HEALTH INTELLIGENCE FOR DECISION-MAKERS

INTELLIGENT health.tech

A Lynchpin Media PUBLICATION

ISSUE 07 www.intelligenthealth.tech

CONNECTED CRIME
The importance of security in healthcare

MENTAL HEALTH
How Headspace is improving lives

INNOVATING OUTCOMES
Utilising EMR for better solutions

PROGRAMMING PROGRESS

Diana Mukami, Digital Learning Director and Head of Programmes at Amref's Institute of Capacity Development, speaks to us about the organisation's work with Cognizant and GSK, and how this has enabled the NGO to improve its digital programmes and provide health workers with real-time data.

THE IMPORTANCE OF EDUCATING HEALTHCARE EMPLOYEES IN CYBERCRIME PREVENTION

In healthcare, 75% of all medical devices are now connected to the Internet. But despite the numerous benefits of these connected devices, it leads to inherent security vulnerabilities that are difficult to patch and secure. Richard Staynings, Chief Security Officer at Cylera, outlines the importance of cybersecurity in this sector and how to educate your staff to ensure you have a strong defence.

The UK's healthcare delivery system is digitalising at pace and this is leading to connected healthcare environments becoming ever more complex and therefore, potentially more vulnerable to a cyberattack.

Healthcare has transitioned from maintaining patient records in manila files at each facility to centralised electronic record keeping with complete system interoperability. This encompasses a broad range of users, including general practitioners (GPs), hospitals, pharmacies, government population aggregate services and public health systems.

Furthermore, the adoption of Internet of Things (IoT) devices for tracking, monitoring and maintenance in the healthcare sector has dramatically increased in recent years. In 2021, US$21 billion was spent on IoT in healthcare – which is predicted to increase to US$54 billion by 2029 as medical technologies continue to develop and the sector drives for greater efficiencies in healthcare delivery.

These connected devices vary from radiological cancer treatment systems, X-ray, ultrasound, CT and PET scanners to infusion pumps that provide life-saving medications. The medical industry benefits greatly from these devices, but they also have inherent security flaws that are challenging to patch against security vulnerabilities and safeguards without the right cybersecurity strategy in place.

It's perhaps not surprising then to know that the healthcare sector is the third most targeted industry globally by cybercriminals, with an average of 1463 malicious attack attempts per week.

Therefore, it's important not to undervalue the level of security that should be applied to these medical devices. Recent studies have shown ransomware attacks are leading to an increase in morbidity and mortality rates and having an impact on even basic healthcare services like scheduling medication. Medical device cybersecurity is a problem that affects more than just patient privacy; it impacts the capability and accessibility of healthcare services, which are essential to guarantee patient care and safety.

Cyber awareness training

The major disruption and damage of a cyberattack on healthcare highlights the important necessity for staff to receive cybersecurity training so they can contribute to the protection of this vital hospital-use equipment. Regular training can help medical employees recognise the warning

signals of a cyberattack, know when one is happening and know how to reduce any risks to patient safety.

Training should include:

1. **Basic cyber-hygiene tips –** Including, using strong passwords that are changed regularly, enabling Multi-Factor Authentication and not clicking on unknown links.
2. **Awareness –** Training employees to recognise the signs of a device that is acting differently from how it should and when it needs to be reported to IT services for review. This should also entail ensuring that medical personnel are well-versed in the risks associated with using these medical devices, such as understanding what a ransomware attack is, what its effects are, how it is initiated and how to respond to unknown emails and steer clear of phishing emails.
3. **Correct processes –** Medical staff members should be aware of the proper procedures for safely connecting medical devices to avoid common mistakes like these devices connecting to a public Wi-Fi network.
4. **Clean up –** All online-connected medical and IT systems need to be properly maintained and managed in terms of IT hygiene. Requirements for IT hygiene should be flexible.
5. **Incident response plan –** In the same way that everyone has a part to play during a fire drill, there should be an action plan in place in the case of a cyberattack.

About

Richard Staynings is a globally renowned thought leader, author, public speaker, and international luminary for healthcare cybersecurity. He has served on numerous working groups and boards and has helped governments and private providers formulate long-term strategies and tactical action plans for improved cybersecurity and patient safety across the industry and across the world.

Richard serves as Chief Security Strategist for Cylera, a pioneer in the space of medical device and HIoT security. He is also author of Cyber Thoughts, a leading healthcare cybersecurity blog, and teaches postgraduate courses in cybersecurity and health informatics at the University of Denver, University College.

Without a suitable cybersecurity incident plan and software backup solution, healthcare organisations run the danger of losing patient data, having an adverse impact on patient care and safety and having their brand name damaged. All employees should be aware of their role and place within this plan.

6. **Crisis Simulation Training –** Once your incident response plan is in place testing this through a Crisis Simulator is recommended. Crisis Simulators are training exercises in which fake crisis scenarios are presented; for example, a ransomware attack, to assess employees' capacity to adhere to their incident response plan religiously and respond to a crisis successfully.

Richard Staynings, Chief Security Officer at Cylera

Cybersecurity training should be performed regularly to ensure staff are up to date with the latest developments in the field. Health facilities should regularly review and identify knowledge gaps among staff to provide pertinent and effective training.

Since many healthcare professionals regularly interact with these devices, their actions are therefore crucial to the prevention of cybercrime. They serve as the patient safety's eyes and ears, managing and keeping a watch on crucial medical and other IoT devices needed to diagnose, monitor, manage and treat patients.

Most medical devices are employed in hospitals and clinics, but since COVID-19, the number of remotely monitored patients has risen. There's an increasing number of traditional and wearable devices sent home with patients, allowing care teams to monitor patients remotely from their homes. This means more systems communicating back to hospitals across the Internet and a greater attack surface for cybercriminals to exploit.

Securing medical devices

With so many medical devices now connecting to the network, how can the industry secure them?

The inventory, risk analysis and risk remediation of hospital IoT (HIoT) linked devices can now be dynamically automated by cybersecurity providers using compensating security measures thanks to advances in next-generation of IoT security technologies. Artificial Intelligence (AI), Machine Learning (ML) and DigitalTwin technology are used to achieve this. With the aid of current network access control (NAC) tools, these technologies enable highly precise analysis and identification of discrete systems, passive risk assessment of frequently delicate life-sustaining equipment and can be seamlessly integrated and automated into the network.

This is an excellent illustration of how cutting-edge security tools are being used to mitigate new risky medical equipment. As many HIoT devices cannot be updated with security patches, medical device 'enclaving' or 'network segmentation' acts as an efficient form of remediation, lowering threats to patients and the medical network. Regulators often allow this compensatory security measure, which enables the ongoing safe use of otherwise end-of-life medical devices.

To protect against the growing threat of cyberattacks, what is required is a combination of people, processes and technology. Advances in AI-based cybersecurity tools mean healthcare organisations can now automate the entire security process, through a progression of asset identification, risk analysis, profiling and improved medical device management. However, you're only as secure as your weakest link and medical staff members are a critical factor in keeping healthcare cybersecure and protecting what matters most – patient care. ✚