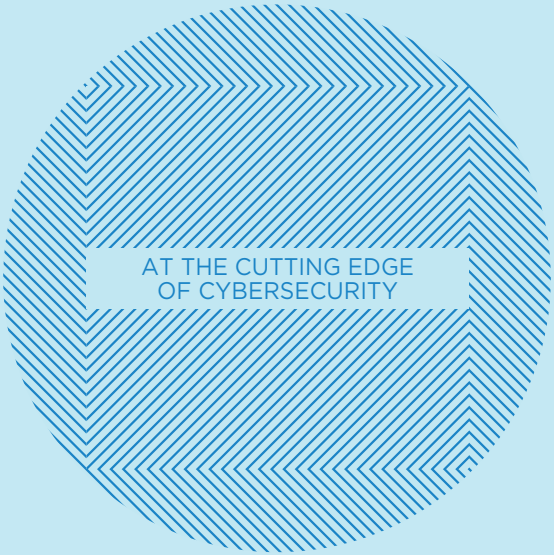

AT THE CUTTING EDGE OF CYBERSECURITY

Until recently the idea of hackers taking control of a pacemaker may have belonged in the plot of a TV show like Homeland, but new regulations in the industry have indicated that the **threat from cybercriminals to medical devices** is very real.

WORDS: **RUTH DORIS**

Dr Anita Finnegan's startup **Nova Leah** is at the forefront of the developing industry of medical device cybersecurity.
The company, which spun out from Dundalk Institute of Technology (DkIT) last summer, has already secured a contract with global dialysis product provider, Fresenius Medical Care for a licence of its first product, Select Evidence. Fresenius Medical Care has more than 300,000 patients and services over 3,600 clinics worldwide.

Select Evidence is the world's first expert cybersecurity risk management software solution system for connected medical devices. The global medical devices market is growing exponentially, and it is estimated it will be worth €440 billion by 2018.

Dr Finnegan worked in engineering and quality management for a number of years before embarking on a PhD programme at DkIT. The initial topic of her research was software validation, however, a conversation about medical device cybersecurity prompted Anita to change her focus. Her research caught the attention of the industry and a few months into her study, industry publications started to take notice.

An invitation to pitch her research at the headquarters of the US Food and Drug Administration (FDA) in Washington led Dr Finnegan to publish two technical reports on the area. Commercialisation funding from Enterprise Ireland enabled her to convert the manual framework from her PhD research into a commercial software solution. Dr Finnegan says: "Once I knew that what I was doing was gaining traction, that it was a solution for the industry, it was the obvious next step to explore that."

Following two years of development the first product was ready and Select Evidence was licenced in 2016. In recent months, the WannaCry ransomware attack, which exploited a Windows system vulnerability, caused chaos across the globe affecting organisations including the UK's National Healthcare System and highlighted the increasing need for more robust systems in the areas of healthcare.

So what devices are at risk? Anything that has a communication capability can be

DR ANITA FINNEGAN
→

hacked, Dr Finnegan says. "We know medical devices are quite vulnerable; they're sitting on a network they can be used as an open door for someone to get in and launch a malware attack on the entire network."

However, despite depictions of hackers in film and television, devices such as pacemakers have been hacked in controlled environments, but no patient has been harmed because of hacking, she adds. While a hacker gaining control of a pacemaker is unlikely Dr Finnegan says the real threat is around the privacy of patient data and comes from malicious users looking for monetary value from patient records.

Your patient or health record is worth three to five times more to a hacker than your credit card details because it includes your health insurance and financial information, she says.

Governments are looking at regulations around the privacy of patient data, and Nova Leah has a specific solution for guiding manufacturers through those processes. As a market first, Select Evidence has no other software solution competitors.

Medical device cybersecurity is almost like a new market within an existing market, Dr Finnegan says. A few years ago, no one really considered implementing cybersecurity requirements into medical devices because no one thought anyone would really hack a medical device.

"When I looked to the medical device domain, and I looked at some of the pain points for the manufacturers, the first one was that cybersecurity expertise didn't exist in the domain and the second one was the cost of compliance for implementing these new practices. And that's very much what I was trying to overcome with our product Select Evidence," Dr Finnegan explains.

With a lack of expertise around cybersecurity medical device manufacturers can implement their own customised systems, however "it's very much a learning curve for them. They don't have any historical data which our system does. It would be quite a lengthy and a costly process for them," Dr Finnegan says.

The other solution for a medical device company is to employ the services of security consultant who can come into the organisation and carry out an assessment of a device and identify the security fixes that are needed. However, the problem with this approach is that the knowledge remains with the consultant who is in on a temporary basis and there is no continuous monitoring of the devices.

Select Evidence is "an intelligent cybersecurity risk management tool; if a manufacturer specifies what their device technologies are we find the vulnerabilities, and then we find the fixes for those vulnerabilities."

Protecting existing devices is one of the big issues, Dr Finnegan says. The FDA has released two guidance documents to manufacturers. The first one recommended that manufacturers implement cybersecurity requirements into new products during the development life cycles. The second recommends continuous monitoring of devices for new vulnerabilities, which covers legacy or existing devices.

Nova Leah's solution can run updates on new vulnerabilities continuously. "So when we find something new for a device that could be in the market for a year, two years, five years, they're alerted, so you're essentially demonstrating that they are conducting that continuous vulnerability monitoring."

Similarly, a device that's been in use for 15 years can be assessed for vulnerabilities using the system.

Dr Finnegan says the next step is to incorporate a communications capability into the product, to allow hospitals and manufacturers to automatically share relevant information.

"One of the big issues in this domain is the fact that the two aren't talking as much as they should with regards to how best to maintain the security of a device. What our system allows manufacturers and hospitals to do is to automate that communication."

The system will allow a manufacturer to let a hospital know when it makes a change to a device, and the hospital will be able to query specific security-related information from the manufacturer using the system, she says.

Nova Leah opened an office in Boston earlier this year, targeting the US imaging and electro market worth an estimated $155 billion of which connected devices account for $51 billion. Nova Leah, which recently announced that it would create 78 new jobs over the next five years, is running some large pilots this year and the company has some follow-on products in development.