Deloitte.

Issue Brief:

Networked medical device cybersecurity and patient safety: Perspectives of health care information cybersecurity executives

Introduction

In a December 2012 episode of the popular television series *Homeland*,[i] the Vice President of the United States was assassinated when a terrorist organization wirelessly hacked his pacemaker. While this scenario may seem far-fetched, recent compelling demonstrations of networked medical devices' vulnerabilities and the potential for intentional threats (for example, insulin-pump hack) highlight concerns about cybersecurity threats to networked medical devices. Hundreds of thousands of medical devices such as patient monitors, infusion pumps, ventilators, and imaging modalities – many of which are life-sustaining or life-supporting – currently reside on hospital networks across the United States. Even more medical devices are accessible via wireless technologies, for example, insulin pumps and pacemakers.

Networked medical devices and other mobile health (mHealth)[ii] technologies are a double-edged sword: They have the potential to play a transformational role in health care but also may be a vehicle that exposes patients and health care organizations to safety and security risks. Among the unintended consequences of health care's digitization and increased networked connectivity are the risks of being hacked, being infected with malware, and being vulnerable to unauthorized access.

As growing numbers of medical devices incorporate wireless capabilities and complex software, operate adjunct to wired medical devices in hospitals, health systems, and home-based care, the scope and nature of required security controls also changes. Information technology, compliance, and risk executives in health care organizations will need to be able to anticipate and address present and future medical device security risks to safeguard patient safety and protected health information.

To understand how health care providers are approaching these challenges, Deloitte[iii,iv] interviewed stakeholders from nine health care organizations as part of a study on patient safety issues related to medical device security. The interview participants included representatives from Information Technology, Information Security, Clinical Engineering, and Compliance (collectively referred to in this report as Medical Device Security Leaders, or MDSLs). The interviews were conducted between May and December 2012. Interviewees represented a broad range of U.S. hospitals and health systems,[v] and they discussed their activities and attitudes about networked medical device governance, risk management, and security. The results show widespread agreement about specific issues; organizational differences in preparedness levels and approaches, and many shared opinions about future developments needed to underpin the industry.

#SecureMedDevice

Produced by the Deloitte Center for Health Solutions

Medical devices: Broadly defined

The Food and Drug Administration (FDA) defines a medical device in section 201(h) of the Federal Food Drug & Cosmetic (FD&C) Act as:

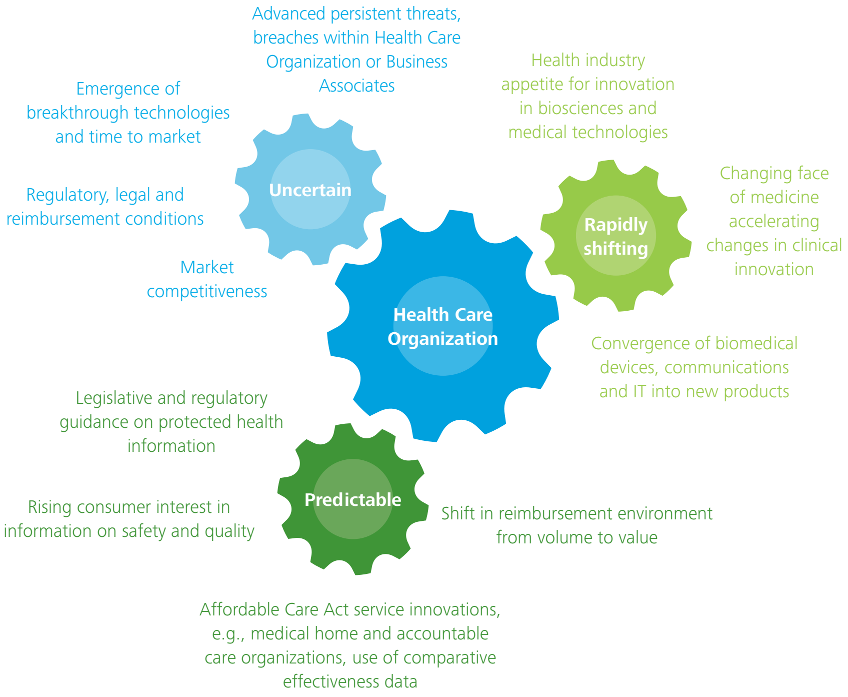
- "an instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including a component part, or accessory which is:
  - recognized in the official National Formulary, or the United States Pharmacopoeia, or supplement to them;
  - intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease, in man or other animals; or
  - intended to affect the structure or function of the body of man or other animals, and which does not achieve its primary intended purposes through chemical action within or on the body of man or other animals and which is not dependent upon being metabolized for the achievement of its primary intended purposes."[5]

As defined above, a medical device is regulated by the FDA and is subject to pre-marketing and post-marketing regulatory controls. In 2011, the FDA issued the Medical Device Data System (MDDS) rule, which clarified medical device regulation to include software, electronic or electrical hardware (including wireless) that makes claims to be useful for the medical purposes described in the MDDS classification (i.e., not generic software). The MDDS classification covers systems that act as a mechanism to transfer, store, convert, or display medical device data without controlling or modifying the function or parameters of a connected medical device.[6] Software that meets the law's definition of "medical device" in the United States has been subject to FDA scrutiny for safety and effectiveness. To date, the FDA has regulated software under the quality system regulation; however, with more focus on the security of such systems, as evidenced by the draft guidance on cybersecurity, this may be changing.

