International Journal of Research in Engineering, Science and Management
Volume-3, Issue-1, January-2020
www.ijresm.com | ISSN (Online): 2581-5792

Cyber Security in Health Care

D. N. Mohan[1], S. Sagar Gowda[2], I. S. Vikyath[3]
[1]*Assistant Professor, Department of Information Science & Engineering, Nagarjuna College of Engineering & Technology, Bangalore, India*
[2,3]*Student, Department of Information Science & Engineering, Nagarjuna College of Engineering & Technology, Bangalore, India*

***Abstract*: Electronic healthcare technology is around the world and creates huge potential to improve clinical outcomes, maintains records and transform care delivery. But there are increasing concerns relating to the security of healthcare data and devices. Increased connectivity to existing computer networks has exposed medical devices to new cybersecurity vulnerabilities. Healthcare is a target for cybercrime for two fundamental reasons: it is a rich source of precious data and its defences are weak. Cybersecurity breaches include stealing health information and ransomware attacks on hospitals, and could include attacks on implanted medical devices. This can reduce patient trust and threaten human life. Ultimately, cybersecurity is critical to patient safety. New legislation and regulations are in place to facilitate change. Changes are required to human behaviour, technology and processes as part of a holistic solution.**

***Keywords*: Cyber security, Medical devices.**

1. Introduction

Cybersecurity has become a crucial issue for many organizations but also for private individuals. As well as for "regular" crime, anyone may become a target of ill-intentioned people, exploiting the vulnerabilities of information systems (IS) in any possible way. Healthcare organizations are some of the entities we trust the most and that hold the most sensitive information about us: name, date and place of birth, medical records, social security details, etc. Suffering from many flaws (low budget, lack of IT organization, excessive use of legacy systems…), healthcare actors have become easy targets for hackers, facing more and more pressure and threats from them.

This article aims at depicting the current state of cybersecurity in healthcare organizations as well as at understanding the main cyber threats they face and how these last ones could be addressed. First of all, the stakes and risks associated to the healthcare environment will be presented. The different types of assets likely to be targeted will be reviewed as well as the profile of the potential attackers/threats and their objectives. Finally, the current state of cybersecurity in healthcare facilities will be portrayed and possible measures to enhance it will be discussed.

Healthcare organizations are sensitive infrastructures due to their criticality for people's well-being and safety. Hospitals, health plans, research labs handle unique and valuable assets that digitization, system interconnection etc. make more and more exposed to cyber threats. In order to assess health sector cyber risks, it is paramount to understand the systems to be defended, their key assets and the impacts a successful attack may have on them. In addition, potential adversaries also need to be identified along with their intentions and capabilities. That way, threats can be better evaluated as well as healthcare systems vulnerabilities.

Electronic health records, also referred to as EHRs, contain a host of sensitive information about patients' medical histories, making hospital network security a primary IT concern. EHRs make it possible for physicians and other healthcare professionals, as well as insurance companies, to share essential information. This makes it easier to both coordinate care and facilitate insurance matters. Never before have medical professionals been able to collaborate in such dynamic ways to meet patients' needs.

In addition to a patient's records, medical provider networks can contain valuable financial information. Since there are very few people who do not see healthcare providers, nearly everyone's personal information is available in some form.

The interconnected nature of EHRs means hackers have access to the data that has collected under patients' names for years. Sharing patient information is integral to providing the best possible treatment to patients, but that same sharing also makes networks extremely valuable targets.

Often, in cybercrimes, the attacker's goal may be to gather information — either to sell or for their personal use. With the content available through electronic health records, a stranger could use insurance information to set up appointments, undergo expensive medical procedures or obtain prescription medication under the patient's name. In these cases, the patient or healthcare organization may be held responsible for the charges or medications.

Although less common, network-linked devices can also be manipulated to administer incorrect treatments or otherwise change a machine's function. These developments put patients' lives in danger as a hacker could use this access for terrorism or hold a health provider ransom. In medicinal situations, where the change of a decimal or a minor change in dosage is the difference between life and death, healthcare providers cannot afford these potential threats.

Regardless of the hacker's intentions, it's easy to see why

network security is so important.

