DOI Number: 10.5958/0974-1283.2019.00161.0

Cybersecurity Threats and Solutions in the Current E-Healthcare Environment: A Situational Analysis

Aneesh Remani Ravi[1], Rajeesh R Nair[2]

[1]Asst.Supervisor, Behavior Health Clinic, Schofiled Barracks, Hawaii, USA,
[2]Asst.Professor, Amrita College of Nursing, Amrita Vishwa Vidyapeetham, Kochi, India

Abstract

The need for cybersecurity measures in the field of healthcare is becoming more prescient given both the increased sophistication of cyber criminal activity and the increased prevalence of low-security mobile devices[1]. Also, hospitals have been slower to increase cybersecurity, but has become an increasing target due to the increased security of the financial industry[2]. The implementation of the Health Information Portability and Accountability Act (HIPAA) has made patient records more portable and accessible, and created more opportunities for breaches[1]. The Health Information Technology for Economic and Clinical Health Act (HITECH) promoting greater implementation of electronic systems for coordination and records. The medical field is also becoming increasing dependent on connectivity, and people are wary of the threats to automated and robotic safety procedures. The threat of high dependence on technology for medical practices presents risks in and of itself, such as cases where it disrupts communication between healthcare professionals, or fails to account for user failures that could be prevented with better feedback before implementation. Healthcare providers are in a difficult position, trying to balance the need for quick, responsive systems for users, and need for cybersecurity measures that can slow down the computer system. In the following pages, Lewin's field mapping approach will facilitate an analysis of the current largest cybersecurity threats and current research on the best methods of thwarting these vulnerabilities.

Key words:- *cybersecurity, e-health care, threats and solutions.*

Introduction

According to a top industry consultant, U.S. healthcare systems are attacked tens of thousands of times per year and are projected to lose around $305 billion from cyber attacks over the next five years. One of the reasons for this significant loss is the use of hacking and malware programs to ask for ransom in exchange for personal data that was stolen. In 2016, over 800,000 records were stolen in four cyber attacks. Ransom is also demanded for access to the computer system itself, which hackers can dismantle knowing the high cost of downtime to healthcare organizations[2]. The problem is that the opportunity for attacks is increasing given the proliferation of different types of system software, hardware, and cloud computing technology. For this reason, Lewin's change theory, specifically his idea of field theory is needed to assess the wide range of attack points in E-healthcare systems. In Lewin's field theory, it is important to assess the environment and how it affects the social relations and behaviors between actors. Instead of changing individuals, it is necessary first to change the group dynamic[3]. In the area of electronic health information systems, this would entail not only the way that security measures are promoted for employees, but the interrelation between the various cybersecurity actors in an organization, including the cybercriminals, coders, software designers, and medical device engineers.

Corresponding author
Mr. Rajeesh R Nair
Asst. Professor, Amrita College of Nursing
Amrita Vishwa Vidyapeetham, Kochi,Kerala,India
email: rnairrajeesh@gmail.com,
rajeeshr22105@aims.amrita.edu
Contact no. 07736675270

The Healthcare Cybersecurity Environment

Langer explains the three main types of black hat, or criminal cyber activity as: 1) stealing data (passwords, credit cards), 2) vandalism of intellectual property 3) terrorism or injury to people. The White Hat, or cyber security experts, are concerned with auditing the services, users, and policies of network traffic to ensure authentication (user verification), authorization (user privilege), and privacy (information stays secure)[1]. Since the cloning of user account data is one of the most prevalent ways of conducting multiple different kinds of attacks, they will also seek additional authentication measures. Due to the risks to data and network integrity, cyber security personnel will also find ways of increasing data reliability and recover ability.

Cybersecurity Threats to Medical Devices

The threat posed by malfunctioning software used in medical devices has become a greater concern as seen in the 1.2 million adverse events in five years, with over 20% related to computer technology, and over 90% of those being high risk. This statistics might even be low given the negative consequences for errors and the reluctance of clinicians to report them fearing loss of patient confidence and reputation. However, the number one risk is not hacking of medical devices, but the lack of integrity of medical databases . However, both risks to devices and to data systems are heightened by old software that is used, and can be repositories for old malware . For examples, research on hospitals in 2012 found that some were relying on long outdated windows operating systems, such as an MRI machine using Windows 95 . A vast majority did not have regular updates to their current versions of windows, leaving them vulnerable to many cyber threats[4]. In addition to addressing these basic software updating issues, **t**here is much more that healthcare organizations can do.

Major Risks of Cyber Criminal Activity and their Counter-Measures

Kruse et al., (2016) identified that the most common strategies for preventing and preparing for cyber attacks involve 1) clearly defining the roles for IT professionals, including timely updates to software, 2) using a VLAN (virtual local area network), 3) using cloud-based computing with high security and data protection/ hardware redundancy, and 4) employee training on the increased importance of cybersecurity measures. By far, the largest numbers of breaches are the result of employees accessing or downloading malicious files, which are not preventable by most health information technology systems, and therefore would require employee training programs[5]. Other studies have found that medical institutions encourage the use of personal mobile devices, but nearly half said they provide no security measures for the use of these devices. A 2017 report by a security company found that employee training could prevent around half or more of cyber attacks on hospitals (Parwani, 2017).

The most basic cybersecurity practice is using a firewall permitting only approved websites for user access, often using a subscription service. The downside is that users will have high dissatisfaction with this system, particularly if they have trouble gaining access to sites that provide an important service, or if the website themselves are approved, but still vulnerable to being used by cybercriminals to attack visitors. After interviewing medical personnel researchers analyzed the data to determine knowledge of security protocols and found that the current IT climate created tensions among employees. Cybersecurity experts are unable to tell whether an attack has the harmful intent and has to treat all evasions as breaches and take appropriate responses. The source of this problem seems to be that designers of the cybersecurity protocols often do not have adequate information about how their policies are going to impact workflow for clinicians[6].

