Cybersecurity Product Lead

Mariana Hu (36) has been working as a Product Cybersecurity Lead in Noah Medical (Medical Equipment Manufacturing company) for the last two and a half years. She got her Bachelor of Science and Master of Science in Biomedical Engineering in the University of Connecticut in the United States.

"I would propose incorporating cybersecurity in the computer science academic programs"

What were your first steps in the world of cybersecurity?

I discovered the cybersecurity world while I was working as a clinical engineer in the United States At that time various healthcare systems began funding multimillion dollar programs in order to reduce cybersecurity risk of medical devices in the hospitals. I had the opportunity to lead various initiatives in one of these programs, such as the development of the cybersecurity risk model and the strategy for medical device cybersecurity hardening. So I took my first steps in the field of medical device cybersecurity in the healthcare systems, the consumers of medical devices. Later I decided to apply my knowledge of medical devices' development by joining a medical device manufacturer.

What are the stages of Medical Devices manufacturing?

1. Concept and Design: This stage involves identifying the need for a new medical device and defining its intended use. The concept is then refined into a detailed design that takes into account regulatory requirements, safety considerations, and manufacturing feasibility.
2. Prototyping: Prototypes of the device are created with the purpose of testing the device's functionality and performance, as well as identifying any design flaws that need to be addressed.
3. Testing and Validation: The refined prototype undergoes extensive testing and validation to ensure that it meets the necessary safety and performance standards.
4. Regulatory Approval: In the USA, before a medical device can be sold or marketed, it must receive regulatory approval from the FDA.
This involves submitting extensive documentation and data to demonstrate the safety and efficacy of the device.
5. Manufacturing and Quality Control: During the manufacturing process, quality control measures are put in place to ensure that each device meets the necessary quality standards.
6. Packaging and Distribution: Manufactured

The Galaxy System™ (all-in-one integrated solution for navigated bronchoscopy) is one of the devices produced by Noah Medical

In what stage Cybersecurity is involved?

Cybersecurity is involved in all stages. During the design and development stage, medical device manufacturers conduct a cybersecurity risk assessment to identify vulnerabilities and implement risk mitigation strategies. During the testing and validation stage, medical device manufacturers conduct cybersecurity testing to ensure that the device is resistant to hacking, data breaches, and other cybersecurity threats. This is usually done with penetration testing. During the regulatory approval stage, the FDA reviews cybersecurity related documentation such as risk assessment, cybersecurity testing reports, and evidence of compliance with the cybersecurity standards. During the Manufacturing and Quality Control phase, manufacturers ensure that the process is secure and protected against cyber threats. During this stage, manufacturers also ensure that the device meets applicable cybersecurity quality standards.

What are the main vulnerabilities of medical devices?

Common vulnerabilities found in medical devices are: use of legacy operating systems that can't be upgraded or patched, insufficient authentication and access controls, and use of default and hardcoded passwords that can't be changed.

Are there any known cases of medical devices being hacked?

Yes, hackers target medical devices due to the protected health information (PHI) that is very valuable on the black market. Recently there have been many cases of ransomware attacks on medical devices.

What is the proper procedure of eliminating the discovered vulnerability?

The first step is to evaluate the risk associated with the vulnerability, because the level of risk will determine the next steps. If the risk is sufficiently low (acceptable), then the manufacturer may send a notice to the device owners explaining that the vulnerability has been discovered and stating its potential risk. The manufacturer may also provide some guidance on actions that the device owners may take to mitigate this risk. They aren't required to provide a patch. But if the risk is high (unacceptable), device manufacturers must not only communicate this to the customer, but also develop a patch within a certain timeframe, typically 90 days since the discovery of the vulnerability.

How does day-to-day look like in your work?

In my day-to-day I work closely with the development team (software developers, system engineers, etc.) to identify medical device's vulnerabilities, assess their risk, and develop the product requirements to implement risk mitigation strategies. I also maintain documentation related to the device's cybersecurity design. Also in my day-to-day I'm developing the medical device cybersecurity program from the ground-up, so I am creating policies and procedures aligned with the current regulatory requirements and best practices.

Please think on the big scale: if you were in charge of, say, all the MedDev cybersecurity field, what improvements would you propose?

I would propose:
- stronger regulatory requirements for medical device cybersecurity, and
- incorporating cybersecurity in the curriculum of computer science academic programs.

What are the steps that, in your opinion, should have been taken, but still haven't.

The two improvements mentioned above plus hospitals should include cybersecurity requirements in the RFP (Request for Proposal) in their medical devices' purchase process

What does the future hold for this field?

Medical device cybersecurity is a growing field. With increasing awareness and stronger regulations, more and more medical devices will be manufactured with cybersecurity functionalities.

Mariana Hu
Product Security Lead
Noah Medical