In September 2020, a ransomware attack in a Hospital in Dusseldorf, Germany caused a major systems failure. This forced healthcare officials to move a critically ill patient. This move resulted in his death. Another ransomware attack in September attacked the US hospital chain Universal Health Services. This attack affected all 250 locations. It forced doctors to keep records on pen and paper. Wireless equipment responsible for monitoring vital signs were shut down. Emergency room times skyrocketed. The need for good security in health care systems is paramount. Cyber professionals face many challenges in the realm of healthcare. Ransomware, phishing attacks, etc. are all threats to patient privacy and health. Researchers and cyber professionals are racing against the clock to develop defense strategies for these attacks. Legislation has also been created to help provide a framework for what is and isn't secure. It also protects patients rights to privacy.

Of all of the cyber threats that healthcare professionals face, phishing seems to be the most encountered. Phishing is when a bad actor tries to trick a user into giving up information or infecting their machine with malware. The most common form of phishing occurs through email. General phishing emails are meant to appeal to as many people as possible. They generally have an urgent tone or claim something that is too good to be true. They also tend to have bad spelling and grammar. This type of phishing isn't tailored to any one person. It is meant to be reach a large group of people to maximize effectiveness. Another type of phishing is spear-phishing. This is where an attacker tailors an email for a specific person or organization. These tend to be much more effective than general phishing. Legacy Systems are also a major concern. A legacy system is anything that is no longer supported by the manufacturer. This could be an operating system, an application, a piece of hardware, etc. Many healthcare facilities have have a large amount of legacy systems. This is due to the fact that medical equipment can be very expensive to replace if it can be replaced at all. Often times, medical facilities do not have a budget large enough to support a proper IT staff that can upgrade these systems. Legacy systems can be dangerous because they lack important security patches. This means that is a new vulnerability is discovered, then there is little that healthcare staff can to to thwart an exploit. As mentioned earlier, international groups have been using ransomware to hold data hostage. Ransomware is a type of malicious program that infects a computer. Typically, once the computer is infected, the program will encrypt the users file. This makes the files unreadable and unusable. The user will then receive a message explaining that if they want their files back, then they will have to may a ransom. This ransom is usually in the form of cryptocurrency. The problem with this is that there is no guarantee that the user will get their files back even if they pay the ransom. Ransomware can come be delivered by a phishing attack. The fact that it encrypts data can mean the loss of important records, and it could seriously slow a hospital down. Physical security is another consideration. There are many ways that attackers can steal information when they have access to critical systems.

There are many threats that healthcare facilities face, but luckily there are ways to protect data and assets. Limiting physical access is very important. This makes it more difficult to install hardware based keyloggers as well as cause direct damage to systems. Sensitive devices should be locked in secure rooms with access limited only to those who absolutely need it. All files should be backed up off site regularly. This way if a ransomware attack occurs and your files are encrypted, your files are safe. Cyber attacks aside, this is good practice anyway. Accidents can happen. Important data should be backed up elsewhere so that you can deal with this. Access to health information should be limited to those who need it. Educating healthcare workers is the best first line of defense. Showing how attackers tend to take advantage of ignorance can be the difference of a successful attack or a failure. Common sense is the best anti-malware. Installing anti-malware or anti-virus software is a great second line of defense against ransomware or other malware. It is not enough to just install the software. You must also frequently update it. Anti-malware is not foolproof. This is why common sense is the first line of defense. All network devices should be connected to a firewall. This can keep outsiders from gaining access to your network. It can also keep employees from going to suspicious web sites that could pose security risks.

Security in healthcare is so vital, that legislation has been passed to help ensure the privacy and safety of patients. The Health Insurance Portability and Accountability Act, or HIPAA for short, was introduced to do just that. It consists of privacy, security, and breach notification rules. A breach is defined as any use of protected health information that violates the security or privacy of a patient. There are three exceptions to this rule. The first is that the healthcare provider has it on good faith the recipient of stolen information wasn't able to retain it. The second is that the information that was accessed was used in good faith. The third is if the information is accessed by the owner. Failure to act within the guidelines of HIPAA can result in major civil penalties. There is also more general legislation that applies to healthcare. Section 5 of the Federal Trade Commission (FTC) states that organizations must adequately secure all computer systems. Also, any attempt to deceive customers into thinking that their data is secure could lead to severe penalties. The European Union General Data Protection Regulation offers protections similar to HIPAA on a much broader scale. It applies to all personal data. Collection of data must be considered lawful. The user must consent to data being collected, the collection of data must be necessary, and where the data serves a purpose that helps the user. The Personal Information Protection and Electronic Documents Act (PIPEDA) is a set of privacy laws that applies to private businesses in Canada and some cases, hospitals.

All in all, Cybersecurity in healthcare is an ever evolving field. There are many challenges that cyber analysts and healthcare professionals face. These include malware, legacy software and hardware, phishing, etc. These threats can cause data breaches, or they can outright destroy data. Luckily these dangers can be dealt with. Limiting physical access is a good first step to securing data. Installing and updating antivirus software also defense against ransomware and other malware. Firewalls also can serve as a first line of defense against various network attacks. There are also many laws in place to guarantee patient privacy. They provide a framework for what is and isn’t considered secure. All in all, Cybersecurity in healthcare is constantly changing. Professionals will need to constantly adapt in order to be able to deal with ever changing threats.

Sources

https://healthinformatics.uic.edu/blog/cybersecurity-how-can-it-be-improved-in-health-care/

https://www.himss.org/resources/cybersecurity-healthcare

https://www.usfhealthonline.com/resources/career/healthcare-cybersecurity-jobs/