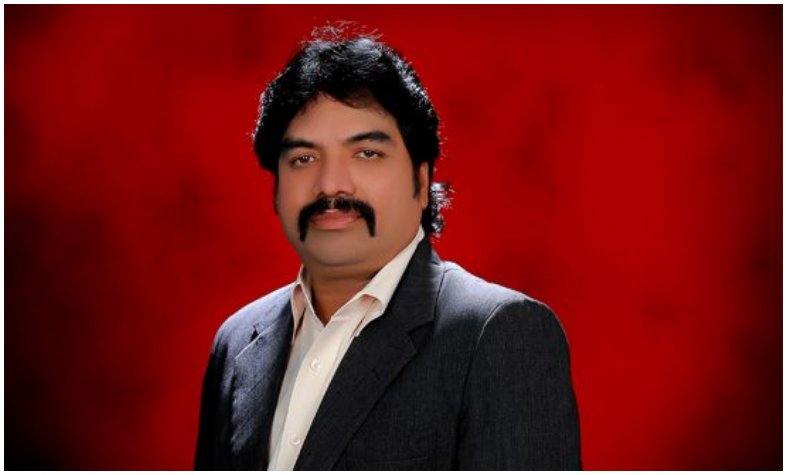
Top 10 Cybersecurity Trends in the Healthcare Sector to Look Out for in 2022

November 29, 2021

Shankar Lingam Sunnathi, Senior Vice President of IT Infrastructure and Compliance, Omega Healthcare Management Services



As SVP, Shankar leads the IT Infrastructure transformation of Omega Healthcare, overseeing the increased adoption of cloud technology, strengthening compliance and data protection and accelerating the adoption of new operating models. His 29 years of experience has been in IT, ITES and Compliance across the Healthcare, BFSI, Pharma, Manufacturing and Fin-Tech sectors. He is also an expert in IT Strategic Planning, Business Process & Technology Systems Development, Enterprise Information Management, and Infrastructure Design & Implementation. He is an IT professional specializing in Global IT Infrastructure Management (India, US, UK, EMEA & APAC). Shankar is an AutomationAnywhere Certified Advanced RPA Professional who also holds a Six Sigma Green Belt certification and an ITIL Foundation certification. He holds a Bachelor's degree in Electronics and Telecommunications Engineering.

A flurry of new threats, technologies, and business models have emerged in the cybersecurity space as the world shifted to a remote work model. Over the years, malicious actors have always targeted the healthcare industry to carry out their mischief, owing to the valuable and sensitive information managed in the industry.

COVID has caused a surge in cyberattacks since such worldwide disruptions are ideal situations for cybercriminals to operate. Organizations are adding cybersecurity experts specifically to scrutinize security and risk issues. Healthcare gaining center stage the past few years, here are the top cybersecurity trends one can anticipate in this sector for 2022:

1. **User Security Awareness:**Healthcare organizations have to take stringent steps to strengthen their security posture. The most common cyber-attack methods must be communicated with users to help them stay vigilant and prevent such attacks. Training and testing users will also help protect the business against cyberattacks, including phishing and other social-engineering attacks.
2. **Hiring Medical Content Writers:**Cyber security in the healthcare sector will be a top focus in 2022. Healthcare organisations should be aware of cyberattacks and take all necessary precautions to prevent them. Most of the cyber-attacks happen at the end-user level —medical professionals, owing to the lack of awareness. Hiring medical content writers to generate educational articles regarding healthcare cybersecurity and its importance is an effective strategy to

CONTACT US

TRENDING THIS WEEK


Need for digital payments players to upgrade their Systems


Five Critical Elements for B2B e-store (e-commerce) Success


How Prepared are you for a Ransomware Attack?