MDSLs and their organizations are operating in an environment that is at once rapidly shifting and uncertain yet predictable (Figure 1). Rapid shifts in the changing face of medicine – both clinical and systemic – are trending toward more diverse, integrated, and seamless care systems. Other change agents include increasing demand and appetite for technological innovation in biosciences, medical technologies, and networked medical device solutions, and reform-related regulatory, legal, and reimbursement issues.

The swift, evolving nature of cybersecurity threats means that the extent and nature of potential networked medical device security challenges is, to a degree, unknowable. MDSLs will need to have in place processes and procedures that address the "here and now" as well as "what may happen in the future." Robust governance, risk identification, and risk management capabilities are essential to helping MDSLs navigate the challenges of an increasingly complex system that is dependent upon integrated and networked technologies. In addition, MDSLs require skills and resources to help their organizations maintain regulatory compliance, improve overall efficiency and effectiveness, and deliver a high-quality and safe patient care experience.

Figure 1. The landscape for medical device security leaders is rapidly shifting, uncertain yet predictable.


Advanced persistent threats, breaches within Health Care Organization or Business Associates
Emergence of breakthrough technologies and time to market
Health industry appetite for innovation in biosciences and medical technologies
Uncertain
Regulatory, legal and reimbursement conditions
Changing face of medicine accelerating changes in clinical innovation
Rapidly shifting
Market competitiveness
Health Care Organization
Convergence of biomedical devices, communications and IT into new products
Legislative and regulatory guidance on protected health information
Predictable
Rising consumer interest in information on safety and quality
Shift in reimbursement environment from volume to value
Affordable Care Act service innovations, e.g., medical home and accountable care organizations, use of comparative effectiveness data

Copyright © 2013 Deloitte Development LLC. All rights reserved.

FDA Guidance

FDA draft guidance: Content of premarket submissions for management of cybersecurity in medical devices (June 2013).

This draft guidance proposes that cybersecurity features be integrated into the device development phase and identifies information that should be incorporated into premarket submissions for medical devices. Security capabilities should cover three specific areas:

1. Limit access to trusted users only
2. Determine trusted content
3. Use fail safe and recovery features

Manufacturers should define and document the following:

- Identification of assets, threats, and vulnerabilities
- Impact assessment of the threats and vulnerabilities on device functionality
- Assessment of the likelihood of a threat and of a vulnerability being exploited
- Determination of risk levels and suitable mitigation strategies
- Residual risk assessment and risk acceptance criteria

One insight from the guidance is the need for medical device manufacturers to produce evidence that their risk assessment process (as outlined in ISO 14971:2007) considered both "intentional" and unintentional security risks to the medical device and addressed those risks with appropriate security controls as part of the device's design. The evidence should be included as part of the premarket approval submission package (e.g., 510K, PMA). Medical device manufacturers should consider during the early phases of the software life cycle the processes and actors (e.g., hackers, organized crime, terrorists, and nation states) that intentionally mean to compromise a medical device for the purpose of either a) harming the patient or b) extracting protected health information. Manufacturers also should consider collaborating with their customers' clinical engineers and physicians to develop a catalog of use cases from which security vulnerabilities can be derived specific to their medical device and its intended use.

http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM356190.pdf

FDA safety communication: Cybersecurity for medical devices and hospital networks (June 2013).

This communication recommends that medical device manufacturers and health care facilities determine that appropriate safeguards are in place to reduce the risk of device failure due to a cyber-attack. Manufacturers are expected to take steps to limit unauthorized access to medical devices and to review policies and practices regarding appropriate safeguards.

In keeping with the FDA communication, manufacturers should:

- Limit access to trusted users
- Protect individual components from exploitation
- Maintain a device's critical functionality

Health care facilities should:

- Evaluate network security and protect the hospital system
- Restrict unauthorized access to the network and networked medical devices
- Determine that appropriate antivirus software and firewalls are up-to-date
- Monitor network activity for unauthorized use
- Protect individual network components through routine and periodic evaluation

http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm356423.htm

Understanding the context

MDSLs face a lengthy "to-do" list as the growth of wired and wireless networked systems brings attendant risks of cybersecurity breaches and concerns about medical device safety and effectiveness. In particular, patient safety issues – injury or death – related to networked medical device security vulnerabilities are a critical concern; compromised medical devices also could be used to attack other portions of an organization's network.

The Government Accountability Office (GAO) has noted that information security risk (particularly intentional threats) associated with certain medical devices is a relatively new field for health care providers, manufacturers, and regulators; however, it is one that is expected to become increasingly important.[7] The FDA stated that "many medical devices contain configurable embedded computer systems that can be vulnerable to cybersecurity breaches."[8]

MDSLs are charged with stewardship of a health care organization's privacy, security, and safety obligations. This means determining that governance, risk identification, and risk management processes are in place that mitigate information security vulnerabilities and breaches and that reduce corporate risk.

