Health Business

ISSUE 22.5
www.healthbusinessuk.net

Business Information for Healthcare Professionals

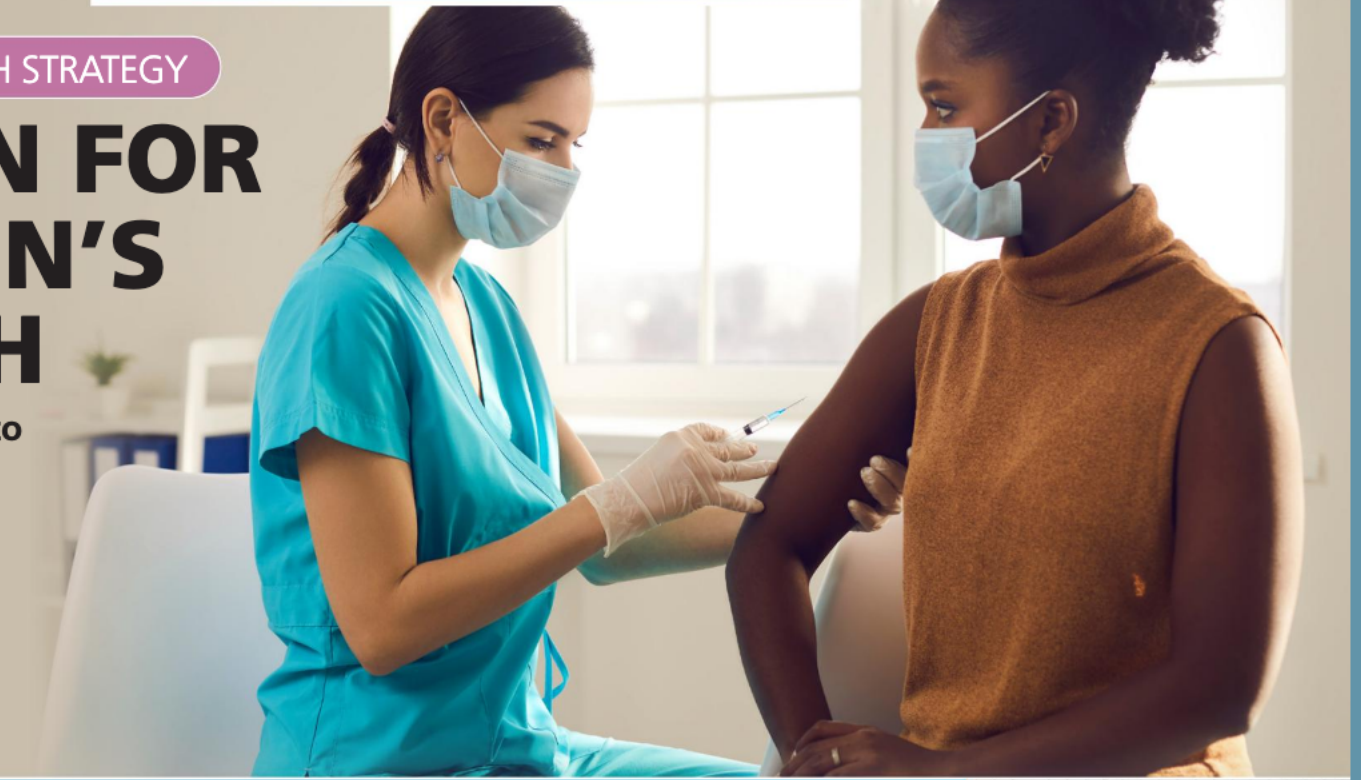
FACILITIES MANAGEMENT

MEDICAL EQUIPMENT

WOMEN'S HEALTH STRATEGY

A PLAN FOR WOMEN'S HEALTH

What can be done to reduce the gender health gap?



PLUS: RECRUITMENT | **NET ZERO** | STAFF WELLBEING | **TECHNOLOGY** | CYBER SECURITY

Mitigating cyber risk

With tens of thousands of dormant medical devices set to be connected to IT networks in the next 2-3 years, potentially exposing our healthcare systems to thousands of vulnerabilities, how can hospitals and healthcare settings mitigate risk to patient safety and care?

Our healthcare delivery system is automating. Through a process of digitalization and adoption of advanced technologies, this is something that has been ongoing for the past 20 years. We have moved from medical records maintained in manila files at each treatment location, to centralised electronic record keeping and full interoperability between discrete medical systems. This includes a long list of users from GPs to hospitals to pharmacies and to government aggregate population and public health systems.

These changes have brought about a dramatic growth of medical devices. These now dominate hospital patient bedsides and act as nurse and monitor. Medical devices are growing at 20 per cent per year globally and at about 6 per cent per annum in the UK. Many of the medical devices found in NHS hospitals and clinics today are not currently connected to the network but are used in a standalone capacity. This however is about to change through interconnectivity and efficiency improvement goals. That means many more connected devices on healthcare networks.

Many medical devices found in NHS hospitals/ clinics today are not connected to the network but are used in a standalone capacity

Medical devices

Medical devices include X-Ray, CT and PET scanners, MRI and radiotherapy machines, to pharmacy robots that dispense medications, to Pyxis cabinets that secure those medications on hospital floors until they are needed, to simple connected infusion pumps and patient telemetry systems that report everything from O2 saturation levels and pulse rate, to automated blood pressure cuffs. They include diagnostic, treatment, patient management and monitoring systems and are ubiquitous across medical providers today.

Most of these are employed in hospitals and clinics, but an increasing number of traditional and wearable devices are sent home with patients following procedures allowing care teams to monitor patients remotely from their homes. Since the advent of COVID-19, the numbers of remotely monitored patients has gone through the roof, and these systems are connected back to hospitals across the Internet. Together medical devices account for more than 75 per cent of connected endpoints at hospitals, and dwarf those devices managed by IT.

