CYBERSECURITY
OF MEDICAL DEVICES AND UL 2900
The healthcare industry is projected to spend an estimated $1 billion (USD) on cybersecurity in 2016 as hospitals and healthcare providers become a major target for hackers and other cybercriminals\(^1\). That’s because medical devices and systems are increasingly interconnected with other devices and systems to facilitate the recording of vital data and the updating of health medical records, and to improve overall coordination of patient care. Vulnerabilities in technologies required to support interconnectivity, including hardware and software, can expose many medical devices to deliberate cyber threats.

Unfortunately, the consequences of successful cyberattacks against medical devices not only threatens the security of confidential patient medical records but can also endanger the health and safety of patients and healthcare workers alike. And the cost of addressing data breaches in the healthcare industry can be more than $360 per record, the highest per record cost of the top industries directly impacted by cybercrime\(^2\). As a result, the security of medical devices and systems against cyberattacks is an essential requirement for medical device manufacturers.

This UL white paper discusses cybersecurity threats to which interconnected medical devices may be vulnerable, and how the application of the requirements of the UL 2900 series of standards can help address those threats. The paper begins with an overview of the scope and impact of global cybersecurity issues and government efforts to address the problem, before focusing on specific cybersecurity threats to medical devices. The white paper then reviews aspects of current standards that address these threats before presenting the risk management approach detailed in UL 2900, Standard for Software Cybersecurity for Network-Connectable Devices. The paper concludes with a discussion of UL’s Cybersecurity Assurance Program (CAP) for interconnected devices and the program’s potential benefits to manufacturers of healthcare products, including medical devices.
Cybersecurity Threats in Healthcare

Virtually unknown just a decade ago, attacks on information technology (IT) infrastructure and systems have rapidly become a major risk to governments, organizations and enterprises around the world. The international accounting and advisory firm PwC places the number of reported IT security incidents at nearly 43 million in 2014, a 48 percent increase over 2013, compromising approximately one billion data records. The cost to the global economy from cybercrime is currently estimated at more than $400 billion annually, and is projected to increase to over $2 trillion by the year 2019.

As advances in technology and information systems transform the modern landscape for patient care, the healthcare industry is especially vulnerable to cyberattacks. The market for interconnected healthcare systems and so-called smart medical devices is expected to reach nearly $58 billion annually by 2023. However, most of these advanced medical devices incorporate embedded computer systems and wireless technologies that make them vulnerable to cybersecurity threats.

According to the U.S. Food and Drug Administration (FDA), specific vulnerabilities that can directly impact healthcare systems and medical devices include:

- Network connected/configured medical devices that have been infected or disabled by malware;
- Malware on hospital computers, smartphones and tablets that targets wireless mobile devices to access patient data, monitoring systems or implanted medical devices;
- Failure to update security software for medical devices and networks;
- Security vulnerabilities in off-the-shelf software; and
- Uncontrolled distribution of passwords intended for privileged device access.

These and other vulnerabilities have resulted in a significant and growing number of cyberattacks against healthcare systems. Statistics reported by the U.S. Department of Health and Human Services (HHS) under the federal Health Information Technology for Economic and Clinical Health (HITECH) Act reveal that more than 1400 breaches of protected health information involving 500 or more patient records have been reported since 2009, affecting more than 150 million patients. More recently, a 2016 survey of healthcare executives found that reported attacks on healthcare operational systems and embedded medical devices increased fourfold from 2014 to 2015, while attacks on consumer medical technologies nearly doubled.
Cyberattacks against interconnected healthcare systems and devices are likely to continue to escalate in part because of the value of healthcare records. Stolen health files and records reportedly sell for 10 to 20 times the price obtained for stolen credit card information, making them much more attractive to hackers and cyber thieves. As a result, ransomware attacks on healthcare are also on the rise. For example, as part of a series of attacks on California hospitals in early 2016, hackers demanded $3.6 million in ransom to unlock the medical records of one Los Angeles-area hospital (the hospital ultimately paid about $17,000 to end the threat).

Aside from comprising confidential patient data, some experts believe that future ransomware attacks will target life-critical medical devices such as infusion pumps and pacemakers. In one frightening portent of this possibility, the U.S. FDA released a safety communication in 2013 alerting healthcare providers to end the use of a computerized pump infusion system due to cybersecurity vulnerabilities. The FDA warned that the infusion system could be accessed remotely through the hospital’s network, potentially allowing unauthorized users to control the device or change the dosages being delivered by the pump.

