Connected Asset Risk Management in Healthcare

Establishing best practices on a Connected Asset Risk Management Program and understanding its key elements is fundamental in healthcare security.

By: Will Long, MIS, CHISL, CISSP, CPHIMS
Chief Security Officer, First Health Advisory

The Internet of Medical Things (IoMT) device security in the health delivery setting has been a well-known blind spot for organizations that want to reduce risk and develop efficient approaches to managing these ubiquitous assets better. The proliferation of these devices has gone far beyond the confines of the campus, further adding to the difficulty of identifying and protecting them, the patients, and operations reliant upon them. Establishing the right technology, expertise, and programmatic vision for a comprehensive medical and IoT device risk program was an idea that had to go beyond compliance, structural frameworks, and traditional cybersecurity controls. Instead, the effort requires a novel, yet repeatable solution able to be accomplished with a modest budget across various provider models.

First Health Advisory (FHA) has collaborated with customers in this vision, bringing together multiple organizational stakeholders, vendor technologies, a variety of subject matter expertise, and support from the highest levels of leadership. This unique business arrangement has cultivated both subjective and objective progress, evident through enterprise risk reduction, workflow efficiencies, and utilization insights never considered in the past.

For decades, IT assets have had well-defined processes for device onboarding, management, and security. In today's modern healthcare environments, this increasing number of connected medical and IoT devices resembles IT assets yet have characteristics that complicate the application of controls and accountability of risk mitigation. As every health care systems usage of medical and IoT devices has facilitated the transformation of healthcare delivery, the influence such devices is having on operational efficiency and patient safety warranted an increase in time-intensive, manual activities combined with hard to find, specialized medical device, integration, and network expertise.

Collaboration Approach

In planning for this multi-disciplinary, technology-intensive, strategic services endeavor, FHA recognizes that these will not be traditional vendor engagements. Well-orchestrated collaboration is a minimum measure of success in developing this program that involves regulatory expertise, manufacturer knowledge, security/network competence, clinical engineering savvy, and a host of business imperatives referenced in the challenge statement. Beyond the technological and business considerations, the collaboration between individuals and departments with vastly different roles in the enterprise proved to be the most impactful of variables. This "operational integration" is unique in aligning our customers executive governance, enterprise risk, and budget

planning with the technical and clinical processes to facilitate a program that unifies a multitude of entities.

When we use this combination of organizational and technological integration, dedicated to IT, security, and continuity of operations throughout the healthcare system, blends an array of subject matter expertise, technology, and process insight in developing a successful road map, framework calibration, and enterprise business goal alignment for protecting a distributed and diverse inventory of devices. First assists our customer in defining a strategy that will drive this novel approach in the lifecycle management of the medical and IoT devices. Deploying new device discovery technology and the right mix of talent to promote integrity, availability, and confidentiality of these devices is a challenge few organizations have tackled comprehensively.

This explicit approach allows our customer to engage one partner to assist in addressing the tactical challenges while advising with strategic and adaptive planning. FHA applies concentrated subject matter expertise to bring immediate impact to our customer while building a foundation for a long-term, comprehensive risk management program. The initial scope focuses on visibility (an accurate inventory) and vulnerability technology selection, deployment, data enrichment, and platform tuning. The combined team leverages device visibility and vulnerability data to validate discovery, improve fidelity, classify device attributes, formalize risk assessment process, and enable executive engagement. As the team begins to operationalize enterprise resilience in support of improved workflow, operating procedures, and objective evaluation reporting, articulating this approach to a broader customer cohort team will continues through ongoing education, awareness, and methodology for a proactive asset management program.

The approach is repeatable and scalable as recognized practices are emerging in this collaboration effort. The will of the organization to allocate time and resources, from IT and Security to HTM/Biomed and Supply Chain is essential to building consensus, shared responsibility, and an understanding the medical device and IoT risk impacts the enterprise. In addition, the will of executive leadership to align these key stakeholders, especially if they do not report up through the same structure, is a major success factor in reinforcing accountability and responsibility while additional collaborators are consulted and informed.

Strategies Utilized

The purpose of the program is to solve an existing problem but also to keep an eye on future growth; accordingly, it is necessary to develop and implement strategies for this unique venture. Ultimately, the team begins by gaining more accurate visibility (inventory) into the world of non-traditional Information Technology assets connected throughout the organizational network system. Through the implementation of a tool specifically created to identify connected medical and IoT devices, the healthcare system resources can gain high-definition visibility into devices that were previously only identified by Internet Protocol (IP) and Media Access Control (MAC) addresses.