2. Common Healthcare Security Threats

- *Staff:* Employees have easy access to patient files. While the majority won't abuse this power, there's no guarantee some won't steal sensitive information. Criminals can use this type of information in identity theft, but it can also be used to intimidate or even blackmail people. There are multiple ways in which staff can steal records. In some cases, employees access confidential financial documents and use patients' credit card numbers to commit a series of fraudulent purchases.
- *Malware and phishing attempts:* Sophisticated malware and phishing schemes that plant malicious scripts on a computer or steal login credentials can compromise an entire system. One of the most challenging issues dealing with malware is that it only takes one seemingly-authentic link to introduce a nefarious cyber presence into your network. It's essential to train staff to recognize common phishing attempts. One common scam is to have emails from authentic-looking sites request login information-something reputable companies never ask through an email. Once a user provides that information, the hacker on the other end can log in to the system.
- *Vendors:* Healthcare providers often work with vendors without assessing the accompanying risk. For example, if a hospital hires a cleaning company, its employees might gain access to computers. While patient information should be locked in ways that the average employee cannot view, it can be difficult to safeguard all points of access since cleaning and maintenance are integral to maintaining a healthy work environment.
- *Unsecured mobile devices:* Healthcare facilities that allow mobile logins don't always require the devices to meet security standards. This leaves their networks vulnerable to malware and hackers since all of the organization's planning and security do not influence staff communication devices. This issue is compounded once staff disposes of the equipment in an upgrade — network information or passwords might still be accessible, making a natural access point for criminals. Unless the organization sets strict guidelines or bans user devices altogether, there is little that employers can do.
- *Unrestricted access to computers:* Computers that aren't in restricted areas can easily be accessed by unauthorized personnel. If these open computers are connected to sensitive patient information, unauthorized staff or others in the area could quickly find damaging information. In other cases, successful phishing attempts on general-access computers provide a gateway for hackers into more sensitive areas of the network. Be sure any computer that holds patient information is placed in a secure location.

3. Address Data Security Issues

- *Educating Employees:* Helping employees understand the role they play in cybersecurity and the impact it can have on patients' lives fosters an atmosphere in which security is valued and respected. Regular briefings and communication on the state of the organization's security reiterate the emphasis the organization is placing on cyber safety. Attending staff training sessions and making cybersecurity a regular topic in meetings could also help drive this message home.
- *Stablishing Procedures:* Create a plan that outlines specific protocols for dealing with information and networks — both physical and virtual — and make sure they are followed. By explicitly expressing the expectations, the process becomes standardized, allowing more comprehensive oversight for network security monitors.
- *Require Software Updates:* Cybercriminals often take advantage of holes in outdated software or other unsecured access points. To combat this, force software updates on machines, utilize two-factor authorization and automatically institute monthly password updates that require characteristics of a "strong" password. You can help your employees out with this by automatically setting company machines to periodically require such changes so that employees only have to come up with a new password or click to allow updates. Once again, this can be incredibly difficult to enforce on staff personal devices, so educating employees on the importance of updates is crucial.
- *Understand Your Network Map:* Utilize technology that provides an overview of the devices and storage on your network. In this way, you can see exactly what information is vulnerable in which ways, and you'll know when new or unauthorized devices have joined the system. This layout will also help you establish the access and restrictions for each device on the network, cutting down on inappropriate staff conduct.
- *Update Your Software:* Be sure all software and operating system information is up to date. These updates include critical patches that discourage potential cybercriminals who jump on previously-found weaknesses in software. If you do not utilize the proper software updates, criminals can still take advantage of the holes left behind by earlier versions.
- *Virtual Private Network Encryption:* Encrypting your network connection is a great way to enhance network privacy and block potential hackers. A Virtual Private Network (VPN) encodes your data so that other viewers cannot see what goes out or comes in on your computer. So even if they are monitoring your connection, they would not receive anything unless they already had access to your computer.
- *Set Strict Access:* Rather than thinking solely about what you need to restrict, consider data from this viewpoint: What do certain employees need to access to do their job? This

establishes a context in which the minimum amount of information is available, cutting the possibility for staff misuse.

- *Think Like a Hacker:* By understanding the basics of how a cybercriminal manipulates a network, you will be in much better position to impede their efforts. While it may be difficult to account for this without a background in healthcare data security measures, this crucial step will highlight any potential gaps in your plan.
- *Use Professional Services:* Though there are many ways health organizations can limit potential threats, your area of expertise is utilizing information to help patients, not managing data security measures in healthcare. By assigning network security to a specialized outside agency, you receive professional network safety and support, allowing your staff to focus more directly on medical-related tasks.

4. Conclusion

Healthcare is vulnerable due to historic lack of investment in cyber security, vulnerabilities in existing technology and staff behaviour. Electronic health records, health care infrastructure and individual medical devices are targets. Cyber security is a patient trust and safety concern. The healthcare sector must protect the personal information of the patients because the hackers can leak them, and other thieves can use them to conduct medical fraud and other financial gains. Cyber security helps in keeping the information of the patient confidential for legal purposes and also prevent cybercrimes.

References

[1] D.V. Dimitrov, Medical internet of things and big data in healthcare, Healthcare Inf. Res. 22 (2016) 156–163.
[2] T. Walker, Interoperability a must for hospitals, but it comes with risks, Manag. Healthc. Exec., 2017.
[3] A. Shenoy, J.M. Appel, Safeguarding confidentiality in electronic health records, Cambridge Q. Healthc. Ethics 26 (2019) 337–341.
[4] C.S. Kruse, B. Frederick, T. Jacobson, D.K. Monti cone, Cybersecurity in healthcare: a systematic review of modern threats and trends, Technol. Health Care, 25, 2019.
[5] R.S. Ross, L. Feldman, G.A. Witte, Rethinking Security Through Systems Security Engineering, ITL Bull. – December 2016.