BioSpectrum the business of Bio & Health Sciences

Cyber Attacks on Healthcare Institutions: Is Care Compromised?

28 December 2022 | Views | By Dr Gopal Sharan, Managing Director, TR Life Science

Healthcare institutions are responsible for handling sensitive patient data, effective cyber security solutions have become essential

Given the sensitivity of patient data, healthcare providers need to be extra cautious against cyber-attacks. Professionals in the healthcare sector need to spare time from their busy and hectic schedules to train or skill themselves against cyber threats so that care is not compromised.

According to data released recently by cyber security think tank Cyber Peace Foundation and Autobot Infosec, the healthcare sector in India has experienced 1.9 million cyber-attacks so far this year as of November 28. Attacks were launched from a total of 41,181 different IP addresses, most of which were found in China, Pakistan, and Vietnam.

The All India Institute of Medical Sciences (AIIMS) New Delhi was forced to resort to manual operations and shut down many of its servers recently as a result of a significant cyber- attack. AIIMS, which had previously declared aspirations to digitise all services by April 2023, denied reports that hackers demanded Rs 200 core as ransom.

How do they do it?

Medical devices do hold any patient data, which can be known to hackers. But, medical devices could provide hackers access to other network devices or allow the installation of expensive ransomware, which could cause problems for healthcare businesses.

Secure network devices enable limiting the damage a medical device attack can cause. Equipment like x-rays, insulin pumps,

and defibrillators are crucial in today's healthcare. For those in charge of web security and patient data protection, these new devices, however, present more attack routes.

Medical equipment performs specialised tasks like providing medication or tracking heart rates. Security is not given much weight in design. Even though the devices themselves might not store patient data, attackers can utilise them to launch an attack on a server that does contain crucial information. In the worst instance, hackers might entirely take control of medical equipment, prohibiting healthcare institutions from giving patients the required, life-saving care.

Medical data is a lot wealthier

As opposed to just one piece of information that could be discovered in a financial breach, healthcare data frequently encompasses all of a person's personally identifying information, making it lucrative on the black market. These attacks frequently result in the privacy and data of hundreds of thousands of patients being violated or taken by those with ulterior motives.

A Trustwave analysis claims that a healthcare data record might be worth up to $250 on the black market, whereas the next-highest value record is only $5.40. (a payment card). It is crucial that healthcare business IT workers do not undervalue this security concern and that actions are taken to preserve this data due to the value of the data and the allure of financial gain. The majority of these breaches can be ascribed to hackers and dishonest insiders who gained access through outside providers.

According to the Ponemon Institute, the costs of rectifying a breach are projected to be $740,000, and the cost of the attack rises by more than $370,000 if a third party is responsible. According to research, ransomware (a newly popular method utilised in recent assaults like the Colonial Pipeline and JBS USA hacks) or SQL injection attacks are the most frequent attack routes.

Worth of Private Patient Information

Healthcare institutions usually keep a very large quantum of patient data. The healthcare sector is a key target because hackers who can quickly sell sensitive information can make a lot of money. These institutions must safeguard patient data and records. In India, data protection is now a priority and like General Data Protection Regulation (GDPR) in European Union, Indian healthcare institutions are also protected through the implementation of the Information Technology Act and Data Protection Rules. The healthcare sector, which has huge continuous financial responsibilities, would be overburdened if they have to pay for their data recovery if attacked by ransomware. Protecting data is always cheaper compared to the payout for any kind of cyber attack. There is always a risk of compromising care. Multi-factor Authentication (MFA) may be an effective safeguard mechanism.

Online attacks are a concern for all healthcare companies. Because they have access to the most data, large businesses are prime targets for hackers. Smaller businesses, however, have more limited security expenses. Smaller businesses are frequently considered as an easy target and a backdoor access chance to target larger firms because they have less sophisticated and modern cybersecurity measures. Because healthcare firms or institutions are responsible for handling sensitive patient data, effective cybersecurity solutions have become essential. There are several solutions available that can be scaled to different business sizes, and healthcare leaders are increasingly conscious of the need to increase expenditure on cybersecurity.

Healthcare Staff and Newer Technology

Medical personnel lack the competence needed to identify and counteract internet risks. It is just not practical for every member of the healthcare team to be fluent in cyber security best practices due to budget, resource, and time constraints. It is widely admitted that cyber security solutions are complex, but with a straightforward user interface, a protective step can be taken. For healthcare professionals, it is always better to have a Simple-to-Access secure network. Solutions like MFA and Single Sign-On (SSO) are becoming more and more popular because they use a secure one-time code to add extra security layers without requiring the user to know anything but their login credentials.

Healthcare professionals are among the busiest and most sought-after in the nation. Staff members work long hours and are

under pressure, so they lack the time and resources to add internet security protocols to their to-do lists. Medical practitioners require efficient working procedures with few interruptions. Any cybersecurity protections that healthcare companies seek to put in place must be evaluated for their potential impact.

IT personnel should try to match security measures with current software. Because so many authentication methods are compatible with programmes like Office 365, medical professionals may carry out their everyday duties without interruption. Authorised users can access various applications by using SSO solutions, which keep their working routines short and simple without sacrificing security. SSO and Risk-Based Authentication (RBA) are examples of frictionless technologies that provide enough security from online dangers without interfering with daily operations.

Cyber-attacks are real for the healthcare sector and professionals/ workers/ staff especially the IT division need to be well-prepared and trained by cyber experts to protect the institutions' data and records.

Dr Gopal Sharan, Managing Director, TR Life Science