Booz | Allen | Hamilton

Commercial Solutions

MEDICAL DEVICE CYBER SECURITY & DATA PROTECTION

What Every Device Manufacturer Needs to Know

Cyber in the C-Suite: Medical Devices

As medical devices become more connected, industry professionals have begun to realize the critical ties between cyber, privacy, and medical device security. These devices, though beneficial, offer inroads into the most intimate aspects of both businesses and individuals. But identifying these ties is just the beginning. Medical device companies must prioritize cyber security and data protection to earn consumer trust and confidence, prevent damage to brands and reputations, and remain competitive in the market.

The Time is Now

Medical devices represent a core element of the increasingly personalized Internet of Things. As medical devices' local and global networks grow, so do new opportunities for revenue growth and customer relationships. Yet, as these networks and opportunities expand, so do vulnerabilities to cyber attack. These attacks have the potential to cause data loss or manipulation, privacy breaches, manipulation of device functions, and entry into connecting networks—resulting in anything from significant financial losses to patient harm. There is an urgent need for medical device manufacturers to secure their products, and industry leaders are beginning to see the scale and scope of the challenge.

Greater Than the Sum of Its Parts

In today's connected business environment, cyber security requires teamwork across a company to identify possible vulnerabilities. A technical solution alone isn't enough to protect you or your customers. The cyber landscape encompasses a unique set of variables, with numerous inroads and unrelenting attackers. Back-end IT infrastructure, network providers, patients, and health care providers all offer points of exposure. The manufacturer's network, the user's device ecosystem, and—for some devices—the provider's network are all targets.

Manufacturers must protect data residing on devices themselves or transmitted to the care provider as well as data that is uploaded by the manufacturer for further analysis or product improvement. Furthermore, securing a device and organization against outside attackers may still overlook vulnerability to malicious insider activity. Leaders of medical device manufacturers must build diverse, yet cohesive, groups dedicated to cyber security, increasing visibility into the vulnerabilities as well as ways to address them.

This isn't just about the device itself; it is about the ecosystem that interacts with and enables your device to provide value to the customer. Elements central to securing your device materialize from every intersection—its components, product design, patients, and each networked connection point. You need an integrated plan to prepare and respond.

Cyber attackers seek weakness.

Weaknesses in a device's network might be caused by an innocent mistake or a lack of awareness, but regardless, those with malicious intent will take advantage of even the tiniest hole. Consider the following access points, which many times go unprotected or unnoticed:

- A device's software updating process
- Data sharing protocols
- Bluetooth connectivity
- Patient support program systems
- Hospital network connections
- Insider access and identity management

Siloed efforts only close a few of the doors to risk, which may leave most of the device's ecosystem unprotected, exposing it to harm.

First Steps to Get Ahead on Cyber Security

There are four organizational actions that leaders can take to immediately address medical device cyber security and data protection. These changes lay the foundation for creating a more trustworthy cyber security program as part of your integrated business.

1. Identify and empower a medical device cyber security leader.
Your organization needs a leader to champion device cyber security. This leader should have access to executive leadership and resources to protect your devices in a way that ensures device integrity, patient safety, and privacy. As the face of medical device cyber security, your leader is accountable for cyber security from the boardroom to the factory floor to the doctor's office to the end user.

2. Build a cross-functional team to support this leader.
Every leader needs a team, and medical device cyber security requires one of the best in your organization. The team's job is to build cyber security into the product ecosystem and business processes. Start by deploying a security-centered approach that sits at the intersection of information technology and product development. This team needs to interface across the enterprise, integrating with or embedding into teams that deal with safety, reliability, privacy, data governance, compliance, risk management, supply chain, and customer service.

3. Manage risk across your ecosystem.
You need to look inward *and* outward before moving forward. Look inward to understand everything that touches the medical device: Plot your complete attack surface so you know what you need to protect, including privacy risks throughout the lifecycle of personal data flowing into and out of the medical device. Follow the data flow, from initial collection to deletion, to ensure it is managed and secured in line with privacy promises and legal requirements. Then, look outward, including to third parties with whom data are shared, to ensure commensurate protections. Build a network of sensors that captures early indicators of vulnerabilities, attack methods, and malicious actors. Once you know the ecosystem and the threats, move forward. Use the data you have in a privacy-protective way to determine the best approach to monitor and mitigate new and ongoing risk.

4. Make it part of a bigger cultural change.
Even with the smartest team and the most advanced capabilities, the security of your devices may fail without full support from the organization. After all, these efforts are not just about compliance or securing parts: this is about maturing your business—enabling connected products and services, making processes more efficient, building industry-leading analytical capabilities, integrating privacy protections, and providing new value to your customers. Translate this vision into a plan of action and build momentum with tangible results.

Organizations with the creativity and flexibility to tackle medical device cyber security in a way that integrates data privacy protections will be better positioned to keep pace with the speed of innovation, competitive pressures, and game-changing revenue opportunities in the connected era. These will be the companies that maintain customer trust, and remain one step ahead.

Now is the time to act.

To learn how Booz Allen Hamilton can help your business thrive, contact:

John Khantzian
Tel +1 267-330-7874
khantzian_john@bah.com

Heath Stockton
Tel +1 571-420-0187
stockton_heath@bah.com

www.boozallen.com/commercial

Booz | Allen | Hamilton