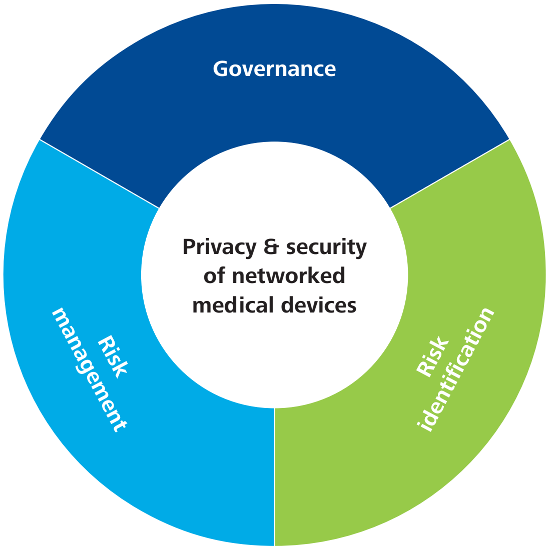
Security concepts

- **Cybersecurity (information security) concepts** is the protection of information and information systems from intentional or unintentional unauthorized access, use, disclosure, disruption, modification, or destruction in order to preserve their confidentiality, integrity, and availability.[7]
- **Vulnerabilities** may include weaknesses in technical security controls and physical security controls of a medical device, hardware, and software, as well as in implementation.
- **Risk** is a measure of potential harm to an organization due to adverse events that might occur and the likelihood of occurrence.
- **Assets** are things that are to be protected from compromise and include patient safety, patient privacy, and an organization's intellectual property, including proprietary care protocols and medical device availability and integrity.
- **Threats** represent the potential for an attacker to violate security and cause harm to assets.
- **Mitigation** is an act or control that reduces risk.

> In 1998, low-power heart monitors at a hospital were overwhelmed with electromagnetic interference and unable to provide critical care readings when a nearby TV station turned on a new digital television transmitter using a previously vacant TV channel.[9]

Key findings

Deloitte's interview findings fall into three areas: governance, risk identification, and risk implementation.



Copyright © 2013 Deloitte Development LLC. All rights reserved.

Governance

Organizational leadership

Close to half (four of nine) of the MDSLs strongly agree that their organizations have a strategy that drives risk management policies and procedures specific to medical device security. Participation in industry initiatives to define security standards is considered important, with around half of the MDSLs indicating active involvement (either personally or organizationally) in initiatives and consortia such as the Medical Devices Innovation Safety and Security Consortium (MDISS) or the Association for the Advancement of Medical Instrumentation (AAMI).

Risk framework

Many interviewees (six of nine) agree or strongly agree that they have a current framework to provide guidance on their organization's medical devices risk management objectives. In one health care organization, the policies and procedures in place do not differentiate between medical and non-medical systems. This organization is taking action to develop additional risk assessment methodologies specific to medical devices. Few interviewees mentioned any specific risk frameworks but those who did cited the ISO/IEC 80001 "Application of risk management for IT networks incorporating medical devices" framework.

Part of the ISO/IEC 80001 risk framework includes having well-defined and -delineated roles for identifying and managing patient safety and regulatory risks for medical devices. One organization indicated that they use a governance structure that clearly assigns responsibilities, policies, and risk management processes; this informs a master agreement that is used for outsourcing medical device support, management, access, and purchase.

Potential risks associated with networked medical devices

- Electromagnetic interference[7]
- Untested or defective software and firmware[7]
- Theft or loss of networked medical devices (external or portable)
- Security and privacy vulnerabilities[10]
  - Misconfigured networks or poor security practices[11]
  - Failure to install timely manufacturer security software updates and patches to medical devices[11] and concerns about causing service disruptions to functional devices
  - Improper disposal of patient data or information, including test results or health records
  - Uncontrolled distribution of passwords, such as employee carelessness in leaving a password unattended in public,[12] disabled passwords, or hard-coded passwords for software intended for privileged medical device access (e.g., to administrative, technical, and maintenance personnel)[8,13]
  - Manipulation, theft, destruction, unauthorized disclosure, or lack of patient data availability to providers
    - Network transfer (via email, remote access channel, or file transfer)[11]
    - Spyware and malware[11]
    - Spearphishing attacks[11]
- Unauthorized device setting changes, reprogramming, or infection via malware[7]
- Denial-of-service attacks[7]
- Targeting mobile health devices using wireless technology to access patient data, monitoring systems, and implanted medical devices[13]

Risk identification

Identify and evaluate

Close to half of the MDSLs (four of nine respondents) state that their health care organization has well-established processes and procedures to identify and evaluate emerging risks around networked medical devices. Others indicate that their organization has no formalized process; is currently identifying medical devices and applicable actions; or does not require that all medical devices go through the organization's standard evaluation process.