Why CFOs Need Next-Gen Intelligent Platforms to Manage Risk


Building Cyber Resilience in the New Normal – Need of the Hour

3. **More Ransomware Attacks:**Ransomware attacks can prove expensive to organizations in several ways. Cybercriminals take control of files and systems and block authorized users from accessing these, till the demanded ransom is paid. Some of these attacks can temporarily halt patients' treatments. Hence, it is imperative for healthcare organisations to take a proactive approach to ransomware. Medical organisations should have backup copies of patient information to continue operating even if a ransomware attack takes place.
4. **Securing EHRs (Electronic Health Record) Systems Will Be Crucial:**The EHR system is a digital platform that stores a patients' medical history and documents. This technology has aided in the sharing of information and secure storage of data. However, it has increased the risk of fraudsters gaining access to medical data. As a result, EHRs must be monitored carefully to ensure patients' safety and personal information. Organizations need to strictly adhere to the medical privacy laws governing the handling of patient records. Artificial intelligence can be used to improve productivity and security by analyzing EHR data.
5. **Biometrics**: More advanced healthcare organisations and pharmaceutical businesses are currently investigating biometric identification management. The use of biometrics in healthcare organisations is expected to grow, essential to add extra cybersecurity layers, control identity management, and access, thus providing a more seamless clinical experience. Biometrics can help prevent 99.9% of all attacks.
6. **Conducting Risk Assessments Regularly:**More cyber-attacks are expected in the healthcare sector, as predicted; regular risk assessments can assist mitigate this. Regular risk assessments and checks for both product and service reviews will aid healthcare providers in identifying locations that could act as weak links in their security frameworks. These fixed-interval evaluations enable healthcare organisations to promptly identify and confirm data breaches that could result in considerable loss. It will also teach medical workers how to identify specific bugs.
7. **Multi-factor authentication (MFA):**Passwords are the most used form of authentication in healthcare, but they're also the most vulnerable. Although multi-factor authentication is not a new concept, its adoption in the healthcare industry has been slow. Medical professionals can use multi-factor authentication to access medical records and provide medication through doctor/patient portals. Patients can also use biometric MFA to gain access to their records, ensuring the privacy and security they deserve.
8. **Network segmentation:**Companies are increasingly using network segmentation to regulate levels of access to sensitive data. The most significant advantage of network segmentation for the healthcare ecosystem is that it can restrict access to medical data while also ensuring compliance with standards like the Health Insurance Portability and Accountability Act of 1996. (HIPAA). Legacy systems that are currently in the process of being upgraded can benefit from network segmentation to reduce their vulnerability. Many attacks begin with phishing emails to obtain access to a company's network, then move through back-office systems and vital infrastructure.
9. **Real-time analytics:** Healthcare organisations are attempting to break down data silos to share data more effectively across networks. Companies are expanding the number of channels and devices that may connect to the enterprise network resulting in an increased data flow. Analytics is positioned as a key enabler for companies looking to improve their customer service. While healthcare organisations are using analytics to improve health management and clinical efficiency, it is yet to be leveraged to strengthen an organization's security posture.
10. **Advancement in Securing Connected Medical Devices:** Wearable medical gadgets, medicine effectiveness tracking, sleep monitors, air quality sensors, and other Internet of Things (IoT) devices are now so prevalent that they are found in almost every home. Though welcome advancements in the medical field, they can be easily hacked due to their widespread use, portability, and internet-ability. In addition to efforts to design and upgrade IoT devices, technological breakthroughs are required to protect them from being hacked.

Cybercrimes are among the most prolific security threats facing the world currently. To remain ahead of these risks, we need to improve our situational awareness and exchange more information. Healthcare institutions must continue to invest in cybersecurity professionals to protect patient data. There is no better moment than now to strengthen cybersecurity defenses while also improving personnel talents and awareness.

Related Articles

How Virtual Event Platforms Cater To Both B2B And B2C Consumers

6 Top Things Entrepreneurs Look for When Hunting for Office Space

What Is The Future Of Content Marketing – Video or Voice?

Five Critical Elements for B2B e-store (e-commerce) Success

DigitalFirst Magazine