currently do not offer end-to-end encryption, making it not truly HIPAA-compliant, even though the Department of Health and Human Services Office for Civil Rights has relaxed enforcement of HIPAA's privacy rule during the COVID-19 pandemic.

Although the issue of how to safely administer health care during a pandemic is a complex one, it is clear that increased awareness is needed concerning the potential cyber threats that pandemics exacerbate. Awareness of these threats can help hospitals and their employees protect themselves and their patients from these vulnerabilities. For instance, being aware that hackers develop phishing scams containing buzzwords during a pandemic, like "WHO," "vaccine," or "donation," can be an essential step in reviewing and flagging such emails, thereby tightening security by the information technology (IT) departments. One technique that can be employed is to have hospital IT departments send out fake phishing emails to their employees and to require training for those who failed to report the phishing attempt. At the very least, this process can raise awareness among employees about cyber security concerns. Companies should also have well-defined software upgrade procedures, should use secure networks like virtual local area networks, and conduct regular penetration tests of their systems. Hospitals need to more closely monitor administrative privileges, as the majority of large scale attacks began with a compromised account like that of a third-party provider, as seen in the case of the Hancock Regional Hospital in January 2018. By monitoring the log activity of user accounts and revoking account access when no longer needed, and employing techniques such as multifactor authentication, hospitals can better protect their IT infrastructure. By understanding the factors that make individuals, health care organizations, and employers more susceptible to cyber attacks, we can better prepare for the next pandemic.

II. CYBER CRIME

Cyber crime is a term for any illegal activity that uses a computer as its primary means of commission and theft. The U.S. Department of Justice expands the definition of cyber crime to include any illegal activity that uses a computer for the storage of evidence. The growing list of cyber crimes includes crimes that have been made possible by computers, such as network intrusions and the dissemination of computer viruses, as well as computer-based variations of existing crimes, such as identity theft, stalking, bullying and terrorism which have become as major problem to people and nations. Usually in common man's language cyber crime may be defined as crime committed using a computer and the internet to steel a person's identity or sell contraband or stalk victims or disrupt operations with malevolent CYBER CRIME Cyber crime is a term for any illegal activity that uses a computer as its primary means of commission and theft. The U.S. Department of Justice expands the definition of cyber crime to include any illegal activity that uses a computer for the storage of evidence. The growing list of cyber crimes includes crimes that have been made possible by computers, such as network intrusions and the dissemination of

computer viruses, as well as computer-based variations of existing crimes, such as identity theft, stalking, bullying and terrorism which have become as major problem to people and nations. Usually in common man's language cyber crime may be defined as crime committed using a computer and the internet to steel a person's identity or sell contraband or stalk victims or disrupt operations with malevolent programs. As day by day technology is playing in major role in a person's life the cyber crimes also will increase along with the technological advances.

III. CYBER SECURITY

All Privacy and security of the data will always be top security measures that any organization takes care. We are presently living in a world where all the information is maintained in a digital or a cyber form. Social networking sites provide a space where users feel safe as they interact with friends and family. In the case of home users, cyber-criminals would continue to target social media sites to steal personal data. Not only social networking but also during bank transactions a person must take all the required security measures.

IV. CHALLENGING TRENDS IN CYBER SECURITY

Here mentioned below are some of the trends that are having a huge impact on cyber security.

Web servers

The threat of attacks on web applications to extract data or to distribute malicious code persists. Cyber criminals distribute their malicious code via legitimate web servers they've compromised. But data-stealing attacks, many of which get the attention of media, are also a big threat. Now, we need a greater emphasis on protecting web servers and web applications. Web servers are especially the best platform for these cyber criminals to steal the data. Hence one must always use a safer browser especially during important transactions in order not to fall as a prey for these crimes.

Cloud computing and its services

These days all small, medium and large companies are slowly adopting cloud services. In other words the world is slowly moving towards the clouds. This latest trend presents a big challenge for cyber security, as traffic can go around traditional points of inspection. Additionally, as the number of applications available in the cloud grows, policy controls for web applications and cloud services will also need to evolve in order to prevent the loss of valuable information. Though cloud services are developing their own models still a lot of issues are being brought up about their security. Cloud may provide immense opportunities but it should always be noted that as the cloud evolves so as its security concerns increase.

APT's and targeted attacks

APT (Advanced Persistent Threat) is a whole new level of cyber crime ware. For years network security capabilities such as web filtering or IPS have played a key part in identifying such targeted attacks (mostly after the initial compromise). As attackers grow bolder and employ more vague techniques, network security must integrate with other security services in order to detect attacks. Hence one must improve our security techniques in order to prevent more threats coming in the future.

