Future Scan Paper: Healthcare and Cyber Security

Author Name

Institution

Future Scan Paper: Healthcare and Cyber Security

Healthcare organizations are especially vulnerable to cyber-attacks for a variety of reasons and make prime targets for cybercriminals. The amount of sensitive personal data that they can obtain about patients is aperitive for many hackers. The Internet has become a huge success for the world, every work has been done on the internet nowadays, and every data has been stored in the cloud where there are so many benefits to having internet there are some disadvantages also. If there are some users who are taking benefits of the world with internet, yet there few people who are taking the advantages of using the internet for some wrong reasons (Kruse, Frederick, Jacobson, & Monticone, 2017). As an example, let's talk about cyber-attacks in hospitals. There is a huge data of patients on the internet attackers can make a disaster by attacking the database of hospitals. Hospitals have a couple of problems that other organizations may not have concerning the cybersecurity. One is a reluctance to patch systems "in case it puts patients at risk", even though the risk to patients from, say, a remote hack of an unpatched IV drug dispenser is much greater than the risk of failure during a planned maintenance upgrade. This is in part due to a myth that medical devices lose FDA certification if patched. Only a significant change in function requires recertification (Fu & Blum, 2014). Another problem is over-regulation. Laws to protect the public are a good thing, but if they force a hospital to spend too much of its security budget on compliance and not enough on actual security, that's an issue.

# Healthcare Cyber Security Market

Cybersecurity spins around the protection of programs, networks, and programs from digital threats and attacks. Digital threats and attacks are generally meant so as to terminate, destroy, alter, or access information which is sensitive. Besides, digital attacks are designed for interrupting normal business processes. As far as healthcare is concerned, cybersecurity is considered as a risk factor concerning healthcare data. Undoubtedly, healthcare organizations’ primary goal is to protect patient information from such sort of threats and attacks. (Martin, Martin, Hankin, Darzi, & Kinross, 2017). Owing to cyber threats, healthcare organizations now require professionals of health informatics who are well acquainted with the current state of cybersecurity.

Cyberattacks and data breaches incidents have been increased in number, and such incidents require an increase in the need for advanced security cloud-based solutions, the demand for healthcare cyber security market has enhanced. Healthcare organizations have adopted cyber security solutions and services in order to protect their patient and hospital information from data. This rising awareness is responsible for boosting this market. However, the lack of skilled workforce among healthcare organizations across is responsible for depleting the market growth during the estimated period.

# Cyber Security and Healthcare

Many hospitals have incorporated technology into their daily operation because of the benefits it presents to their firms. However, the use of technology exposes the data belonging to these institutions for access by unauthorized users. These tech-savvy criminals access the information by carrying out a cyber-attack against the organization (Martin et al., 2017). However, there are ways in which hospitals can use to prevent this from happening.

* Restore and Backup: Hospitals can protect themselves from cyber-attacks with the help of most effective tool i.e. backup and restore.
* Security Environment: If staff members are not acquainted with cyberattack and its implications then the protection of sensitive data could become difficult for hospitals. Healthcare organizations have to have a security culture to evade ransomware attacks.
* Security of medical devices: Motion sensing alarms or DLP software could be handy for the security of physical devices. Every sophisticated medical device, nowadays, comes with a computer, and if there is not any cyber security software in the device then data could be stolen easy (Coronado & Wong, 2014).

With the advancements in technology, the security systems are always upgrading and so are the cyber-attacks. It’s a race where we try to outrun the latter to protect our data from security breaches. There is an ever-increasing need of individuals for improving cybersecurity systems.

# Implications of Cyber Security in Healthcare

Hospitals are unique in the sense that records of healthcare organization, for hackers, is roughly ten to hundred times the worth of the data of credit card holders. While a credit card record can easily be changed with a single phone call, medical information cannot. If medical information is captured by a hacker, it means they've owned healthcare organization, and the identity of patients could be stolen Another unique component of hospitals is that the computer systems are sometimes directly responsible for life and death*.*Fortunately, we haven't yet had a hacking incident whereby someone was actually killed. A few years ago, Vice President Dick Cheney was worried that terrorists would take over his pacemaker so he had it modified to make that impossible. So, hospitals and healthcare industry companies need to be spending wisely on cybersecurity and probably should be spending more in general. We can't have computer security negligence get to the point where lives are lost (Kruse et al., 2017). Cyber criminals always look for soft targets, they search weak spots in the organizations. Employee education is one of the most effective strategy that risk management offers to avert cyber-attacks. There is no doubt that first line of defense in any organization is always the educated employees. Online communities and groups serving cybersecurity articles, prevention and rectification methods for cyberattacks etc. are a good source to gain knowledge about cybersecurity.

# Future Concepts

Of the leading causes of death in the US, medical error is the one, and secures third place among the leading causes of the death. Even though development of cyber-security concerning healthcare in its early phases, the benefits far outweigh the limitations in Blockchain technology. Mainly because, inefficiencies in the system are much more than the improvements that have been made in health care cyber-security. Blockchain could be a future of health care cyber security, and it sounds interesting as well. As blockchain technology becomes more centralized in the development of therapies, pharmaceutical and biotechnology, research and development is moving towards a cross-organizational alliance of information across multiple companies, government agencies and research institutes. Organizations are very partial to share any valuable data in that it gets hacked or stolen, an all too common problem in supply chain management. Blockchain offers the possibility for all changes on the chain to be encrypted, disabling any method of changing past entries, and something that was not possible before now in the drug development field (Coventry & Branley, 2018).

There are many major use cases for blockchain in the healthcare and life sciences industries, but the most important are utilization of the records in health care. With the establishment of health records that have integrity and have association with patients cyber security in healthcare could be strengthened. However, the establishment of such health records is one the biggest challenges in healthcare IT. Blockchain technology makes it possible to create and manage all changes across multiple independent proprietary systems with safe and secure access by all parties.

# Conclusion

Patients have to have confidence in healthcare organizations concerning the security of their personal information in hospital’s database. Besides, clinical mangers also have to ensure that every patient’s information is safe and secure. The requirement of cybersecurity in healthcare spins around the aversion of any cyberattack and ransomware that affect the healthcare organizations badly. Healthcare organization are, undoubtedly, the soft targets for hackers. Besides, hackers also prefer to target such organizations because of an easy access to huge piles of sensitive information. The initiative taken by governments now necessitates all the hospitals and healthcare organizations to implement cybersecurity to their networks. Assuming that a cyberattack has the potential to harm human lives (such as when important systems of a hospital are targeted) it might be possible to view it as attempted homicide or even murder in X cases (where X is the number of patients in ICUs for example). This means that suddenly the criminals will find themselves in very hot water even internationally and might be more careful with the targets they chose.

# References

Coronado, A. J., & Wong, T. L. (2014). Healthcare cybersecurity risk management: Keys to an effective plan. *Biomedical Instrumentation & Technology*, *48*(s1), 26–30.

Coventry, L., & Branley, D. (2018). Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. *Maturitas*, *113*, 48–52.

Fu, K., & Blum, J. (2014). Controlling for cybersecurity risks of medical device software. *Biomedical Instrumentation & Technology*, *48*(s1), 38–41.

Kruse, C. S., Frederick, B., Jacobson, T., & Monticone, D. K. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends. *Technology and Health Care*, *25*(1), 1–10.

Martin, G., Martin, P., Hankin, C., Darzi, A., & Kinross, J. (2017). Cybersecurity and healthcare: How safe are we? *Bmj*, *358*, j3179.