Effective strategies must protect medical devices

By Ken Zalevsky

Medical devices are a critical component of the global health care infrastructure, accounting for about $350 billion spent annually. The U.S. Department of Health and Human Services estimates that there are more than one billion patient encounters (visits to physician offices, hospital and outpatient emergency departments) annually in the United States alone, which all likely involve the use of medical devices. These devices include a wide range of products, from tongue depressors and bandages through life-sustaining products such as pacemakers, and more recently, associated software systems. Given the number of encounters and range of devices, medical device safety is of significant importance to the health care industry.

The Food and Drug Administration (FDA), an agency within the Department of Health and Human Services (HHS), is responsible for ensuring that medical devices sold in the United States are safe and effective. However, the increased complexity and connectivity of medical devices has made this task exponentially complex for both medical device manufacturers and the FDA. Recent legislation from the FDA has been aimed at guaranteeing the safety of medical devices, prior to making them available commercially, by requiring cybersecurity documentation as part of the pre-market approval process.

In August 2015, the FDA issued an alert, warning of security flaws identified in a commercially available infusion pump, which resulted in the removal of those pumps from the market. This unprecedented action by the FDA has given effective notice to medical device manufacturers that products must be secured and maintained over their entire life cycle, from deployment to retirement.

The challenge facing medical device manufacturers today is clear — reliably produce safe and secure medical devices, maintain the safety and security of those fielded devices and respond appropriately to continued changing regulations. Investment in products and services that support compliance is not optional. Medical device manufacturers, in order to remain viable, must adapt traditional processes and policies in addition to adopting new processes and policies.

Driving factors

Health care organizations, including medical device manufacturers, are being driven to adopt a cybersecurity strategy...

- To ensure patient safety.
- To respond to legislation.
- To remain competitive.
- To respond to customer inquiries.
- To maintain reputation.

Organizational cybersecurity strategy and risk profile

How should health care organizations respond to the challenge of cybersecurity? How do they go about putting an infrastructure in place, and what is the high-level plan? The first step is to quantify the actual risk in question. An assessment of potential organizational risk enables the proper framing of the problem. Every organization has a different risk profile and tolerance, so this necessary step will aid in actually scoping the problem and ensuring that the solution is an appropriate fit. The goal in this step is to get the organization to start thinking in terms of cybersecurity risk and to develop a target risk profile that is acceptable across the enterprise.

Risk framework

Adopting a risk framework can provide the organization with proven practices and processes and enables continued focus on the cybersecurity challenge. The National Institute of Standards and Technology (NIST) has developed a cybersecurity framework which integrates proven cybersecurity practices and provides assessment mechanisms that can be useful as organizations begin to take up the cybersecurity challenge. In addition, the continued evolution of the NIST framework means that organizations can mature their processes and infrastructure over time.

The business processes below, outlined in the framework core, define an evergreen infrastructure that can form the foundation of an effective cybersecurity program.

Identify

Develop the institutional understanding to manage cybersecurity risk. This is the scoping phase of the implementation project, and it is sometimes beneficial to narrow the initial focus and then expand as the organizational adoption process matures.

Protect

Develop and implement appropriate safeguards. This involves assessing the assets identified in the first step for vulnerabilities and documenting mitigation controls. The three main categories of safeguards are administrative, technical and physical and utilizing this classification structure can help ensure thorough coverage.

Detect

Develop and implement appropriate activities to detect the occurrence of a cybersecurity event. Put controls in place to enable reviews of critical processes in order to enable detection.

Respond

Develop and implement appropriate processes and policies to enable a response to a cybersecurity event. For most organizations, the response details are outlined in an Incident Response Plan, discussed in more detail in the section below.

Recover

Organizations need a recovery plan which enables remediation of the breach such that the vulnerability that led to the breach in the first place has been resolved. Recovering to the initial state of the organization could replicate the vulnerability, leaving the organization exposed to a similarly executed breach in the future.

