Healthcare IT News

A APAC Feature

# Healthcare cybersecurity – the impact of AI, IoT-related threats and recommended approaches

**An interview with Richard Staynings, Chief Security Strategist, Cylera.**

Currently leading healthcare security strategy at Cylera, a biomedical HIoT security startup, Richard Staynings has more than two decades of experience in both cybersecurity leadership and client consulting in healthcare. Last year, he served on the Committee of Inquiry into the SingHealth breach in Singapore as an Expert Witness. He recently spoke to Healthcare IT News on some of the current developments in healthcare cybersecurity.

**Q. Artificial Intelligence (AI) applications in healthcare are all the rage now, and so are cybersecurity threats, given the frequency and intensity of healthcare-related incidents. In particular, some of the cyberattacks have become more sophisticated through the use of AI to get past cyber defenses. On the medical devices front, AI is also being used to constantly manage and secure the rising number of healthcare IoT devices as they connect and disconnect from hospital networks. How do you think the application of AI in healthcare cybersecurity will be like in the next few years?**

A. Healthcare is widely considered to be an easy and soft target because "who in their right mind would attack the weak and defenseless?" …. or so the thought goes! The fact is that healthcare presents a rich target for cyber criminals because of the value of the data hosted and processed. When you couple that with a chronic historical underinvestment in the development of capable cybersecurity teams and tools across healthcare, you can see why perpetrators are so keen to break walk in. But it's no longer the theft of medical records, or PII that concerns me, it's the wholesale theft of intellectual property from research universities and pharmaceuticals by rogue nation states, (one in particular) and the potential to hold both hospitals and their patients to ransom by just about anyone. That's what really worries me most.

I believe we are on the cusp of an AI arms race. Attackers are busy designing new attack vectors and methods to get by cyber defences that heavily leverage AI and Machine Learning (ML). Advanced persistent threats (APTs) that hide unnoticed on the network for years sometimes, while gathering vital information and gradually expanding their footprint till they own the entire network, just as the attack on SingHealth in 2018 demonstrated. AI that perfectly emulates the normal acceptable behavior of users and systems on the network and as such goes undetected by even the best cyber defences.

'Offensive AI' mutates itself as it learns about its environment to stealthily mimic humans to avoid detection. It is the new cyber offensive weapon of choice and will automate responses to defensive measures rather like playing chess with a computer – it learns as it goes. But increasingly the intent of attacks is not just to steal information but to change it in such a way that integrity checking is impossible. Did a physician really update a patient's medical record or did 'Offensive AI' do it? Can a doctor or nurse trust the validity of the electronic medical information presented to them? This is the new threat and it is best executed by AI.

Why would anyone do this? Well, I can think of at least three reasons: Cyberwar, monetary extortion, and as a distraction from even more nefarious attacks against military targets or military secrets.

AI is already being used very effectively for cyber defence. Advanced malware protection that inoculates the LAN and responds in nano-seconds to anomalous behavior patterns. Biomedical security tools that use AI to constantly manage and secure the rising number of healthcare IoT devices as they connect and disconnect from hospital networks, just as my company, Cylera makes. AI-powered attacks will outpace human response teams and outwit current legacy-based defenses. 'Defensive AI' is not merely a technological advantage in fighting cyberattacks, but a vital ally on this new battlefield and the only way to protect us all from the cyber criminals of the future.

**Q. You will be conducting a cybersecurity workshop titled "The rising threat of Internet of Things -Everything from Medical Devices to Hospital Management Systems" at the upcoming HIMSS AsiaPac19 conference. Could you give us a primer on some of the common IoT-related cybersecurity threats in healthcare?**

A. So unlike IT devices, by and large IoT devices can't be centrally managed, patched, updated, or secured. IoT devices are simple and functional. They open and close a set of elevator doors, and move the elevator car to the desired floor. That's all they do. They do it well and they do it millions and millions of times during their life spans. The same is true with medical devices that administer drugs to a patient at a certain flow rate based upon the drug library, report on vital patient statistics like BP, heartrate and O2 saturation, and scan patients for broken bones, tumors, and other ailments. Most were designed at a time long before sophisticated and well-funded nation state cyber criminals, and a time when devices were by and large not connected to the Internet.

Now these devices are managed remotely from hundreds of kilometers away by third party vendors who can do the job better, faster and cheaper than having a number of Full-time Equivalents (FTEs) on staff locally. Thanks to digitalization and interconnectivity, devices now communicate directly with HIT applications and the EMR – something most older systems were never designed to do. And they certainly were never designed to connect securely. By network-connecting these highly insure devices we have opened Pandora's Box, and the number of network-connected HIoT devices is growing at an exponential rate.