Inventory management is a critical component of risk identification and most MDSLs (seven of nine) say that their organization has some sort of inventory management for medical devices. Some interviewees state that their inventory management is a work-in-progress and expect to complete the process within the next few years. One respondent indicated that they do not differentiate between "connected" and "unconnected" devices in their current inventories. Inventory management may be decentralized across a health system's various in-patient and outpatient facilities and contained in disparate and non-centralized IT group asset management systems. One organization incentivizes executives to determine medical device inventory completeness and another has outsourced the inventory/asset management process to a third party. Many (six of nine) respondents indicate that they classify networked medical devices based upon the degree of patient criticality (e.g., life-sustaining); for others, this classification is under development but as yet incomplete.

Know the potential threats

According to the interviewed MDSLs, some of the key threats to networked medical devices include:

1. Hacktivists (i.e., anonymous individuals) wishing to cause service interruption.
2. Thieves desiring to sell or monetize personal health information (PHI), engage in identity theft, commit financial fraud against individuals and/or the health care organization, or defraud Medicare and/or Medicaid.
3. Malicious groups or individuals seeking to cause harm to patients (possibly targeting VIP patients) or seeking to damage the health care organization's brand.
4. Malware which evades existing antivirus engines and rules but is not specifically targeted at medical devices.

Data flow

Identifying and documenting how regulated data (e.g., protected health information) is stored, processed and/or transmitted by networked medical devices is important, and many MDSLs (six of nine) agree or strongly agree that their organization undertakes this task. In some organizations, processes to map interfaces with downstream systems and to record movement of sensitive data are under development; in others, these steps are built into the risk assessment process.

Risk management

Organizational systems

A health system – or hospital-level procurement processes – should have specific privacy and security requirements that medical devices must meet prior to their purchase from the manufacturer. The MDSLs' organizations have various approaches to address this requirement, including technical review committee evaluation and third-party evaluation. One respondent's organization is currently developing security-specific procurement requirements for networked medical devices. At another organization, new medical devices go through a rigorous process but lifespan issues with existing or legacy devices present a problem; in particular, the installation of timely updates and patches to deal with any vulnerability in older devices. Further, interviewees say that incorporating ongoing security support and maintenance into vendor agreements is not widely done or is an area where MDSLs have experienced roadblocks.

Vulnerability management

Risk-mitigating measures should be defined and supported by policies and procedures. Many MDSLs (six of nine) feel strongly that they have defined and implemented mitigating measures for networked medical devices that may be lacking appropriate safeguards. For example, many legacy medical devices (in service more than five years) run on proprietary operating systems and firmware. These legacy devices are difficult to test for vulnerabilities because off-the-shelf security scanning tools do not exist. All of the MDSLs indicate that they have spare components or environmental safeguards as backup for medical devices to protect against device failure.

While many of these health care organizations' networked medical devices run on proprietary operating systems and firmware, just as many run on well-known commercial operating systems. These medical devices are susceptible to the same vulnerabilities as other types of systems (e.g., servers, applications) that sit on a network.

Typical mitigation strategies range from quarantining medical devices that do not meet security standards to monitoring and taking appropriate steps on an as-needed basis. Specific actions include determining that new medical devices have up-to-date software and security patches, implementing compensating controls, and sampling devices randomly to gauge compliance.

Segregating a network (when it does not impact patient safety) to reduce permeability, including quarantining segments of the organization, is highly dependent upon the provider's size, scope, and geographic structure. More than half of interviewees (five of nine) say they are neutral about implementing organization-wide network segregation – for some, segregation varied by type of device rather than by organizational structure. (It is noted that mobile devices are identified as a category for which no good segregation solutions currently exist.) Other strategies for network segregation include creating sub-networks for medical devices unable to upload enterprise security software.

More than half of the MDSLs (five of nine) state strongly that they put physical safeguards in place to reduce theft or damage to networked medical devices. One strategy is use of risk management processes to identify medical devices with physical control weaknesses such as no encryption, substandard passwords, broad access, or a public location. Remediating solutions include locking down CPUs or medical devices; retaining spare components; pre-negotiating contracts with vendors to maintain device operation or prevent failure; and instituting environmental safeguards such as an uninterrupted power supply, particularly for critical-care life support systems.

In the June 2013 Safety Communication on cybersecurity for medical devices and hospital networks, the FDA observed that it has become aware of cybersecurity vulnerabilities and incidents that could directly impact medical devices or hospital network operations, including failure to provide timely security software updates and patches to medical devices and networks and to address related vulnerabilities in older medical device models (legacy devices).[8]

Manufacturer and FDA engagement

MDSLs recognize the need to be proactive in engaging with medical device manufacturers to share networked medical device cybersecurity and privacy vulnerabilities. Many agree or strongly agree (five of nine) that their organization effectively engages with manufacturers for this purpose – some work with manufacturers to implement cybersecurity controls when a new medical device is procured, others share cybersecurity incidents with vendors. Looking ahead, one respondent suggested that providers need to develop better and more specific vendor requirements to support long-term medical device cybersecurity management.

