How did you first become interested in hacking and cybersecurity?

My parents were poor, but somehow—I still don’t know how—they bought me a computer for Christmas when I was in sixth grade. A year later, my friends and I were reverse engineering video game software so we could get higher scores and better equipment (primarily virtual swords and shields). Those foundational lessons we learned are still very relevant when looking for security issues in modern software and even medical devices. Thanks, Mom and Dad!

What is the most common type of cybersecurity attack on a healthcare facility, and why?

Networks are under constant attack. Go ask your IT security folks about what they see on a daily basis; it might surprise you. Most of what you’ll see are automated, indiscriminate attacks against employees who happen to browse to the wrong webpage or open the wrong attachment. These attacks are not targeted toward the healthcare industry, but target anyone unlucky enough to be at the wrong place at the wrong time. These are the most common types of attacks we see against healthcare facilities. Every once in a while, though, we’ll see someone who is targeting healthcare. While more rare, these attackers are very familiar with the data available within a healthcare facility. I’ve seen a healthcare facility have one of its patient databases encrypted and a ransom demanded by an attacker.

What is usually the weakest link, securitywise, in a healthcare facility? How so?

I don’t really like the term “weakest link.” We all have jobs to do, and sometimes our daily lives can make it difficult to maintain strong security. Instead, of thinking about “weak links,” I think it’s better to look at who is most often targeted. It’s often the normal employee of the healthcare facility who is targeted. These folks are just trying to do their jobs, but they usually have access to some very critical systems and/or data, which makes them very attractive targets for attackers.

What is the best way for healthcare facilities to safeguard against those attackers?

Awareness, training, and responsiveness are excellent ways for employees to safeguard against attacks. Working at a healthcare facility, I’m sure you know the signs of choking and shock, as knowing these signs could be essential to your success in saving someone’s life. Information security in healthcare is no different. Having awareness and training on what potential compromise looks like and quickly communicating that information to the right people can save your patients’ data and, maybe one day, your patients’ lives.

Billy Rios is a cybersecurity expert and founder of Laconicly LLC. He often consults with healthcare institutions and describes what an attack against a healthcare organization looks like from the hacker’s perspective.
In general, what can healthcare facilities and/or manufacturers do to make medical devices more resistant to attack?

This is a great question! We have a long way to go in order to secure our medical devices. Manufacturers can step up their security game by putting forth the effort to ensure they are releasing reasonably secure products. Security isn’t a zero-sum game; it’s possible to have both reasonable security and an excellent user experience. I think the Apple iPhone is a great example of how we can have both security and a great user experience. If our medical devices were as secure as our smartphones, I think it would be a great win. Hopefully the new FDA 510(k) guidance will help push this forward.

Healthcare facilities face a different challenge. They don’t have much opportunity to improve on the security engineering of a medical device. Instead, most of the work done by healthcare organizations is protecting the device through deployment considerations and security monitoring. Healthcare facilities do have one key driver that no one else has—they decide where they spend their equipment dollars. Having security requirements built into the procurement and acquisition processes can show manufacturers that you are serious about device security. If you need help with developing strong procurement language, talk to the Mayo Clinic or Kaiser Permanente. They have excellent security-related procurement language.

What about their networks?

Networks are notoriously difficult to secure and defend. There is an old saying that always makes me chuckle: “If you’ve seen one hospital network, you’ve seen one hospital network.” Currently, network and equipment deployments within healthcare organizations are not regulated. Healthcare facilities are on their own when it comes to architecture and security protections for their networks. It’s a very serious responsibility, and it’s the foundation for keeping patients and their data safe.

What do you think about President Obama’s increased emphasis on cybersecurity as it relates to protecting consumer data? How does that relate to healthcare?

It certainly shows that the administration takes cybersecurity seriously. Legislation will help drive key components on how we view cybersecurity. I will warn you about relying on legislation and the government to save you against cyberattacks. As someone who works closely with several state and federal government agencies on cybersecurity, it’s a very daunting task. Many state and federal organizations are still trying to figure out what the appropriate role of government is and what types of initiatives have the most impact. These efforts simply have not trickled down to individual healthcare facilities. I’m not sure if they will any time soon.

Can you explain what an escalation exercise is and how it relates to cybersecurity in healthcare?

There are a couple different ways you can exercise escalation. We often are asked to conduct an “adversarial assessment,” which shows what an attacker would be able to gain access to if they decided to attack a particular healthcare facility. Normally, we’ll start with one or two users on the hospital corporate IT network. From these users, we’ll escalate to other users and other systems. Once we have these other systems, we’ll escalate to medical devices or key patient databases. At the end of the exercise, we have a map of how someone could get access to various data and equipment on the hospital network.

What type of medical device might we be surprised to learn is open to exploitation by hackers?