Instead of being managed by IT and security, medical devices are usually managed by clinical engineering or biomed technicians, or a mixture of different vendors, many doing so remotely from outside of the hospital. Most of these technicians know little about cybersecurity and IT, and report outside of the IT department in health systems. So historically, there has been very little cybersecurity oversight of medical and other healthcare IoT (HIoT) devices. Nor has there been good cross-walking between teams, though this is changing rapidly.

Unlike traditional IT systems such as workstations and laptops, medical and HIoT devices are quite different. They have very limited CPU, memory and storage capacity, so limited in fact that updated firmware and software that requires a larger footprint cannot be supported. So few are ever patched or updated. Many of these pose a security risk to healthcare networks because of the number of unpatched/unpatchable vulnerabilities that they carry.

Lifespan

Unlike a Windows workstation that has a useful lifespan of two to three years, many medical devices are expected to perform for 15 years or more before finally being retired and scrapped. They are in fact amortized in hospital finances to depreciate over this period so early retirement is usually not an option given the state of healthcare finances. Combined with this, few manufacturers are willing or good at providing timely patches against known CVEs and threats in the wild that affect their systems, even when these systems will support a patch or update, nor have governments mandated that manufacturers do so.

The result is that healthcare suffers from growing cybersecurity risks that could result in another WannaCry cyberattack that takes down much of the NHS and other health systems.

Medical devices can easily be turned into footholds on the network by hackers looking to exfiltrate valuable data or by cyber extortionists spreading malware or ransomware. Medical devices are often attached on one side to the network and the other side to a patient. The patient is thus very thinly isolated from attack over the internet by perpetrators thousands of miles away. Medical devices such as ventilators are used to keep patients alive, yet security is often totally missing on these devices. Few of us would conduct our internet banking on an unpatched 15-year-old PC, yet we trust the health and wellbeing of our loved ones to old unpatched medical devices.

Reducing risks

So, what can be done to reduce risks as existing HIoT systems are connected and to the growing number of new and other devices? The biggest issue is that traditional network vulnerability scanning will crash, break, or permanently damage fragile medical devices. Second, that hospitals generally have a really poor inventory of what devices they own, where they are located and what firmware and software levels each maybe running. And third, that patching devices is difficult even when patches are made available by manufacturers.

We need tools that use advanced technologies like artificial intelligence to identify and profile inventory, and risk assess medical devices passively so as not to harm fragile systems yet still meet industry governance compliance standards. From that profile we can easily establish a baseline of 'normal' network activity for each device and quickly alert when anomalous traffic is attempted – perhaps a sign that a device is being compromised.

NHS Trusts need to evaluate which manufacturers provide secure devices that are supported in a timely manner and remove all others from approved purchase lists

We can also apply compensating security controls to highly vulnerable devices that cannot be patched using existing technologies already owned by trusts and built into their networks. Network Access Control can 'enclave' or 'micro-segment' all at-risk devices and thus provide an additional layer of protection. With the right tools this can be done easily with a simple click of a switch. This avoids having to 'get nasty' with manufacturers for security patches, or the need to strike manufacturers that do not support their devices with timely patches from the approved list of manufacturers for future purchases.

With compensating controls in place, providers can safely continue to use unpatched devices and still be compliant while operating at an acceptable level of risk against cyberattack. Patients are safe, the integrity of the healthcare network is safe, and hospitals don't need to find millions of pounds to replace perfectly working devices that manufacturers are not providing patches for.

Solutions

So, what should be done to ensure that devices currently being used in a standalone manner are safe to connect to the network? First, these devices need to be assessed for current versions and patched where patches are available. Second, all medical devices should be joined to separate firewalled network segments from PCs and everything else. This does not mean a simple separate VLAN (Virtual local Area Network) but a firewalled network zone. This will protect medical devices from critical HIT and vice versa. Third, security and clinical engineering/ biomed teams need to work together to reduce any risks as much as possible. Finally, NHS Trusts need to evaluate which manufacturers provide secure devices that are supported in a timely manner and remove all others from approved purchase lists.

Taking these steps will ensure that your healthcare setting is cyber ready and mitigating against any risk that connected devices could have on patient safety and care. ■

Richard Staynings, Cylera chief strategist
Richard is chief security strategist for Cylera and a globally renowned thought leader, author, public speaker, and international luminary for healthcare cybersecurity.

INFORMATION TECHNOLOGY

4C Strategies – Independent ICT Consultants

4C | STRATEGIES

4C Strategies is an independent ICT consultancy specialising in technology and infrastructure projects.

The company covers all aspects of technology and infrastructure in the enterprise environment, with consultants showing demonstrable experience in helping clients to procure new technologies to meet their business requirements, providing end-to-end support on ICT projects by delivering a portfolio of consultancy services to meet client requirements, from audit and strategy through to procurement, implementation and resourcing.

4C Strategies has been assisting organisations in the healthcare industry for over 20 years. Expertise covers all aspects of IT technology and infrastructure, including: digital strategy, IT and technology strategy, data centres, servers and storage, patient data security, desktop telephony, Microsoft Teams and wide area networks.

Trevor Nelms, Director from West London Mental Health Trust, said: *"4C Strategies has assisted in a range of complex ICT projects, from inception through to deployment, and demonstrated a rare ability to bring together technical expertise with business acumen and tight project management skills."*

Contact one of 4C Strategies' qualified healthcare technology consultants today. ■

FURTHER INFORMATION

Tel: 01858 438938
nhs@4c.co.uk
www.4c.co.uk