digicert®

DRIVING SECURITY AND COMPLIANCE ALONG THE MEDICAL DEVICE LIFECYCLE

DigiCert's Mike Nelson on Meeting the New Medical Device Security Expectations

ISMG
INFORMATION SECURITY
MEDIA GROUP

digicert®

MIKE NELSON

Nelson oversees strategic market development for all products, including Device Trust, Software and Content Trust, Enterprise Trust, and Trust Lifecycle Manager. He is dedicated to promoting patient safety and preventing disruptions to the delivery of care. Before joining DigiCert, Nelson spent his career in healthcare IT, including time at the U.S. Department of Health and Human Services, GE Healthcare, and Leavitt Partners. He frequently consults with organizations, contributes to media reports, and speaks at industry conferences about the risks of connected technology and what can be done to improve the security of these systems.

Over the past decade, the industry has made gradual strides toward enhancing security for connected medical devices. Now, with the FDA wielding the power to regulate these devices, including the ability to deny approvals for those that fail to meet specific cybersecurity requirements, a pivotal shift toward ensuring patient safety has materialized.

In this video interview with Information Security Media Group, **Mike Nelson**, Vice President of Digital Trust at DigiCert, discussed:

- Navigating the complexities of FDA cybersecurity regulations for medical devices;
- Common challenges medical device manufacturers encounter throughout the device lifecycle;
- Effective strategies for safeguarding devices and securing the software supply chain.

EVOLUTION OF MEDICAL DEVICES

TOM FIELD: Tell me about the evolution in medical device manufacturing and how you became involved in the healthcare sector.

MIKE NELSON: I've been involved in healthcare on the medical device side for quite some time. I started my career at Health and Human Services,

"There's no silver bullet to security, but having a good deployment of public key infrastructure is a good starting point because it allows you to check so many of the boxes that are in the guidance."

the department that oversees the Food and Drug Administration, which is responsible for regulating the safety and security of medical devices. I then went to a small company, GE Healthcare, building medical devices and their associated software.

That's where I saw the challenge of cybersecurity for the first time. I've done some consulting, and then I ended up at DigiCert, a world leader in cyber. We've done a lot in the medical device space and work with a lot of large manufacturers.

When I joined DigiCert, there was no regulation around building cyber-secure products. It was always an afterthought. It was part of the QA process and something that we wanted to say that we did, but we didn't put a lot of energy and focus on it. Today, with the number of connected devices, the software, the complexity of software running on those devices, the landscape has changed dramatically. Data and the amount of data being generated by these devices is just astronomical, and so is the value that it's providing for providers to improve quality of care outcomes.

As of October of last year, the Food and Drug Administration has the ability to regulate the security of connected medical devices and device manufacturers that are submitting a 510(k) to the FDA for approval. They have to demonstrate that those devices are cyber-secure, and that's done with a handful of documents based on the NIST cyber framework. If the device is not secure, they can deny it going to market. For the first time ever, the government now has the ability to regulate that and to make sure that devices going to market are secure.

IMPLICATIONS OF THE NEW FDA GUIDANCE

FIELD: What are the expectations for new products and the things devices have to be equipped with now?

NELSON: The Food and Drug Administration has put out guidance for medical device manufacturers to follow, and it's based on the NIST cybersecurity framework, which includes "identify, protect, and detect devices" and then "respond and recover from incidents." It requires manufacturers to show how they can identify vulnerabilities, how they respond to those vulnerabilities and how they can recover. They have to have documentation that shows that they're prepared for that. They also have to show what they're doing to protect those devices, and the FDA is requiring things like strong device authentication to back-end systems or to other devices.

They're requiring encryption of data and strong identity. They're requiring devices to have the ability to be updated once they're in the field. They're requiring software signing and the use of software bills of materials. All of these security best practices are in the guidance from the Food and Drug Administration, but they are also security fundamentals. They are things that those of us who've been in cyber start with. The guidance document is good. The Food and Drug Administration has done a good job of having the baseline requirements and holding the industry to a higher standard.

HOW TO IMPROVE MEDICAL DEVICE SECURITY

FIELD: Where should those that don't currently meet the standards start, and what are some of the security best practices they should be doing now?

NELSON: It comes down to awareness of risk. You have to get the risk assessment to know where you're vulnerable and what ways the devices can potentially be attacked. Then you have to prioritize those risks. The Food and Drug Administration is not making these guidelines optional, so if you have software running on your device, you need to do code signing to ensure the integrity of that build. You need to share a software bill of materials with all submissions, use certificates to authenticate connections, and protect data at rest and in transit.