Cybersecurity and the Critical Infrastructure

As part of the overall effort to address cybersecurity threats, the healthcare industry is generally considered part of the so-called critical infrastructure, which can be defined as “IT assets, networks, services and installations that, if disrupted or destroyed, would have a serious impact on the health, security or economic well-being of citizens and the efficient functioning of a country’s government.” In addition to healthcare, those industries most often designated as part of the critical infrastructure include defense, energy generation and distribution, water systems, transportation and shipping, financial services and public safety.

Because of their overall importance, entities that work within designated critical infrastructure industries are expected to comply with government-mandated cybersecurity requirements and practices. In the European Union (EU), for example, the European Programme for Critical Infrastructure Protection (EPCIP) identifies critical infrastructure entities within the transportation and energy industries and details specific requirements applicable to entities within those industries. These requirements include the development of an operator security plan that identifies important infrastructure assets, provides a detailed threat assessment based on asset vulnerability, and details countermeasures to combat cyber threats. Some countries, including Germany and the United Kingdom, have additional cybersecurity requirements applicable to critical infrastructure entities.

In the U.S., the protection of critical infrastructure against cyber threats is largely based on voluntary compliance with standards and practices. Issued in February 2013, Presidential Executive Order 13636 (Improving Critical Infrastructure Cybersecurity) called on the National Institute of Standards and Technology (NIST) to develop risk-based cybersecurity measures and practices that could be adopted by entities designated as part of the critical infrastructure. The resulting Cybersecurity Framework, published by NIST in 2014, encourages organizations to consider cybersecurity risks in the context of its overall risk management process, and provides structured guidance for reducing cyber threats based on existing standards, guidelines and practices.
FDA Guidance on Cybersecurity for Medical Devices

The FDA has published two separate guidance documents related to the issue of cyber-security in medical devices. The first guidance was published in 2014 and addresses the content of premarket submissions for the management of cybersecurity in medical devices. Specifically, this guidance identifies and addresses cybersecurity issues that medical device manufacturers should consider in the design and development of their products.

The guidance recommends that manufacturers follow a risk management approach that includes the following five elements:

- Identification of assets, threats and vulnerabilities
- Assessment of the impact of threats and vulnerabilities on device functionality and end users/patients
- Assessment of the likelihood of a threat and of a vulnerability being exploited
- Determination of risk levels and suitable mitigation strategies
- Assessment of residual risk and risk acceptance criteria.

The FDA’s cybersecurity premarket submission guidance also provides specific recommendations regarding documentation that should be included as part of a manufacturer’s premarket submission to the Agency. Recommended documentation includes a list of all cybersecurity risks that were considered in the design of a given device and a corresponding list of controls that were implemented to address those risks. In addition, manufacturers are expected to supply with their premarket submission user instructions that include recommended cybersecurity controls applicable to a given device’s intended use.

A separate draft guidance addressing the post-market management of cybersecurity in medical devices was issued by the FDA in January 2016. The draft guidance acknowledges that even the most diligent efforts to address potential cybersecurity risks ahead of placing a medical device on the market cannot account for future vulnerabilities resulting from the introduction of new technologies. Therefore, the draft guidance recommends that device manufacturers monitor, identify and address cybersecurity vulnerabilities as a routine part of their post-market management and oversight of medical devices.
According to the draft guidance, specific elements of an effective post-market cybersecurity risk management program would include the following components:

- Monitoring cybersecurity information sources for identification and detection of cybersecurity, vulnerabilities and risk;
- Understanding, assessing and detecting the presence and impact of a vulnerability;
- Establishing and communicating processes for vulnerability intake and handling;
- Clearly defining essential clinical performance to develop mitigations that protect, respond and recover from the cybersecurity risk;
- Adopting a coordinated vulnerability disclosure policy and practice; and,
- Deploying mitigations that address cybersecurity risks early and prior to exploitation.

In cases where a specific vulnerability could compromise the essential clinical performance of a device and represent a reasonable probability of death or serious adverse health consequences, the draft guidance recommends that manufacturers notify the FDA. The draft guidance also strongly advises medical device manufacturers to participate in a cybersecurity information sharing and analysis organization (ISAO) to facilitate the timely dissemination of cybersecurity information and intelligence among device manufacturers, providing a competitive advantage over companies that don’t engage in sustainable practices or those that fail to promote their efforts.

