HEALTHCARE SECTOR CYBERSECURITY WITH RECOMMENDATIONS
The health sector is a crucial industry that offers life-critical services by leveraging new technologies to enhance patient care and treatment. On the other hand, cyber-threat actors and criminals seek to exploit cybersecurity flaws and vulnerabilities to steal patient health information, disrupt essential healthcare services, and for monetary gains.

Currently, COVID-19 disease has created new cybersecurity realities for healthcare providers. In addition to the prevalent challenges of providing care to infected people, healthcare has become a direct target of cyber-attacks. The World Health Organization (WHO) reported a dramatic rise of cyber-attacks directed at the organization’s staff, while phishing emails targeting the public have increased fivefold.

Understanding healthcare cybersecurity and recommended measures can go a long way in protecting health institutions, patient health data. And critical care IT infrastructure.

Top cybersecurity concerns in healthcare

Technology continues playing a vital role in enhancing patient care delivery. Health facilities utilize IT and Internet connectivity for various reasons, including acquiring, processing, and sharing patient data, lab reports, maintaining radiological equipment, among others. Technology facilitates patient care, but it can also be vulnerable to multiple attacks. As has been witnessed in the past, technology unavailability due to attacks can severely impact the global healthcare system. A Health Care Industry Cybersecurity Force concluded in its report that cybersecurity in the industry is in a critical condition. In fact, the healthcare industry lags behind other sectors in the security and protection of IT infrastructure.

Also, research reports show that cyber-attacks, such as ransomware, are increasing rapidly, with the healthcare industry being among the most targeted. For example, Israel cybersecurity researchers recently announced the development of a computer malware designed to add tumors in MRI and CT scans. Such viruses can lead physicians into making an erroneous diagnosis, endangering patient safety.
Furthermore, various health facilities have a differing approach to technological use, with some using old, obsolete, and outdated medical devices. Others use connected equipment to treat and monitor patients remotely. Some of the internets of medical things (IoMT) may contain weak security protocols, hence threatening hospital, patient, and staff safety. Gaping security holes, coupled with human errors, may result in unauthorized disclosure of confidential health information or trigger massive breaches with far-reaching consequences.

Encryption blind spots can also enable hackers to bypass the cryptographic tools used to secure vital health information. A large number of hospitals and insurance firms store classified health data in local and cloud storage locations. Weak encryption provides cyber adversaries with an easy way to steal the information. These and many other cybersecurity concerns should be a wake-up call for the healthcare industry to step up efforts for improving cybersecurity.

**Recommended cybersecurity practices**

1. **Combat insider threats**

A Verizon insider threat report revealed that insider threats had been a cybersecurity concern for 46% of healthcare institutions. Intentional insiders are challenging to identify and manage, and they continue plaguing the healthcare sector. The report also indicated that insiders could be bribed, recruited, or coerced to collaborate with cybercriminals at the expense of healthcare cybersecurity. Therefore, the health sector needs to adopt appropriate strategies for detecting and stopping insider threats as early as possible. Aggregating security information in a central location to close visibility gaps and aid continuous monitoring is a viable solution.

2. **Password security and MFA**

Internationally recommended password practices are effective in mitigating insider threats. Employees in healthcare entities use passwords to secure their workstations. Being the first line of defense, strong password security focuses on factors such as password length, characters, symbols, and passphrases. Regularly changing the passwords eliminates the possibility of a malicious insider cracking it, thus preventing impacts caused by insider threats. Passwords should be reinforced by multi-factor authentication (MFA), which requires the provision of multiple items for users to be authenticated. Other mitigation strategies used today in healthcare settings include employee awareness and training, risk assessment and management, outsourcing security functions to reputable managed service providers, and implementation of access controls to restrict incidences of unauthorized access.
1. IoT security

Hackers have increasingly used edge devices, such as thermostats and routers, to access protected devices and systems. With the current crave for Artificial Intelligence (AI), it has become easier for hackers to access overall systems like automation through the edge devices. In most cases, a large number of these IoT devices have sketchy security features. Blockchain can be used to secure the devices by decentralizing their administration. Decentralizing provides IoT devices with the capability to make security decisions independently. Not depending on central admin or authority makes the edge devices more secure by detecting and acting on suspicious commands made through unknown networks. Besides, hackers often penetrate the central administration of a machine and automatically gain full control of the devices and systems. By decentralizing such device authority systems, blockchain ensures such attacks are harder to execute.

2. Securing DNS to prevent DDoS attacks

A Distributed Denial of Service (DDoS) attack occurs when users of a target resource, such as a network, server, or website, are prevented from accessing it. These attacks shut down or slow down the resource systems. Intact Domain Name System (DNS) is very centralized, making it a perfect target for cyber actors who infiltrate the connection between the IP address and website name. Such an attack renders the resource inaccessible, redirectable to harmful websites, or unavailable due to crashing. Blockchain can be used to diminish these kinds of attacks by decentralizing the DNS entries. Applying decentralized solutions removes all single and exploitable points, thus strengthening security against DDoS attacks.

3. Decentralizing information storage

Business data hacks, breaches, and theft are a constant cause of concern for most companies. Most businesses still use the centralized form of the storage medium. Hackers can easily access centralized storage by merely exploiting a single vulnerable point. Such an attack leaves sensitive and confidential data exposed to sorts of illegal use. By using blockchain, sensitive data may be protected by ensuring a decentralized form of data storage. It would make it harder and even impossible for hackers to penetrate a decentralized data storage.

4. Securing critical autonomous systems and equipment

Due to advancements in AI and machine learning, automated vehicles and weapons are possible, thanks to the internet that facilitates the transfer of data from the sensors to the remote-control databases. However, hackers target to penetrate and gain access to networks like Car Area Network (CAN). When tapped into, these networks offer complete control and access to vital automotive functions. Such occurrences would have a direct impact on the safety of humans. But through data verification through the blockchain, many adversities can be prevented.