With the ability to now recognize assets down to device type, manufacturer, operating system, and many other parameters, the team profiles the devices into categories for monitoring and action appropriately. Based on profiles and device types, the implemented system provides alerts on device vulnerabilities that were previously invisible to standard IT security systems.

Upon categorization and identification of vulnerabilities, risk analyses are performed on impacted assets within the inventory, and plans are produced for the remediation or mitigation of the security gaps identified by the system.

With the introduction of a new security system into an otherwise standard IT security architecture, it is essential to fully integrate the technology into the overall network planning architecture. Technical integrations are performed to enrich the data already gathered by the new platform. Additionally, policies, procedures, and workflows are reviewed for modification, and needed documentation is created and tailored to fully assimilate the IoT security program into the overall risk management framework.

A clear understanding of Roles, Accountability, those to be consulted, and those to be Informed (RACI) is foundational and completed to direct the program constituents. Downstream and upstream activities, committees, event response, and future programmatic decision flow will use the RACI chart as a touchstone for guidance and strategic visioning.

Through full visibility and operationalization of the technology, processes, and people, our customers now have a governance structure that facilitates long-term planning and budgeting decisions. Information gathered through the program informs security planning and requirements and aids purchasing decisions for complicated and expensive medical devices. Furthermore, this solution facilitates scalability for strategic organizational initiatives, as well as visibility to smart room and future IoT technologies that are being incorporated into new facilities across multiple campuses.

Outcomes Achieved

FHA collaborates with its customer in this vision, bringing together multiple organizational stakeholders, vendor technologies, broad subject matter expertise and support from the highest levels of leadership. The unique business arrangement has cultivated both subjective and objective progress, evident through enterprise risk reduction, workflow efficiencies, and utilization insights never considered in the past. Through this collaboration and strategic planning, our customers can gain full visibility into assets, along with status, locations, security concerns, and utilization statistics. This effort saves significant hours of manual location, inventory, and control of IoT devices for our customers.

Accordingly, this previously unseen aspect of organizational security is brought to the forefront and fully assimilated into the overall corporate risk management framework ensuring continuous identification and profiling of new devices added to the network and monitoring of existing assets for security and operational utilization purposes. The basis of great security programs is policies, processes, and procedures to ensure that security responses to violations are enforceable. The addition of medical device and IoT connected asset language and workflows into the overall operations adds another segment to overall governance.

Many organizations are missing the single pane of glass view into the utilization of connected assets, such as CT scanners, X-Ray machines, MRIs, and similar devices that could cost multiple millions of dollars. If utilization can prevent the unnecessary acquisition of an MRI, the savings would be tremendous. Through the implementation of this tool, our customers can see the utilization metrics for these devices and appropriately determine when new devices are required, or when the needs can be met with creative scheduling of patients to less busy machines.

Upon implementing the technology, our customers can confirm the existence critical and high vulnerabilities resulting from sometimes thousands of verified security alerts. Using the information provided and the workflows established throughout the project, our customers can close many of the warnings and continues to move through longer-term plans for remediation and mitigation of connected asset vulnerabilities. First looks for ways to mature the programs through more advanced integration of the data and optimization of workflows with the goal of unveiling previously unforeseen efficiencies, ultimately lowering enterprise risk while developing cost saving processes and structure.

Recommendations for Success

FHA continues to collaborate with customers to address this challenge from a programmatic perspective has been a foundational element of success that provides continuous innovation, process optimization, flexibility through regulatory changes, and adoption technological advancements not available at the onset of the initiatives. As other's consider developing or maturing a program around Medical and IoT devices, consider identifying connected asset vulnerability management platform vendors and measure their capabilities against organizational requirements. Once the best fit is selected, follow a controlled programmatic structure for the implementation and operationalization of the platform and associated data. Consider not only the technology but ensure the processes and people elements are integrated into the overall organizational framework. Follow the processes outlined for implementing a risk management framework, such as the one developed by HITRUST or National Institute of Standards and Technology (NIST) and consider the Association for the Advancement of Medical Instrumentation's (AAMI) Risk Management standards.

Institute a cross-functional cybersecurity committee with decision-making power for all connected assets regardless of reporting structure. Consider a reorganization of reporting structure for Healthcare Technology Management (HTM) and Clinical Engineering to reflect a single executive, such as the CIO with overall responsibility for all assets connected to the network, to include traditional and non-traditional devices.