Generally speaking, all devices have a long way to go. If you look at a recent U.S. Department of Homeland Security (DHS) advisory (https://ics-cert.us-cert.gov/alerts/ICS-ALERT-13-164-01), you’ll see that poor cybersecurity spans across multiple vendors and various classes of devices. I’ve been conducting security research on various infusion pumps over the last few years; these devices are very interesting.
Late last year, the DHS started looking into at least two dozen cases of possible cybersecurity flaws in medical devices ranging from artificial heart implants to hospital infusion pumps. I understand hackers want to steal patient data, but can you explain why a device is a hacking target as well?

One question I often hear from healthcare providers is, “Why would anyone attack a medical device?” The answer I give is, “I don’t know.” It’s impossible to guess the motivations or the emotional state of another human. People can show some of the most compassionate efforts toward each other, but people can also be irrational. Why someone would use a cybersecurity exploit to hurt another person, I don’t know. Is it possible from an engineering standpoint? It certainly is. Instead of focusing on the motivations of individuals, I try to help raise the bar for medical device security engineering. If we can raise the bar for medical device security engineering, we make it difficult for anyone to exploit a medical device, regardless of their motivation. Our patient safety and cybersecurity should not rely on the goodwill of strangers. Solid engineering is the better option.

In your opinion, what is the best practice for hospital risk assessments, i.e., how often should they be done and how deep should they dig?

This is a tough one. When I look to healthcare facilities and cybersecurity, I see two very strong leaders: the Mayo Clinic and Kaiser Permanente. These two organizations are pushing healthcare cybersecurity forward in a serious way. I also understand that not every organization can do what a Mayo Clinic or a Kaiser Permanente can do. I understand that some healthcare organizations have

Poor cybersecurity spans across multiple vendors and various classes of devices.
small staffs, tiny budgets, and can’t spend significant resources on cybersecurity. Please remember, regardless of size or budget, your organization always has a voice! Let your suppliers and device manufacturers know that cybersecurity matters to your organization. These conversations add up and can change the security landscape in a significant way.

What do you see as the single biggest challenge as it relates to hospital cybersecurity and threats from hackers?

We’ve set hospitals up for failure. The software and devices on your network are very susceptible to attack. Some manufacturers are making strides to improve their software and device security, but hospitals are laden with what we call legacy software and legacy devices. As such, this software and hardware has never gone through any type of cybersecurity review. These devices and software are extremely vulnerable to attack. This legacy equipment often is expensive, difficult to replace, and has a long equipment life cycle. Securing legacy devices and software is one of the biggest challenges to healthcare cybersecurity.

How do you think that challenge should be addressed?

Replacing the equipment is most preferred, but in most cases, it’s simply not practical. Information sharing can help secure legacy devices. If your organization conducts a risk assessment against a legacy device, share the results of that assessment with other organizations! If your organization discovers a novel way to secure a security exposure for a sensitive device, share that information with other organizations! When it comes to cybersecurity, we’re all on the same team.

Is there another industry healthcare should be looking to when it comes to its approach to cybersecurity?

I really like what the mobile device industry has done with cybersecurity. Your iPhone and Android phones are reasonably secure. Is it perfect? Of course not. No software and device can be 100% secure, but smartphones are a great example of great cybersecurity with great user experience. If our medical devices could be at least as secure as the phone you have in your pocket, it would be a great thing for patient safety.

If you could change one thing in healthcare cybersecurity today, what would it be, and why?

Information sharing! I know of many different organizations doing wonderful things in cybersecurity. Mayo Clinic is pushing device security forward in a big way. Kaiser Permanente is investing heavily in cybersecurity. The U.S. Department of Veterans Affairs is working on some great initiatives. I’m sure there are other organizations that are discovering ways to protect their patients from cybersecurity vulnerabilities and exploits. If we worked together on this problem, I think we’d be a lot more effective!

If we can raise the bar for medical device security engineering, we make it difficult for anyone to exploit a medical device, regardless of their motivation.

No software and device can be 100% secure, but smartphones are a great example of great cybersecurity with great user experience.
The Healthcare Technology Management Collection

A must-have for clinical engineering departments, the 2015 edition includes 25 of AAMI’s most popular HTM resources.

Practical information written by, and for, engineers and technicians, this CD includes guidance on:
• The Joint Commission
• IT
• Troubleshooting Equipment
• Benchmarking Salaries and Benefits

Order code: HTMC
List $730 / AAMI member $510

Order your Copy Today!
Call +1-877-249-8226
Visit www.aami.org/store
The AAMI Foundation thanks Carefusion for its generous Diamond-level partnership in supporting the National Coalition to Promote the Continuous Monitoring of Patients on Opioids.

www.aami.org/opioids