The big question is how do we understand what we have on our networks, assess and quantify their threats and vulnerabilities, and remediate those risks in such a way that patients are not placed at potential harm from attack by medical device. How do we identify when one of these devices is behaving abnormally so we can swap it out before attempting to treat a patient based upon false data? How can we identify when a device has been compromised and is being used to attack the hospital? These are things that physicians, nurses, and biomedical technicians are not currently trained to look for!

**Q. Cybersecurity is a constantly evolving field these days with the rapid advancement of technologies as well as the increased sophistication of cyber-criminals. How do cybersecurity professionals such as yourself learn to stay ahead of the curve and keep abreast of the latest developments/ training?**

A. Many people who remember the dot com era of the late 90s will remember the term "Internet Year" to describe the rapid pace of change affecting IT at the time, where a year's worth of development would be crammed into a few months. Well in cybersecurity, things change by the week. That includes threats, vulnerabilities, threat-actors, attack-vectors, new offensive and defensive technologies, and even a few advances on the procedural front as we discover better more efficient ways of doing things.

I can't talk for everyone in my line of work, but I spend a lot of time reading blogs, tweets and other social media posts from experts in the field, as well as a lot of articles from the cybersecurity and industry trade press like Healthcare IT News. I also read more than my share of white papers and academic journals. My reading includes developments not just in cybersecurity but also healthcare and other industries which allows me to consider the implications of new non-security technologies and how they might impact cybersecurity and risk.

One thing that really concerns me right now is the exponential growth in IoT – everything from network-connected home thermostats, to internet connected refrigerators, connected vehicles, to connected cities where traffic lights are optimized to allow the free passage of an emergency ambulance through rush hour traffic and everything else. This is an area I spend a lot of time researching. IoT devices already outnumber the human population of the planet, and by next year there will be in excess of 20 billion network connected devices. Now consider that even a small percentage of these devices might be out to attack you and you can see the magnitude of the problem. The growth of botnets, now far overshadows unpatched Windows machines that have been turned into zombie attack systems by their real owners – the hackers and nation state cyber forces that easily took advantage of weak security and now own their user's online banking information and shady personal photographs. I sometimes think you should be required to pass an owner's test before being allowed to purchase a home computer!

I also consider security and industry conferences to be a great source of vital information. I probably speak at 20+ conferences every year and attend quite a few more on top of that. I always learn something from the discoveries and relayed experiences shared by other speakers and practitioners in the space. There's also a lot to be learned by the way healthcare is delivered and secured in different countries even though I work in quite a few. HIMSS, CHIME, AEHIS, RSA, BlackHat, and KiwiCon, currently top my list, as do conferences and summits put on by various publications in the space. They are all good, and if you can spare the time and afford the admission then you always come away with something in my experience.

**Q. A constant challenge for healthcare organisations is the management of limited resources and budgets for cybersecurity measures, and cybersecurity can often become an afterthought. What advice would you give to them in their approach to cybersecurity, particularly in light of their resource constraints?**

A. In one sentence? Treat Cybersecurity risk in the same way you treat Patient Safety because the two are inextricably linked in today's connected digital healthcare environment. Many hospital CEOs, Boards of Directors and Ministers of Health haven't realised this yet. The sooner they do the better for all of us.

Another piece of free advice for healthcare boards is that healthcare compliance does not equal to security. The industry suffers from a myopic focus upon protecting the confidentiality of patient data, when in fact operational and reputational risks to data integrity and system availability are far more important and potentially damaging. No one is going to die because of a confidentiality breach, they could however easily die as the result of an integrity or availability cyber-attack. The industry needs to adopt a risk-based approach to security based upon assets rather than controls. Only then will healthcare boards begin to understand their level of exposure, and feel inclined to do something about it.

In essence we have several giant gaps currently. A gap between the ease of a perpetrator attacking a victim, making lots of money from that attack, then walking away scot-free, versus making cyberattacks difficult and very costly for the perpetrator – whether that perpetrator is an individual, a criminal group, or a nation state.

The other gap we have is in resourcing. According to the Cisco Annual Cybersecurity Report, there is a 12x demand over supply for security professionals. We need to train tens of thousands of security analysts, architects, threat analysts and security operations staff for the world of tomorrow. We also need to allocate much greater budgets towards securing the future of our businesses, whether that business is a profit-making enterprise or a public service. This is a simple legal question of negligence in my opinion. If those ultimately responsible choose to ignore or accept a critical risk against the advice of their security and risk executives, then they should be held personally liable. Especially in healthcare where patient lives are at stake. ■

**Richard Staynings will be speaking at a session titled "The importance of AI and ML in Healthcare Security" scheduled on October 9 from 1.30pm - 2.00pm at World Ballroom B, Level 23. He will also be conducting a cybersecurity workshop titled "The rising threat of Internet of Things -Everything from Medical Devices to Hospital Management Systems" on the same day scheduled from 3pm-5pm at Lotus Suite 6, Level 22.**