Those are good starting points. Each one of those security approaches uses technology known as public key infrastructure. There's no silver bullet to security, but having a good deployment of public key infrastructure is a good starting point because it allows you to check so many of the boxes that are in the guidance.

SECURITY CHALLENGES FOR MEDICAL DEVICES

FIELD: When you look at the lifecycle stages— design, develop, build, deployment— where do you see medical device manufacturers struggling the most?

NELSON: One of the challenges for healthcare is that once devices are deployed, it requires a collaborative approach to secure the device from that point forward. That's because healthcare providers, the hospital systems, don't want manufacturers updating the device whenever they want. You certainly don't want to be performing an update to a surgical robotic in the middle of surgery; it could cause harm to a patient. So there has to be coordination and collaboration between the healthcare provider and the manufacturer. That's a new muscle that's being developed.

I see a lot of struggles in terms of maintaining security of those devices once they're deployed. Planning for updates and making sure that the security of those devices is maintained are the biggest challenges. Manufacturers are doing a better job of designing and building secure devices. We've seen tremendous improvement on that, and the Food and Drug Administration can be commended for that. But the biggest challenges still remain in coordinating the maintenance of security and the management of security once those devices are deployed.

CENTRALIZING AND STANDARDIZING MEDICAL DEVICE SECURITY

FIELD: Let's talk about some of the successes. Can you share any examples of successful cybersecurity practices you've seen implemented by the manufacturers to fortify the security of their devices and achieve compliance as well?

NELSON: We're working with a handful of the top medical device manufacturers. There are two components of security for devices. You need to protect the device, and you need to protect the software on the device. We're working with a large medical device manufacturer out of Germany, B. Braun. We've done some public case studies with them.

"What the Food and Drug Administration has done sets a precedent for the industry to say, 'We can no longer tolerate insecure devices. Patients' lives or patient health can be impacted from cyber vulnerabilities.

Braun is providing a centralized security approach to code signing and to birth and operational certificates for devices that go in the field so that they can be updated. They have created some good governance language and policies for their global team of products. They push that governance language out and say, "If you're doing security, you need to be following these approaches. We have a tool set for you that allows you to do that in a very seamless way, and we can achieve economies of scale with that."

Braun is centralizing security, and a lot of other large manufacturers are centralizing their security approach, which brings a handful of benefits to the manufacturer. It gives you certainty that the solution is going to be deployed in the right way. It also gives you centralized management and visibility into the devices that have that technology. And it gives you the ability to mitigate and to intervene if something goes wrong because you have better management and visibility of it. There are tremendous benefits from an economic standpoint; you get economies of scale. It allows you to do more and spend less.

MEDICAL DEVICE SECURITY MATURITY

FIELD: Any final thoughts you want to share on the future of medical device cybersecurity?

NELSON: We are going to see a lot of maturing in the next couple of years. What the Food and Drug Administration has done sets a precedent for the industry to say, "We can no longer tolerate insecure devices. Patients' lives or patient health can be impacted from cyber vulnerabilities, and the industry no longer will tolerate that."

We're going to see a lot of maturity. We'll see healthcare organizations start making purchasing decisions based on the security of devices. Healthcare organizations are getting smarter in their purchasing and saying, "We're not going to buy devices that have massive cyber vulnerabilities." More maturity and better practices around security are coming.

Partner with DigiCert for a security foundation that enhances your initiatives. Contact us at digicert.com/contact-us to learn more.

digicert®

From patients to payers, from data to devices, digital trust is a must for the medical world. Learn how DigiCert is securing every corner of the healthcare ecosystem: www.digicert.com/industry/healthcare-security

About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to information security and risk management. Each of our 36 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment and fraud. Our annual global summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

(800) 944-0401 • sales@ismg.io

BANK INFO SECURITY® · CU INFO SECURITY® (Just for Credit Unions) · GOV INFO SECURITY® · HEALTHCARE INFO SECURITY®

infoRisk TODAY · CAREERS INFO SECURITY® · Data Breach TODAY (Prevention. Response. Notification.) · CyberEd.io

CIO.inc · DeviceSecurity.io · PaymentSecurity.io · FraudToday.io

CYBER THEORY · CyberEdBoard · Xtra mile LIFECYCLE MARKETING · GREYHEAD

ISMG
INFORMATION SECURITY
MEDIA GROUP

902 Carnegie Center • Princeton, NJ • 08540 • www.ismg.io