Medical Devices and Cybercrime: Are Your Patients at Risk?

POWERFUL INSIGHTS

Issue

Over the past few years, there has been an increase in the number of medical devices (from infusion pumps to CT scanners) that are connected to networks, either wirelessly or through systems that support them. During the same period, the number of cyberattacks against healthcare organizations has also increased. What happens when cyberattackers, maliciously or as a byproduct of a separate attack, impact patient safety and privacy? Healthcare organizations can’t wait to find out. They need to act now to evaluate this risk and implement appropriate countermeasures, for the following reasons:

• Medical devices are increasingly connected to networks to enable additional patient care options but often without appropriate security controls in place.

• Significant device vulnerabilities, including hard-coded credentials and insecure communication protocols, can result in protected health information (PHI) exposure and impact patient safety.

• The FDA, FBI and DHS have released multiple advisories on medical device security risks and the FDA has published formal guidance on addressing the cybersecurity of medical devices.

• The Office of Inspector General (OIG) at the Department of Health and Human Services announced earlier this year that it is including medical device security in its audits.

Because attacks and security incidents are now seen as common occurrences rather than exceptions, being able to demonstrate due care is critical for healthcare organizations. Leaders that haven’t prepared and responded to these emerging threats and federal agency advisories will find it difficult to explain their choice when a cyberattack on a medical device causes — intentionally or unintentionally — an adverse patient safety event.

Challenges and Opportunities

Medical devices have not traditionally received the same amount of security scrutiny in healthcare organizations as other technologies. Historically, such devices have been viewed as “black boxes” rather than computers with software, which is what many of them have become. The biomedical teams that manage such devices often don’t see information security policies applied to computers as equally applicable to medical devices.

In addition, doctors provided with the latest technological advances that allow them to configure implanted devices or monitor patients remotely are not given enough information to ensure that this advanced technology will not result in an unintended violation of their oath to “do no harm.”

Finally, many healthcare organizations have historically been focused on meeting HIPAA or Meaningful Use requirements, and have not spent sufficient time reviewing the risk posed by connected medical devices. As a result, many have not yet implemented appropriate countermeasures to reduce the risk of a successful attack.

While these are significant historical challenges, by addressing them promptly, organizations will demonstrate the due care patients expect and regulators require and ensure their doctors are prepared to provide care in an increasingly connected medical environment without violating the first rule of medicine.

Our Point of View

A small amount of preparation now can have a significant impact on ensuring patient safety and privacy. We believe that:

• Information Security (IS) and biomedical teams need to initiate productive risk discussions urgently, and may require outside expertise to bridge the knowledge gap.
• IS, Legal, Compliance, and Procurement departments need to understand what process improvements need to be in place to limit the organization’s liability resulting from security vulnerabilities of medical devices.

• Finally, healthcare organizations need to view medical device security from a holistic life cycle perspective (procurement, implementation, maintenance and decommissioning) to ensure a proactive instead of reactive approach to potential cyberattacks.

Business leaders with the appropriate risk mindset related to patient safety will address these issues now. Doing so not only will help protect their organizations from future negative repercussions, but also will be consistent with their organizations’ mission to put patient care first.

PROVEN DELIVERY

How We Help Companies Succeed

Protiviti helps healthcare organizations navigate emerging risks such as those posed by connected medical devices. We offer a unique blend of technical and healthcare industry talent and can assist organizations in making informed decisions on how best to limit their liability and ensure patient safety.

Our team of healthcare information security experts includes professionals with significant industry expertise as well as hands-on researchers and thought leaders who consult regularly with government agencies and device manufacturers on medical device security. This ensures that our clients receive first-hand guidance from those with the most current information.

By partnering with Protiviti, management can demonstrate a direct impact on its organization’s mission and values surrounding patient safety and quality clinical care. We work by educating key stakeholders on the potential dangers of connected medical devices and by helping build an effective program and framework to mitigate the risk.

Services we offer as part of our medical device security practice include:

• Medical device risk assessments
• Biomed security vulnerability assessments
• Penetration testing for key medical devices
• Medical device procurement process consulting
• Biomed incident response readiness assessments
• Medical device security program remediation support
• Manufacturer vulnerability remediation liaison assistance

Contacts

Jeff Sanchez (Los Angeles)  
+1.213.327.1433  
jeffrey.sanchez@protiviti.com

Susan Haseley (Dallas)  
+1.469.374.2435  
susan.haseley@protiviti.com

Scott Laliberte (Philadelphia)  
+1.267.256.8825  
scott.laliberte@protiviti.com

Rocco Grillo (New York)  
+1.212.603.8381  
rocco.grillo@protiviti.com

Cal Slemp (New York)  
+1.203.905.2926  
cal.slemp@protiviti.com

David Taylor (Orlando)  
+1.407.849.3916  
david.j.taylor@protiviti.com

About Protiviti

Protiviti (www.protiviti.com) is a global consulting firm that helps companies solve problems in finance, technology, operations, governance, risk and internal audit, and has served more than 40 percent of FORTUNE 1000® and FORTUNE Global 500® companies. Protiviti and its independently owned Member Firms serve clients through a network of more than 70 locations in over 20 countries. The firm also works with smaller, growing companies, including those looking to go public, as well as with government agencies.

Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.