Develop and test an incident response plan

No matter what policies, processes or control mechanisms are in place, no organization can prevent a breach from occurring 100 percent of the time. Studies have shown that having an incident response plan can greatly reduce the cost of a breach, if one should occur. The Ponemon Research Institute in 2014 released the Cost of Data Breach Study: United States. In this study, Ponemon research showed that organizations with incident response plans can decrease the cost of a breach by about $17 per record. This could be significant, depending on the size of the breach. In addition, having an incident response plan provides organizations a script for testing their responsiveness. By developing a plan and then simulating a breach event, an organization can exercise the incident response plan and detect and correct any gaps. It has been shown that, analogous to disaster recovery plans, organizations with incident response plans can more effectively respond to breach incidents and minimize long-term impacts.

Develop a current risk profile and a target risk profile

To plot the path to a goal, it is important to know the starting position. The organization should create a current risk profile in order to detail the risk across defined categories and subcategories. This can be done through organizational assessment and has the additional benefit of requiring process documentation to be reviewed and accurate.

Once the current risk profile is defined, the organization will then create the target profile, which represents the desired acceptable risk. In other words, in the absence of being able to mitigate 100 percent of the risk, organizations must determine a comfort level for acceptable risk.

With both the current and target risk profiles defined, the organization can then run a gap analysis, which will highlight areas for focus and should include the development of mitigating controls.

With an evergreen infrastructure in place, organizations can then begin to monitor the ever-changing cybersecurity landscape and should have the flexibility to respond, and expand to accommodate.

The health care cybersecurity challenge

In their premarket guidance released in October, 2014, the FDA has stated, “FDA will not typically need to review or approve software changes made solely to strengthen cybersecurity.” This means that medical device manufacturers have the freedom to patch and update fielded products for cybersecurity vulnerabilities without FDA review. This is good news, however, it solves only a portion of this complex problem. The amount of effort involved for the medical device manufacturer to monitor for critical security vulnerabilities, assess the potential impact of those vulnerabilities on fielded product, and ultimately package and deploy those patched systems is enormous. And, more importantly, most medical device manufacturers do not already have these processes in place, so would need to begin with building the capabilities before even being able to address the issue.

In addition to the implementation of entirely new processes, requiring potentially new skill sets, medical device manufacturers are challenged by the continuous discovery of vulnerabilities that must be addressed. Unlike other industries wrangling with the same cybersecurity issues, in health care, patient safety is critically important. So simply applying the latest patches without thoroughly understanding the potential impact of those patches on other parts of the system, is not an option.

Typically, the existing testing infrastructure can be leveraged to verify and validate the safety of a device after a cybersecurity vulnerability has been patched. However, it is important to thoroughly understand the potential impact of a patch on the system by identifying all of the affected components. In other words, when patching for a specific vulnerability, tests must be performed to determine if there is an impact elsewhere in the system, potentially on a component that directly interacts with the portion of the system that was patched. Again, most organizations are adept at testing, however, the challenge remains that cybersecurity vulnerabilities are evolving at a pace that will require the modification of current processes in order to meet this tremendous demand. Through continuous monitoring of cybersecurity vulnerabilities and the evolving threat landscape, assessment and prioritization of potential threats and diligent application and thorough testing of patched systems, organizations can begin to respond to the health care cybersecurity challenge.

Conclusion

Cybersecurity in health care is of primary concern to patients, providers and regulatory agencies. Health care breaches are happening every day. Medical devices have been hacked, patient records are being stolen and health care organizations are facing continuous threats. While health care organizations can’t prevent a breach from occurring, there are strategies and tactics to help mitigate the potential damage of a breach. Adopting a cybersecurity risk framework enables organizations to leverage proven processes and maintain an evergreen cybersecurity risk-mitigation strategy.

Ken Zalevsky is a certified cybersecurity leader from Carnegie Mellon University, and a director in the Informatics Software R&D Group at Bayer. The opinions expressed in this article are entirely those of the author and not of his employer.

Share this story: dotmed.com/news/28778