Another strategy is to limit incoming email to only approved sources, which can also be purchased as part of a security software package, such as Barracuda Essentials for Email. For these measures, users can also be given separate devices for PHI network activities, and daily browsing, personal email activities. Programs like the Cisco Identity Services Engine are available for this purpose, but do not stop a cybercriminal once he/ she has gained access to user privileges in the system . Therefore, the security solution involves detection scanning of the network activity to prevent intrusions. It is also important to use an active scan of vulnerabilities in the system[1].

Suggested steps for improving the security of networks, include implementing security policies that prevent users from installing software, auditing of the firewall and data integrity, removing unneeded services from servers while tightening the incoming and outgoing

traffic permitted by needed services, and frequently checking data integrity and file changes . Although there is no sure way to completely secure computer systems against all attacks, Langer suggests the creation of security drills to test the network detection and prevention capabilities. For example, the cybersecurity team could practice attacking the network and using another team to defend it. Drills could be conducted where a successful attack is simulated, like all patient data being hacked, and IT security professionals practice rebuilding the systems[1].

Protecting Medical Devices from Cyber Threats

To address the vulnerability of cyber threats to medical devices, technology manufacturers should design the software with the previously mentioned risks (such as outdated software) in mind[4]. However, until this is done, a wide array of other protective measures have been developed, for example, for devices that respond to patient needs in real time. Particular systems are faced with unique cybersecurity risks, such as diabetes therapy systems, which monitor glucose metabolism and insulin response. These devices communicate via wireless technology, making the remote software and computer systems and the insulin pump they are connected to vulnerable. A cyber attack could have adverse effects on the patient, such as either hypoglycemia or hyperglycemia. Zeadilly, Issac, and Baig, propose what is known as a rolling or changing the encryption key after every transmission of data. The down side is that this encryption is only as good as the encryption algorithm[7]

Protecting Patient Private Information

Another cybersecurity threat is the stealing of authentication keys needed for decryption of network data. Liang et al., suggest a two-part system, where communications between sensor nodes, they also send authentication code that is unique to the sensor and the patient private identity. This technique could be added to any routing protocol to prevent clone attacks and injection of false information into the system . Social networks use profile-matching approach algorithms that assess the likeness of two profiles without making apparent connections between their characteristics . This method proposed uses what are called the eCPM, iCPM, and IPPM protocols, (standing for explicit, implicit, and implicit predicate profile matching respectively), which allow comparison of values without revealing them and keeping all information sharing without it being linked to user profiles[8].

One of the most significant problems with securing patient data is that they often transmit health data through their private messaging and email systems. Therefore, the patient location should not be monitored in real time since this data can be used by hackers to determine a patient's daily patterns and habits which can be used to fully identify a patient . Lu et al., have proposed a method where a patient with similar conditions can share their experiences over a social network securely by using a pseudonym and then authenticating shared data for each user. The authors present a framework that divides processing into separate non-threatening components, so that devices and sensors cannot be overloaded.[9]

Conclusion

Currently, the federal government, and the financial services sector spend around 15% of their budgets on cybersecurity measures, but healthcare organizations spend far less. The preceding research indicated that improving this ratio could significantly reduce risk from cyber threats that are presented on several fronts. The first priority should be on employee training, as lack of awareness is how most network intrusions occurThe next step will require institutional analysis, and determination of the systems and functions most vulnerable (software security updating, devices firmware upgrade, etc.). Although in the future we will hopefully see more integration of healthcare technology engineering design processes and cybersecurity demands, the development of other devised methods, protocols and network technologies, is rapidly filling the gaps in healthcare security.

Conflict of Interest:- Nil

Source of Funding:- Self

Ethical Clearance:- Taken from the institutional ethical committee of Amrita College of Nursing, Kochi.

References

1. Langer SG. Cyber-Security Issues in Healthcare Information Technology. Journal of digital imaging. 2017 Feb 1;30(1):117-25.
2. Krisberg K. Cybersecurity: Public health increasingly facing threats. American Journal of Public Health. 2017 Aug 1;107(8):1195.

3. Barry S. Effect of Provider Education on Pulmonary Rehabilitation Referrals and Discussions with Patients.
4. Fu K, Blum J. Controlling for Cybersecurity Risks of Medical Device Software. Biomedical instrumentation & technology. 2014 May;48(s1):38-41.
5. Kruse CS, Frederick B, Jacobson T, Monticone DK. Cybersecurity in healthcare: A systematic review of modern threats and trends. Technology and Health Care. 2017 Jan 1;25(1):1-0.
6. Koppel R, Smith SW, Blythe J, Kothari V. Workarounds to computer access in healthcare organizations: you want my password or a dead patient?. InITCH 2015 (pp. 215-220).
7. Zeadally S, Isaac JT, Baig Z. Security attacks and solutions in electronic health (e-health) systems. Journal of medical systems. 2016 Dec 1;40(12):263.
8. Liang X, Li X, Zhang K, Lu R, Lin X, Shen XS. Fully anonymous profile matching in mobile social networks. IEEE Journal on Selected Areas in Communications. 2013 Sep;31(9):641-55.
9. Lu R, Lin X, Shen X. SPOC: A secure and privacy-preserving opportunistic computing framework for mobile-healthcare emergency. IEEE Transactions on Parallel and Distributed Systems. 2013 Mar;24(3):614-24.