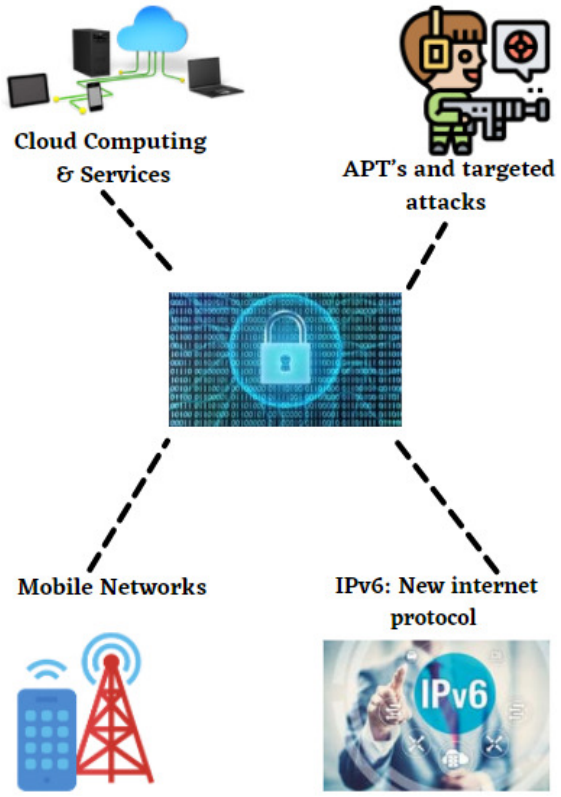

Fig. 1 Trends Changing in Cyber Security

Mobile Networks

Today we are able to connect to anyone in any part of the world. But for these mobile networks security is a very big concern. These days' firewalls and other security measures are becoming porous as people are using devices such as tablets, phones, PC's etc all of which again require extra securities apart from those present in the applications used. Further mobile networks are highly prone to these cyber crimes a lot of care must be taken in case of their security issues.

IPv6: New internet protocol

IPv6 is the new Internet protocol which is replacing IPv4, which has been a backbone of our networks in general and the Internet at large. Protecting IPv6 is not just a question of porting IPv4 capabilities. While IPv6 is a wholesale replacement in making more IP addresses available, there are some very fundamental changes to the protocol which need to be considered in security policy. Hence it is always better to switch to IPv6 as soon as possible in order to reduce the risks regarding cyber crime.

Encryption of the code

Encryption is the process of encoding messages in such a way that eavesdroppers or hackers cannot read it. In an encryption scheme, the message or information is encrypted using an encryption algorithm, turning it into an unreadable cipher text. This is usually done with the use of an encryption key, which specifies how the message is to be encoded. Encryption at a very beginning level protects data privacy and its integrity. But more use of encryption brings more challenges in cyber security. Encryption is also used to protect data in transit, for example data being transferred via networks (e.g. the Internet, ecommerce), mobile telephones, wireless microphones, wireless intercoms etc. Hence by encrypting the code one can know if there is any leakage of information.

VI. HEALTHCARE INDUSTRY IS AT RISK

Organizations are becoming increasingly susceptible to online attacks threatening day-to-day work and compromising confidential patient data. Long, busy days mean healthcare staff doesn't have the time and resources to educate themselves about online risks. The potential disruption caused by a complete overhaul in online security is just too big for a lot of organizations to even consider.

Healthcare leaders are ready to increase spending on cyber security. But with new threats uncovered every day, it's difficult to know where an organization would be better off investing their budget. High demand for patient information and often-outdated systems are among the nine reasons healthcare is now the biggest target for online attacks.

Private patient information is worth a lot of money to attackers

Hospitals store an incredible amount of patient data. These organizations have a duty to protect their patients' personal records. With GDPR coming into play this year, it's becoming increasingly important for hospitals to keep their information secure.

Financial penalties – whether they be fines for not cooperating with GDPR or paying to retrieve their data from ransomware are real and an alarming thought for a healthcare industry that's already struggling with financing daily work demands.

IT professionals are realizing that the cost of securing their data with solutions like multi-factor authentication (MFA) is far less than the pay-out from ransomware or similar attacks. MFA is a solution that requires more than one piece of information to identify a user and then generates a one-time password on each login session. This makes it a lot harder for hackers to steal passwords and other information.

