BioSpectrum
the business of Bio & Health Sciences

Listing out 2021 healthcare cybersecurity priorities

12 March 2021 | News

Health organisations are often susceptible to risks through negligence by employees in the form of weak passwords, unencrypted devices, and other failures of compliance

Data in a healthcare organisation is constantly created, replicated, modified, moved around, and disseminated, leaving it exposed to cyber threats. Unlike other industries, the cybersecurity in the healthcare industry is chronically underinvested and outdated.

The lack of security framework invites several cyber-attacks & can cause some serious damage. Some of the most common threats faced by the healthcare industry are:

- Malware and ransomware attacks to exfiltrate data often shut down devices, servers, and even networks, making the data inaccessible to health professionals.
- Not all organisations have the capacity or capital to invest in infrastructure and personnel required for maintaining the constant stream of data. Many health organisations are, thereby, using cloud-based storage for reduced costs and ease of maintenance. Lack of secured encryption on the cloud computing storage can be exploited by cybercriminals for phishing attacks, cyber-frauds, and more.
- Health organisations are often susceptible to risks through negligence by employees in the form of weak passwords, unencrypted devices, and other failures of compliance.

Given the challenges it is safe to say that the struggle to stay updated and secure is larger than ever for healthcare organisations. The time has come to approach cybersecurity strategically. From network access control and installation of firewalls and anti-malware technology, securing the healthcare enterprise is a multi-layered endeavour. Keeping data secure, healthcare industry professionals are now adding data loss prevention (DLP) solutions as another layer of protection. The DLP solution helps with the proactive management of the electronic records of the healthcare ecosystem.

It can offer a tightly integrated endpoint and network, thereby, ensuring that sensitive data is protected from internal and external threats. Having a single console automated security system can set policies, manage incidents and violations, save time and reduce costs. Additionally, the DLP solution offers remediation consoles and promotes data protection awareness

amongst employees through frequent reminders and checks. Although deploying a sound DLP strategy is crucial for the current environment, it is only one part of the broader data protection programme. Health organisations must look into the following factors for an all-comprehensive data protection measure.

Build-up the security culture within the healthcare workforce – The hospital workforce, in general, do not maintain the same level of security awareness as someone in banking or manufacturing industry might. It is essential to train the healthcare staff from doctors and nurses to hospice care attendants and admin staff in maintaining good cybersecurity measures. The measures could be as simple as using two-step verification, regular updates on passwords, training on software and operating system maintenance, and more.

Provide breach training – Employees must be trained on handling security breaches and the right ways to report them. Timely action by a well-informed employee can help prevent data from being compromised further.

Due diligence of third-party partners – Healthcare industry relies on several factors. From doctors and surgeons to nurses and other hospital staff. It also adds hospice staff and caretakers to the list. The list is ever-growing. Healthcare organisations must ensure that their outsourced partners are reliable, follow regular cyber audit checks and have remediation measures including data loss prevention (DLP) tools. Additionally, healthcare organisations should sign a confidentiality agreement with a penalty clause to avoid third-party data leaks and breaches.

Know your network – With the constant evolution of technology, there are multiple devices including mobiles, laptops, medical assets, and more connected through the IoT network. Plan the network updates and security measures based on what is being used, and how.

Controlled access – Access to protected information such as health records, personally identifiable information, and more should be granted strictly on a need basis.

To summarise, the digitisation of the health industry is key. Unfortunately, the healthcare sector has fallen behind in implementing cybersecurity measures. To avoid the potential risk and damages of cybercrime, the healthcare sector will have to step up its cybersecurity game. Data loss prevention measures coupled with employee awareness and due-diligence culture are the key elements for digital security in the healthcare sector.

Filip Cotfas, Channel Manager, Cososys, Romania