MITIGATING CYBERSECURITY RISK

CRITICAL STEPS FOR MEDICAL DEVICE MAKERS
Medical devices are becoming ever more connected, with health system networks and the Internet, with data repositories and analytics engines, and with other devices. While this “connectedness” can add tremendously to their clinical value, it also makes them more vulnerable to cyber threats.

This stark reality is not limited to healthcare, of course. According to the World Economic Forum Global Risks report published in January 2016, 90% of companies worldwide recognize they are not sufficiently prepared to protect themselves against cyber attacks. This perception has been reinforced by numerous high-profile security breaches at major corporate and retail organizations that have compromised the personal data of millions of consumers.
In the healthcare arena, there’s a critical difference as cyber crimes could potentially threaten not just the integrity of personal data, but patient safety as well.

In July of 2015, the FDA issued a Safety Communication alerting health systems to the potential cybersecurity vulnerabilities of a particular infusion pump. Citing a risk of unauthorized system access, the FDA communication urged healthcare organizations to disconnect the device from their networks and transition to alternative systems.²

In 2014, the FDA published guidance focused on incorporating cybersecurity into medical device product development.³ This guidance, coupled with recent and pending legislation, is increasing the manufacturer’s liability and enhancing penalties associated with cybersecurity breaches. This has changed the landscape of healthcare product development accountability. An organization’s failure to perform adequate due diligence can result in higher penalties in the event of a breach. Beyond the issue of the loss of highly sensitive data, the FDA’s escalated interest is predicated on the fact that these types of breaches create the possibility of serious patient injury, or even fatality.

Healthcare providers are also focusing accountability on device makers. Many are now asking device suppliers to execute legal business associated agreements (BAA) which share or even transfer the liability of a data breach to the supplier, if the device is found to be culpable. This highlights the potential for business risk for device manufacturers, ranging from financial losses to business disruption to irreparable damage to brand equity on top of the potential for legal and regulatory action resulting from negligence to proactively address the risk of cyber threats.

$445 BILLION
ANNUAL COST OF CYBER CRIME TO GLOBAL ECONOMY¹
Compounding the potential risk is the mindset many healthcare device manufacturers have about cybersecurity.

The conventional approach focuses on protecting a company’s network and technical infrastructure. In other words: “cybersecurity is IT’s problem.” That approach is no longer valid.

Medtech companies need to think differently about security as it relates to their products, their business risk, and their customers and patients. With today’s complex, interconnected medical devices, cybersecurity cannot be an afterthought; it must be integral to the product.

Security must be a central concern starting right from the very beginning of system architecture and continuing through the entire product development lifecycle.

Security should be a central focus not just for engineering, but for stakeholders at all levels across the company, from the board room and risk management to R&D, legal and public affairs.

Taking on cybersecurity can be intimidating for device companies for which security is not a core competency.

However, effective cybersecurity can be achieved by companies that are willing to take the necessary steps to reduce risk factors and ensure compliance. Conducting a thorough risk assessment, properly developing a structured plan, and then closely following that plan are all critical steps for mitigating organizational exposure through a successful cybersecurity implementation.
Since there is no proven method to eliminate all risk, defining the acceptable risk level is necessary for determining effective security controls. Without a definition of acceptability, investments in security are not guided and can result in investments without a return.

To determine this new definition of “done,” the product’s risks must be itemized by considering the following questions:

→ What and where are the vulnerabilities?
→ How would someone exploit these vulnerabilities?
→ What degree of harm could occur if an entry point was unexpectedly or even unknowingly exploited?

By quantifying the impact of these potential harms, companies can identify critical vulnerabilities. An organization may have cybersecurity controls already in place, and these existing controls can be enhanced and aligned to directly protect against the identified vulnerabilities. This is critical for mitigating safety risks and for controlling the associated adverse legal and business risks.
It is crucial to evaluate risks and appropriately update mitigation measures throughout the product development lifecycle.

This process will likely have an impact on several artifacts in an organization’s quality management system (QMS), but it also involves a significant educational effort within the workforce. Product development teams must understand what to look for and be well versed in secure development strategies. This may seem a daunting challenge for many organizations. However, encryption, digital signatures, and other technical controls have an abundance of prior art that can be used to support the process.

In order to achieve meaningful progress towards ensuring cybersecurity, organizations must fill the identified gaps. Depending on the complexity of the product’s architecture, this may not be a trivial task. The initial risk assessment is an extremely valuable input to this activity. Based on the acceptable risk level, product developers are able to design products that protect not only patients, but medtech companies as well. Security controls can be assessed so those that do not reduce identified risks will not be added, thus focusing development investments on activities that would yield a return.
In today’s hyper-connected world, security attacks are a reality.
As healthcare products become more connected and as cyber attacks grow in frequency and ingenuity, the risk posed by cyber threats is increasing significantly. Much is at stake, from revenue loss to product recalls to patient safety and brand tarnishment; or worse, the risk of a regulatory body shutting down business operations. And the greatest risk of all to medical technology companies may be the “unknown risks” cyber vulnerabilities that are overlooked due to insufficient forethought or expertise.

These risks exist not just with new products in development, but also with existing products. The FDA issued draft guidance recommending that manufacturers “monitor, identify and address cybersecurity vulnerabilities and exploits as part of their postmarket management of medical devices.” This is in addition to the FDA’s premarket guidance for management of cybersecurity in medical devices.

To effectively manage the cybersecurity risk, business leaders—from chief executives and risk management officers to legal and technology leaders—need to ask themselves some important questions:

→ Have we fully considered the potential security vulnerabilities within our products and designs?

→ Have we made cybersecurity risk management a priority at every stage in a product’s lifecycle from concept to end of life?

→ Do we have the requisite expertise and professional bandwidth to address potential vulnerabilities, both for new products and for those already in the marketplace?

→ Do we have the expertise to identify which cybersecurity investments will lead to the best ROI in terms of risk mitigation?

Answering “yes” to these critical questions requires that medical technology companies change their approach and make cybersecurity a central focus of their product development and support strategy. By creating a culture of security awareness that permeates the entire organization, augmenting in-house expertise when and where it is needed, companies will be well positioned to reduce cybersecurity risk and to earn customer trust, a major competitive advantage.
ABOUT THE AUTHOR

Tim Bosch is Vice President and Chief Architect for Medical & Life Sciences at Altran North America, and has served as lead consultant and system architect for numerous medical devices and healthcare informatic systems.

ABOUT ALTRAN

As a global leader in Engineering and R&D services (ER&D), Altran offers its clients a new way to innovate by developing the products and services of tomorrow. Altran works alongside its clients on every link in the value chain of their project, from conception to industrialization.

For over thirty years, the Group has provided its expertise to key players in the Aerospace, Automotive, Defense, Energy, Finance, Life Sciences, Railway, and Telecom sectors, among others. In 2017, the Altran group generated revenues of €2.282 billion. With a headcount of more than 33,000 employees, Altran is present in more than 20 countries.

SOURCES


MITIGATING CYBERSECURITY RISK

Critical Steps for Medical Device Makers