Nearly all MDSLs (seven of nine) believe that medical device manufacturers need to improve ongoing cybersecurity and privacy support and maintenance for networked medical devices. Most feel that they have to be proactive in reaching out and educating manufacturers on how to secure medical devices to meet regulatory requirements. MDSLs would prefer more proactive manufacturer communication and attention to the timely provision of updates, guides, and guidance in security patch deployment to address cybersecurity vulnerabilities.

Intentional threats

The FDA draft guidance, *Content of premarket submissions for management of cybersecurity in medical devices* (June 2013), calls attention to "intentional" threats when designing a medical device. Examples of potential "intentional" threats within a health care environment include:

- Malware and viruses infecting medical devices
- Organized crime attacking a VIP patient's personal medical device
- Hackers/nation states targeting Distributed Denial of Service (DDoS) attacks against a hospital network
- Organized crime conducting exfiltration attacks against hospital medical devices for ePHI
- Hackers testing their skills against a hospital's vulnerable network (including networked medical devices)
- Disgruntled employees uploading Trojan horse code to networked medical devices

Networked medical devices landscape

Currently, health care providers are not required to report security incidents to the FDA's MedWatch or MedSun program or the device manufacturer, unless a death or serious injury has occurred. One interviewee notes that the FDA does not distinguish between safety and security incidents and that this distinction might encourage health care organizations to more frequently report incidents. Another respondent suggested that regulatory attention be directed toward the manufacturing sector and compliance with security controls.

Additional insights

Looking beyond immediate governance and risk-management issues, the interviewed MDSLs offer two additional insights:

Understand and anticipate the extent of and reasons for cybersecurity vulnerabilities

While the MDSLs and the industry in general[7] have not experienced instances of intentional threats to networked medical devices, most MDSLs express concern about devices' potential vulnerability to cybersecurity and privacy issues; in particular, wireless-digital radiography and wired/wireless infusion pumps. Most MDSLs share the view that it is possible to hack or cause denial of service to networked medical devices in the "real world." Potential reasons why intentional disruption might be possible include direct internet connectivity and unpatched cybersecurity weaknesses. Other vulnerabilities that could give rise to unintentional cybersecurity threats relate to device design and product lifecycle issues, including software upgrade releases. Actual cybersecurity incidents involving networked medical devices that MDSLs shared during the interviews include:

- An entire monitoring system being taken offline for several hours because it was infected with the Conficker virus;
- A wireless IV pump being affected by "wireless chatter," ultimately impacting the dosage rate for the pump;
- A medication management automated dispensing system becoming infected with malware and being taken offline for several hours.

The MDSLs cite two factors underpinning the medical device vulnerability issue: 1) the degree to which the medical device manufacturer focuses on information and device cybersecurity; and 2) provider systems and structures (e.g., non-centralized purchasing) which may fail to properly vet device cybersecurity prior to purchase; may require more secure remote device support and maintenance by the manufacturer; and may provide insufficient network architecture/segmentation for isolating some of the more vulnerable devices.

Health care providers likely will need better cybersecurity tools, approaches, and support from medical device manufacturers to address the thousands of legacy networked medical devices with a long "shelf-life" that are sitting on hospital networks that cannot easily be tested for cybersecurity vulnerabilities.

Industry improvement: It's a team effort

Many MDSLs (five of nine) agree that accountability for medical device cybersecurity and privacy is a shared responsibility of manufacturers and health care providers; the FDA, in turn, is responsible for providing regulatory oversight, cybersecurity and privacy standards, and guidance. Some MDSLs differentiate between manufacturers' responsibility for safe manufacturing practices and medical device support and providers' responsibility for device operations (e.g., network security, patient training, clinical engineering and IT). One MDSL says that patients also have some accountability for devices in the home health care environment.

Several suggest that manufacturers could develop more capabilities to address privacy support and cybersecurity issues; further FDA oversight or attention may assist manufacturers in this regard. One respondent says that industry consortia, such as the Medical Device Innovation, Safety and Security (MDISS) Consortium, Health Information and Management Systems Society (HIMSS), and the Association for the Advancement of Medical Instrumentation (AAMI), can help to drive industry recognition of cybersecurity and privacy issues.

