BioSpectrum
the business of Bio & Health Sciences
ASIA EDITION

Essentials of ensuring cybersecurity in the IoMT and telemedicine landscape

19 July 2023 | Opinion | By Hithaishi C Bhaskar

Jess Ng, Country Head of Singapore and Brunei at Fortinet, unravels best practices to mitigate cyber security risks in the healthcare, clinical and pharma ecosystem

Healthcare is evolving with the advancement of digital technology, providing efficient patient care modules at hospitals through access to myriad electronic devices and records. Through Internet-of-Medical-Things (IoMT) devices, healthcare providers can now coordinate care more seamlessly and reduce transactional friction between patients and care teams. Cyber security becomes a responsibility with the deployment of web applications, to prevent data breaches. As the health care ecosystem becomes increasingly interconnected, it might get challenging to tackle ransomware attacks on patient medical and financial data. Moreover, it's also essential to comply with healthcare regulations and policies unique to each country governing the clinical data sharing framework. **Jess Ng, Country Head of Singapore and Brunei** at **Fortinet,** takes us through a deeper understanding of IoMT and telemedicine cyber security threats and strategies to combat the risk. Fortinet is a global driving force in the evolution of cybersecurity and the convergence of networking and security.

- **How crucial is it for the healthcare sector to adhere to more rigorous cyber security measures?**

Cybersecurity is of utmost importance for the healthcare sector, considering the significant role it plays in society. With the exponential growth of sensitive information handled by healthcare providers, threat actors are increasingly drawn to exploit this data for fraudulent activities. As a result, trust is eroded, and regulatory penalties are incurred. By adhering to rigorous cybersecurity measures, healthcare providers can minimize their attack surfaces, reducing the ability of threat actors to breach and disrupt systems. A strong cybersecurity stance becomes an essential component in ensuring exceptional patient care and support.

- **How does cybersecurity in pharma and drug production systems differ from the healthcare ecosystem?**

While both the pharmaceutical and healthcare ecosystems face similar cybersecurity concerns, there are distinctive vulnerabilities to consider. These vulnerabilities range from phishing attacks to employee errors and oversights. Moreover, the pharmaceutical industry has additional considerations, such as reliance on third-party vendors for daily operations. For instance, pharmaceutical organizations depend on clinical research firms for expertise in curative chemicals and logistical

companies for accurate medication deliveries. Managing these dependencies and associated risks is crucial in the pharmaceutical and drug production systems.

- **What are the frequently encountered cyber security risks and what are the best practices to mitigate the impact?**

Phishing attacks are a prevalent cybersecurity risk faced by healthcare organizations, posing threats to patients' sensitive information and resulting in regulatory fines. Another significant risk is the proliferation of Internet of Things (IoT) devices in healthcare, which, if left unsecured, can act as gateways for cyber attackers. The rise of telemedicine and remote connectivity, accelerated by the COVID-19 pandemic, also introduces new vulnerabilities for data interception. To mitigate these risks, healthcare providers can adopt best practices such as regular software updates and patching, deploying zero-trust solutions for granular user access management, and implementing automated backup procedures.

- **With the advent of Internet-of-Medical-Things (IoMT) and burgeoning telemedication sphere, how can patient data be safeguarded?**

Ensuring cybersecurity in the IoMT and telemedicine landscape requires an integrated platform that unifies security solutions across various environments, including data centers, cloud services, and IoT devices. This platform should incorporate open-ended connectors and APIs to leverage security insights from third-party tools, maximizing coverage and return on investment. Supporting solutions like next-generation firewalls (NGFWs) enable comprehensive threat visibility and scalable protection measures, while identity and access management (IAM) solutions help proactively manage insider threats. Implementing these measures safeguards patient data in the IoMT and telemedicine sphere.

- **What are some IoMT that are more susceptible to hacks and why? What is the potential impact it could have on patients and healthcare workers?**

Electronic healthcare record (EHR) systems are particularly vulnerable to hacks due to the sensitive patient health information they handle, making them prime targets for data breaches and ransomware attacks. Portable devices like laptops, tablets, and smartphones are also attractive targets as they contain credentials and patient records, which hackers can exploit. Additionally, legacy systems are prone to disruption from advanced cyberattacks since they lack necessary safeguards and manufacturer support. Prioritizing enforcement efforts on legacy systems until they can be replaced with more secure solutions is crucial in mitigating risks for patients and healthcare workers.

- **How does Fortinet foresee cybersecurity trends and developments in the Asian region? What are your projections for FY 2023 and onwards.**

We anticipate the emergence of new types of attacks within the healthcare ecosystem throughout 2023 and beyond. One particular trend that will gain significant popularity is the use of cybercrime-as-a-service (CaaS) models, allowing users with minimal technical knowledge to disrupt entire operations. Furthermore, the dark web offers specialized models, including money laundering-as-a-service (MLaaS), that can identify and target specific users.

Alongside the rise of as-a-service cyberattacks, threat actors may employ criminal solutions like deepfakes and pre-compromised identities to falsely implicate organizations in malicious acts. While it is advisable for users to exercise skepticism when consuming online content, healthcare providers must proactively implement preventive measures to thwart such attacks.

Another major challenge for healthcare organizations will be the prevalence of wiper malware, designed to irreversibly destroy data on targeted machines. As healthcare providers heavily rely on patient information for delivering proper care, these attacks can cripple healthcare workers' ability to perform their duties and result in severe loss of life.

Hithaishi Bhaskar

hithaishi.cb@mmactiv.com