BioSpectrum the business of Bio & Health Sciences ASIA EDITION

The Conundrum of Modern Healthcare: Digital Innovation and Managing Cyber Risk

31 August 2022 | Analysis

"Southeast Asia, especially the ASEAN region where digitalisation has grown rapidly, has become an attractive target for cyberattacks threat" says Tamer Baker, VP of Global Healthcare at Forescout

Like any other industry today, the healthcare sector has taken strides towards digitalization and innovation. The role of technology has become mission critical within healthcare organisations, underpinning their ability to deliver greatly improved services to patients, and operate at far higher levels of efficiency. Southeast Asia, especially the ASEAN region where digitalisation has grown rapidly, has become an attractive target for threat actors. The challenge is compounded by an ongoing cybersecurity skills shortage that often leaves security teams understaffed and unable to keep pace with the increasing sophistication of cyberattacks.

The explosive adoption of technologies such as telemedicine and connected medical devices has helped streamline workflows and enhanced outcomes for both patients and healthcare professionals alike. Despite all the positive outcomes that technology can bring, it has significantly increased the challenge of securing an edgeless environment where people, devices, apps, data and networks intertwine. If not addressed, an attack can impact a patient's privacy, health and safety, alongside financial and reputational damage.

Bridging the gap between healthcare and security

More Internet of Medical Things (IoMT) devices are being introduced into healthcare networks, especially with the recent rise in telemedicine. This has expanded attack surfaces that can be exploited by threat actors, creating operational challenges should these digital assets be breached or need to be taken offline. Deloitte estimates that 70% of medical devices will be connected by 2023 – making cybersecurity for healthcare IoT an industry focal point.

While they are critical to healthcare organisations, connected medical devices can make it difficult to ensure patient data is kept safe. A study conducted by Forescout earlier this year is a prime example of this. After finding potential security issues on the Axeda platform of IIoT solutions provider, PTC, Forescout discovered seven supply chain vulnerabilities, called Access:7. These vulnerabilities affected more than 150 device models from over 100 manufacturers. Over half (55%) of these vendors impacted were found to be in the healthcare sector.

Despite its prevalence, HDOs often lack the capabilities that would provide them with comprehensive visibility into the network of connected devices, and necessary access controls over them. This hampers efforts to identify critical events, zero in on the source of the problem, and effectively respond when an attack occurs or is imminent.

The future of cybersecurity in healthcare

Organisations can bolster their IoMT security by orchestrating a solid foundation with a well-thought-out defense architecture. The overall strategy should focus on building protection for the most exploitable areas of the organisation – connected medical devices and digital clinical assets.

Here are several essential steps that HDOs can adopt to enact a comprehensive cybersecurity strategy well adapted for the digital-first healthcare landscape.

1. **Get complete visibility of your asset inventory**

Having an accurate, detailed, and up-to-date inventory of connected assets allow teams to fully understand what and where devices sit within their network environment. Through automated discovery, organisations will maximize asset visibility and accountability, making it easier to discover new vulnerabilities in a timely manner.

2. **Continuously monitor all devices**

As hospitals have a whirlwind of devices with differing usage patterns, establishing a reliable monitoring system can help organisations accurately classify and evaluate assets. A detailed understanding of network traffic patterns is vital for security teams to properly group devices that serve similar functions and assign them the appropriate security policies and controls.

3. **Identify unauthorized interactions by cross-referencing endpoints with devices and protocols**

It only takes one vulnerability for a threat actor to gain access and carry out a cyberattack. Organisations need to fully understand device endpoints and their role in the network. By checking your inventory list against a database of known unique device identifiers (UDIs) and associated communication protocols, organisations can identify any unauthorised network interactions and take appropriate action where necessary.

4. **Continuously assess assets for vulnerabilities**

Regular assessment for vulnerabilities is a fundamental part of an organisation's security plans, allowing security teams to proactively mitigate risks of malicious attacks. Good asset and network hygiene involves reviewing devices for outdated or otherwise vulnerable software and operating systems, weak passwords, and known vulnerabilities yet to be properly patched. A Forescout study found that more than a third of healthcare organisations were utilising devices running on unsupported version of Windows, creating security risks.

5. **Baseline expected behavior for each device group**

Collecting and evaluating relevant data on all assets within the ecosystem will provide HDOs with a point of reference on the expected network behavior of each device group, allowing them to set the appropriate security parameters. Should there be any unusual deviations, security teams can quickly identify and remediate threats.

6. **Use machine learning to detect anomalies**

Going beyond asset visibility, another challenge is understanding what goes on between connected devices. Leveraging machine learning capabilities allows hospitals to monitor network communications and swiftly extract information for analysis, comparing device behaviours to identify possible anomalies.

7. **Audit your network structure before segmentation**

An audit of the HDO's network structure provides the necessary information for proper segmentation of devices. Without this in place, intruders who gain unauthorized access can move laterally to other networks or devices, allowing them to launch broader attacks across the organisation.

8. **Enable rapid remediation with an integrated, single source or truth**

All the above insights should be packaged together to help ensure network and device insights are integrated into the security team's preferred interface – whether SIEM, NAC or network security system – to provide an enhanced organization-wide view of the network. That view should reflect actual integration among your security tools and how they work together to take the right corrective action, immediately and automatically . Output from these systems should also be aggregated within dashboards and reports to increase senior management awareness and confidence in your cyber operations.

9. **Conduct ongoing vulnerability testing**

In today's volatile cybersecurity landscape, vulnerability research should be conducted regularly and for all devices in deployment. Security configurations should be studied in a lab environment (disconnected from the actual network) for possible backdoors and security implications, with the actions undertaken in accordance with the vulnerabilities identified.

10. **Stay ahead of threats with continuous, automated cybersecurity**

Networks should be monitored continuously to ensure both segmentations and governance do not degrade over time. If any network patterns are found to be violating the established baseline, the device should be immediately isolated and if needed, flagged for review.

Taking action for a secure future:

Cyberattacks on the healthcare sector have been on the rise. While healthcare data is a prime target for cybercriminals, attacks could have devastating, real-world impact on human life and well-being especially if critical devices are compromised. Now more than ever, the healthcare industry needs to re-evaluate and update operational and security systems to strengthen defenses, adopting more comprehensive, automated cybersecurity strategies.

By Tamer Baker, VP of Global Healthcare at Forescout