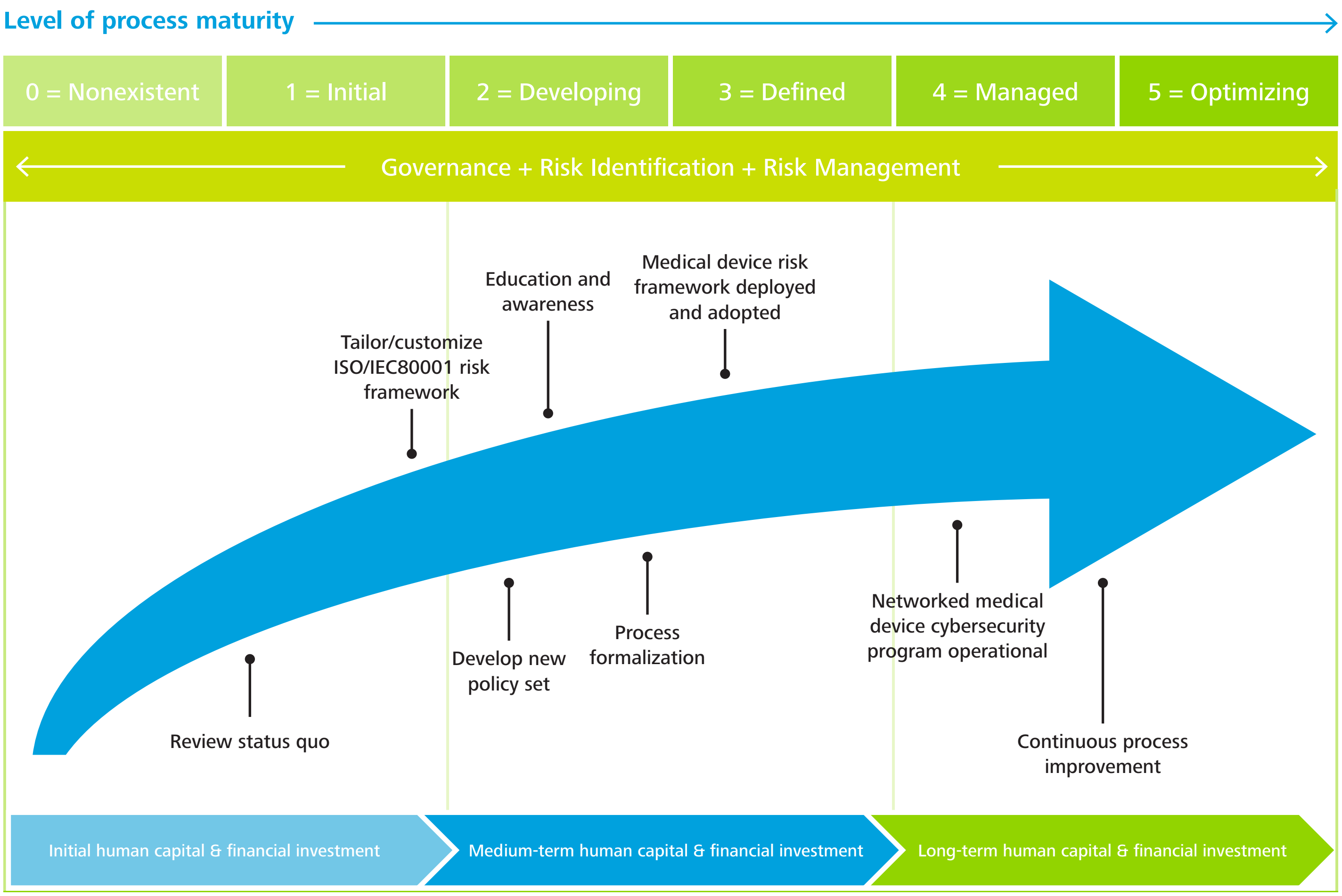
It appears that much more can be done within provider organizations to increase awareness among stakeholders – physicians, Chief Medical Information Officers (CMIOs), CIOs, and clinical engineering teams – about current and potential medical device threats and vulnerabilities. Educating these stakeholders may increase their support for appropriate cybersecurity capabilities in devices being considered for procurement.

Stakeholder considerations

Overall, MDSLs recognize that their challenges are substantial and their time and resources limited, so they are juggling short-term priorities with longer-term needs, both of which they see as essential. There is widespread consensus among interviewees about near- and long-term strategies and priorities; however, getting there is the challenge.

Options for MDSLs who may be dealing with networked medical devices privacy and cybersecurity issues include assessing their organization in the areas of governance, risk identification, and risk management relative to their current and desired state, then mapping a pathway forward (Figure 2).

Figure 2: Networked medical device process maturity model



Level of process maturity
0 = Nonexistent
1 = Initial
2 = Developing
3 = Defined
4 = Managed
5 = Optimizing
Governance + Risk Identification + Risk Management
Education and awareness
Medical device risk framework deployed and adopted
Tailor/customize ISO/IEC80001 risk framework
Review status quo
Develop new policy set
Process formalization
Networked medical device cybersecurity program operational
Continuous process improvement
Initial human capital & financial investment
Medium-term human capital & financial investment
Long-term human capital & financial investment

Copyright © 2013 Deloitte Development LLC. All rights reserved.

Looking to the future, MDSLs should consider focusing on the following areas to enhance the effectiveness of their organizations' strategies to attain appropriate levels of medical device safety and security.

1. **Read the FDA's draft guidance, *Content of premarket submissions for management of cybersecurity in medical devices (June 2013)* and related *FDA Safety Communication.***

- The draft guidance and safety communication will inform MDSLs about threats, risk, and vulnerabilities from the FDA's point of view.
- The draft guidance also will provide insight into the types of security features and capabilities that health care organizations can anticipate in future networked medical devices.

2. **Understand the organization's risk.**

- Conduct an organization-wide situational and environmental analysis.
- Understand the degree and complexity of risk facing the organization.
- Conduct due diligence on appropriate standards and strategies to mitigate identified risk and develop an action plan and corresponding resources plan (human capital and funding) required to address the issue.