In addition to their specific recommendations, both of the FDA's guidance documents on cybersecurity in medical devices reference the NIST Framework noted previously in this paper, and encourage manufacturers to incorporate Framework Core elements in their risk management plans.

It is important to note that FDA guidance documents are advisory in nature and do not have the force of law. However, failure to comply with guidance recommendations can potentially slow the FDA’s review of a premarket application or subject a manufacturer to sanctions for unsafe products currently on the market. Therefore, compliance with the recommendations contained in FDA guidance documents is highly advisable.
A number of standards are currently available that address key aspects of the safety and security of interconnected medical devices and related software. A partial list includes the following standards:

ISO 14971—Medical devices – Application of risk management to medical devices

EC 60601-1—Medical electrical equipment
– Part 1: General requirements for basic safety and essential performance

IEC 62304—Medical device software – Software life cycle processes

IEC 80001-1—Application of risk management for IT-networks incorporating medical devices
– Part 1: Roles responsibilities and activities

IEC 80001-2-2—Application of risk management for IT-networks incorporating medical devices
– Part 2-2: Guidance for the disclosure and communication of medical device security needs, risks and controls

IEC/TR 80001-2-8—Application of risk management for IT-networks incorporating medical devices
– Part 2-8: Application guidance
– Guidance on standards for establishing the security capabilities identified in IEC 80001-2-2

IEC/TR 80001-2-9—Application of risk management for IT-networks incorporating medical devices
– Part 2-9: Application guidance
– Guidance for use of security assurance cases to demonstrate confidence in IEC/TR 80001-2-2 security capabilities (under development)

IEC 80002-1—Medical device software
– Part 1: Guidance on the application of ISO 14971 to medical device software

AAMI/UL 2800—Safety and Security Requirements of Interoperable Medical Systems (under development)

AAMI/TIR 57—Principles for medical device information security management

While compliance with the requirements in these standards is essential for dealing with the risks associated with cyber threats to interconnected medical devices, they do not directly evaluate the risk assessment process used by manufacturers to objectively assess the breadth and extent of cyber threats to which their devices might be exposed. Further, these standards do not provide clear and objective criteria to assess the actual effectiveness of product features designed to thwart the threats identified as part of the risk assessment. For manufacturers whose medical devices are subject to FDA pre-market approval, these gaps may complicate the review process as envisioned in the Agency’s guidance on the management of cybersecurity in medical devices.
Addressing the Gaps

To address these gaps, UL developed a series of Outlines of Investigations to provide verifiable criteria for assessing the cyber vulnerability of network-connectable products and systems. Applicable to a broad range of interconnected devices, the UL 2900 series, Standard for Software Cybersecurity for Network-Connectable Devices, is intended to address software vulnerabilities and weaknesses, minimize exploitation, avoid known malware leaving the production line, review security controls and increase security awareness and preparedness. For medical devices, UL 2900 will consist of three parts, as follows:

UL 2900-1: General Requirements for Network-Connectable Devices—Addresses general testing requirements applicable to all types of interconnected devices

UL 2900-2-1: Particular Requirements for Healthcare Systems—Address specific testing requirements applicable to healthcare systems and medical devices

UL 2900-3: General Requirements for the Organization and Product Development Security Lifecycle Processes for Network-Connectable Devices (under development)—Addresses general testing of organizational processes for conducting a risk assessment to determine applicable cyber threats
UL’s 2900 series of cybersecurity standards offers documented criteria for assessing the vulnerability of all types of network-connectable products and systems to cyber threats. Using tests such as known vulnerability scanning, malware scanning, static code analysis and others, UL 2900 series of standards help to identify software vulnerabilities and weaknesses, address known malware issues, review security controls and increase overall security awareness. As such, they provide medical device manufacturers with a method for demonstrating their efforts to provide for the security of their products against cyberattacks, as well as the safety and security of patients and their medical data.

UL’s 2900 series of standards are a core component of the UL CAP, which helps to address security risks in a wide range of interconnected devices and systems, including industrial control systems, automotive applications, building automation and smart home systems, networking equipment and consumer electronics. The UL CAP employs a holistic view of security, from product security to secure system integration, all with the goal of mitigating cybersecurity risks.

For more information about the UL 2900 series of standards and the UL CAP, visit http://ul.com/cybersecurity, or contact Medical.Inquiry@UL.com.

©2016 UL LLC. All rights reserved. This white paper may not be copied or distributed without permission. It is provided for general information purposes only and is not intended to convey legal or other professional advice.
Endnotes


Endnotes