Medical devices are an easy entry point for attackers

There aren't many downsides to innovations in healthcare technology these days. Medical devices like x-rays, insulin pumps and defibrillators play a critical role in modern healthcare. But for those in charge of online security and patient data protection, these new devices open-up more entry points for attacks. Medical devices are designed for one purpose like monitoring heart rates or dispensing drugs. They're not made with security in mind. Although the devices themselves may not store the patient data that attackers pursue, they can be used to launch an attack on a server that does hold valuable information. In a worst-case scenario, a medical device can be completely taken over by hackers, preventing healthcare organizations from providing vital life-saving treatment to patients.

Hackers know that medical devices don't contain any patient data themselves. However, they see them as an easy target, lacking the security found on other network devices like laptops and computers. Threats against medical devices can cause problems for healthcare organizations giving hackers access to other network devices, or letting them install costly ransomware. Keeping network devices secure wherever possible helps to limit the damage that could be caused by an attack on medical devices.

VII. CONCLUSION

This paper presents a systematic literature review on cyber risk in the healthcare sector. It describes the main literature information on cyber risk. It highlights the poor attention of the scientific community on this topic, except in the United States. The studies related to the health facilities are not enough to answer healthcare needs. The literature lacks research contributions to face the cyber risk management challenge in the healthcare sector. This topic should be developed in other countries and subject areas such as Business, Management and Accounting; Social Science; and Mathematics. The results of this research highlight the need for further studies to investigate empirically the cyber risk especially connected to some classes and subclasses of operational cyber security risks. For instance, scholars should provide more contributions to External Events which hazards, legal issues, business issues, and service dependencies. The implications of this research are twofold. One the one hand, it highlights knowledge of the literature on the cyber risk. On the other hand, it identifies gaps in the literature which need to be filled and, consequently, future research opportunities. This research has a main limitation, i.e., it analyzed only the documents related to the keyword "health"; this criterion may narrow the field excessively. However, we chose this keyword strategy to understand the current situation on cyber risk in the healthcare sector, especially during the COVID-19 pandemic. This limitation may also be the strength of this research. Thanks to this research

criterion, it identifies knowledge gaps in the literature and offers future research opportunities in studying cyber risk. Firstly, scholars may investigate the literature on cyber risk in other sectors and replicate the best practices in the health facilities. Secondly, it encourages new managerial solutions derived from practical experiences of consults and practitioners.

REFERENCES

[1] Mohammad S. Jalali, Jessica P. Kaiser, " Cyber security in Hospitals: ASystematic, Organizational Perspective", J ournal of Medical Internet Research 20(5), April 2018, 10.2196/10059.

[2] CW Jobs [Internet]. London, UK: 2016. Cyber crime timeline; URL:http://www.cwjobs.co.uk/careers-advice/itglossary/cyber-crime-timeline. Accessed: 2016-08-09. (Archived by WebCiteR at http://www.webcitation.org/6je8V9 cyI).

[3] U.S. Department of Health and Human Services. Security standards: technical safeguards [Internet]. Baltimore, MD: CMS; URL:http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/techsafeguards.pdf. Accessed: 2016-08-09. (Archived by WebCiteR at http://www.webcitation.org/6je8cfMpZ).

[4] U.S. Department of Health and Human Services. Fact sheet: ransomware and HIPAA [Internet]. Baltimore, MD: CMS; URL:http://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf. Accessed: 2016-08-09. (Archived by Web CiteR at http://www.webcitation.org/6je8iBYI5).

[5] Wu F, Eagles S. Cybersecurity for medical device manufacturers: Ensuring safety and functionality. Biomed Instrum Technol. 2016 Jan 20; 50(1): 23-33. Available from: 10.2345/0899-8205-50.1.23. [10] HCPro.com Ransomware a new threat to healthcare sector. Physician Practice Perspective. May 2016; 11-12.

[6] Conn J. Federal task force takes on healthcare cybersecurity. Modern Healthcare. URL:http://www.modernhealthcare. com/article/20160416/MAGAZINE/304169890. Accessed: 2016-08-09. (Archived by WebCiteR at http://www.webcita tion.org/6jdtejLCt) April 16, 2016.

[7] Rowe K. Healthcare IT transformation: how has ransomware shifted the landscape of healthcare data security? Healthc Inform. 2016 May; 33(3): 44-45.

[8] Blanke SJ, McGrady E. When it comes to securing patient health information from breaches, your best medicine is a dose of prevention: a cybersecurity risk assessment checklist. J Healthc Risk Manag. 2016 Jul; 36(1): 14-24. Available from: 10.1002/jhrm.21230.

[9] Hagland M. With the ransomware crisis, the landscape of data security shifts in healthcare. Healthc Inform. 2016 May; 33(3): 41-47.

[10] American Health Information Management Association. Healthcare increasingly targeted by ransomware attacks. J AHIMA. 2016 May; 87(5): 12.