3. **Adopt a formalized risk management framework for networked medical devices and implement administrative and functional policies.**

- Adopt a risk management framework such as ISO/IEC 80001 and tailor it to the organization's risk culture and environment.
- Develop standardized procurement policies that enhance security:
  - Integrate networked medical device-specific security and privacy evaluations and requirements into the procurement process. Consider leveraging the "Manufacturer Disclosure Statement for Medical Device Security – MDS2" and augment this standard questionnaire with organization-specific requirements.
  - Conduct "white box" reviews of networked medical devices being considered for purchase, either internally or via a third party.
  - Incorporate ongoing security support and maintenance into vendor agreements.
- Institute resiliency measures:
  - Arrange that spare components are available on-demand for networked medical devices to maintain operations in case of a failure.
  - Institute environmental safeguards (e.g., generator backup, uninterruptible power supplies, redundant HVAC) to protect facilities that house critical-care and life-support medical devices.
- Address manufacturer arrangements:
  - Gain support from networked medical device manufacturers to continuously identify vulnerabilities and risks, create safety measures to mitigate damage, and provide ongoing firmware, patch, and antivirus updates.

4. **Enhance vulnerability management for networked medical devices.**

- Inventory and classify networked medical devices.
  - Establish an up-to-date, centralized, and complete inventory of networked medical devices. Stratify the inventory to include wired, wireless, and legacy (those in service more than five years) networked medical devices.
  - Classify networked medical devices by patient criticality.
- Limit access to authorized users via maintained authorized access control lists and strong authentication controls.
- Leverage the established inventory with appropriate monitoring tools to detect and analyze unknown/rogue devices.
- Conduct routine security risk assessments and audits of networked medical devices.
- Update appropriate antivirus software and firewalls with support from the device manufacturer if available.
- If it is unrealistic to develop in-house, in-depth vulnerability assessment capabilities, consider outsourcing vulnerability management to third-party solution providers.

5. **Increase security education and awareness among medical device stakeholders.**

- Establish and/or enhance education and awareness programs for stakeholders, including clinical engineers and physicians, the CMIO and the CIO, to increase their knowledge and understanding of the threats, vulnerabilities and risks (TVR) to networked to networked medical devices.
- Involve team members such as clinical engineers and physicians in developing and implementing procurement policies and processes that address minimum security requirements for networked medical devices.
- Incorporate TVR analysis into risk reports on networked medical devices.
- Translate risk findings into stakeholder language and present the findings at various forums (e.g., brown bag lunches, special briefings, etc.).

6. **Leverage the National Health Information Sharing and Analysis Center (NH-ISAC).**

- Consider collaborating with the NH-ISAC and FDA to explore ways to share security incident and vulnerability discoveries related to networked medical devices while also addressing provider concerns about liability. The NH-ISAC already is working with a number of organizations at the state and federal levels, and medical device security is a high-priority area.
- Advocate FDA and NH-ISAC collaboration to develop a comprehensive outreach plan to health care organizations which outlines the benefits of leveraging NH-ISAC capabilities, as well as the overall public health benefit of sharing medical device security vulnerability information with the FDA (via the NH-ISAC). Examples of outreach could include webinars, a national roadshow briefing to be held at provider facilities, and an invitation-only national summit bringing together provider and device manufacturer executives.

7. **Protect vulnerable legacy medical devices via network segregation.**

- Consider where appropriate implementing network segregation measures, such as Virtual Local Area Networks (VLANs), and firewall and router access control lists.
- Anticipate that network segregation measures by themselves may not be sufficient; “bridges” between networks likely will exist, and may not be fully understood in complex networks. Therefore where appropriate, consider implementing network monitoring capabilities in tool sets such as network analytics solutions and security information and event management (SIEM) solutions.[6]

8. **Learn from other industries’ experience**

- Many industries, such as Public Utilities and Oil & Gas, have faced the challenge of defending and protecting complex and unique devices with embedded systems from cyberattacks. Lessons learned from their experience should be considered in the health care environment.
  - Recognize that medical devices are a focus area for security researchers, and vulnerabilities and disclosures will occur – sometimes with little, if any, warning. This unpredictability will require capabilities across the ”protect, defend, respond, and recover” spectrum.
  - Engage deeply with the security community, where appropriate, including peers at other organizations.
  - Prepare to invest in building capabilities beyond operational security, including investing in human resources or third-party specialists to access capabilities in emerging areas such as cyber threat intelligence and network and malware analysis.
  - Realize that those who wish to cause harm or disruption via medical devices have both time and resources in their arsenal, and are prepared to play ”the long game.”

Conclusion

The U.S. health care system is moving rapidly toward widespread adoption and integration of wired and wireless networked medical devices – these devices facilitate medical care and produce an immense volume of clinical and administrative information. Much rides upon the medical devices availability, integrity, and cybersecurity and – of utmost importance – upon the safety of medical devices used in patient care.

Moreover, the disruptive power of networked medical devices and other technologies, and the accompanying waves of innovation they have sparked, are transforming the health care industry, propelling stakeholders to reassess and repurpose how they provide services. Additionally, evolving technologies and permeable boundaries among existing and new entrants in the health ecosystem can increase the complexity of managing protected health information and providing a safe environment for patients.

Technology's promise lies in its ability to improve the quality and timeliness of patient care while lowering costs. However, as more medical devices become networked and use wireless technologies, unintended safety, privacy, and cybersecurity issues could arise. Health care organizations are challenged to anticipate the full spectrum of intentional and unintentional threats that might expose potential vulnerabilities in their networked medical devices. Yet anticipate they must, as well as put into place comprehensive systems to mitigate regulatory, financial and ethical risk; facilitate work flow and workforce efficiency; strengthen the privacy and cybersecurity of protected health information; and promote the safety of patients under their care.

Appendix

Methodology

Deloitte sought to understand the activities and attitudes of health care industry information technology, compliance, and risk executives regarding governance, risk management, and security of networked medical devices. Deloitte conducted in-person interviews with nine executives representing academic medical centers, regional not-for-profit health and hospital systems, Catholic hospital systems, and for-profit hospital systems between May and December 2012. The number of medical devices managed by respondents is as follows: fewer than 5,000 (2 of 9 respondents); between 5,000 and 10,000 (2 of 9 respondents); between 10,000 and 50,000 (2 of 9 respondents); and between 50,000 and 500,000 (3 of 9 respondents).

The survey was designed to elicit health care providers' perspectives on:

1. The extent of vulnerable networked medical devices, including how and who could hack devices
2. Identifying current and future risks to patient safety
3. Identifying the group(s) responsible for health care organizations' security/risk management policies and procedures.

To begin a discussion or for further information on medical device security, safety and risk management in the Life Sciences and Health Care industry, please contact:

Russell L. Jones, CISSP, CIPP/G
Partner
Security & Privacy Services
Deloitte & Touche LLP
rujones@deloitte.com

Bruce Murphy, CISSP
Principal
Security & Privacy Services
Deloitte & Touche LLP
brmurphy@deloitte.com

Mark Ford, CISSP
Principal
Security & Privacy Services
Deloitte & Touche LLP
mford@deloitte.com

Larry Spears
Director
Governance, Regulatory & Risk Strategies
Deloitte & Touche LLP
lspears@deloitte.com

Authors

Russell L. Jones, CISSP, CIPP/G
Partner
Security & Privacy Services
Deloitte & Touche LLP
rujones@deloitte.com

Sheryl Coughlin, PhD, MHA
Head of Research
Deloitte Center for Health Solutions
Deloitte Services LP
scoughlin@deloitte.com

Contact information

To learn more about the Deloitte Center for Health Solutions, its projects and events, please visit www.deloitte.com/centerforhealthsolutions.

Deloitte Center for Health Solutions
1001 G Street N.W.
Suite 1200
Washington, DC 20001
Phone 202-220-2177
Fax 202-220-2178
Toll free 888-233-6169
Email healthsolutions@deloitte.com
Web www.deloitte.com/centerforhealthsolutions

Follow @DeloitteHealth on Twitter

#SecureMedDevice

To download a copy of this report, please visit www.deloitte.com/us/securemeddevice

Acknowledgements

Deloitte Consulting LLP
Geoff Pascoe
Specialist Master
Federal Healthcare Consulting

Deloitte Services LP
Elizabeth Stanley
Research Manager

Claire Boozer
Operations Specialist

Lynn Sherry
Senior Manager, Marketing

Carol Lynne Jones
Senior Manager, Marketing

Kathryn Robinson
Manager, Marketing

Deloitte and Touche LLP
Alex Stamps
ERS Manager

Phil Cantu
ERS Manager

Veronica Lim
ERS Senior Manager

Thank you to the individuals and health care organizations who participated in the interviews for this study.

Endnotes

i Season 2, Episode 10 of *Homeland*, a fictional television series broadcast on the cable network Showtime (Showtime Networks, Inc.) and produced by Fox 21.

ii mHealth has been defined as "medical and public health practice supported by mobile devices, such as mobile phones, patient monitoring devices, personal digital assistants (PDAs), and other wireless devices." World Health Organization, mHealth. New horizons for health through mobile technologies, in Global Observatory for eHealth series 2011, World Health Organization: Geneva, Switzerland. http://www.who.int/goe/publications/goe_mhealth_web.pdf

iii As used in this document, "Deloitte" means Deloitte LLP and its subsidiaries. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.

iv Interviews were conducted by members of Deloitte's Audit and Enterprise Risk Services (AERS) practice

v Including academic medical centers, regional not-for-profit health and hospital systems, Catholic hospital systems, and for-profit hospital systems.

References

1 Halperin D, Heydt-Benjamin TS, Ransford B, Clark SS, Defend B, Morgan W, et al. "Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses." 2008 [cited July 2013]. Available from: http://www.secure-medicine.org/public/publications/icd-study.pdf.

2 "Hacking Medical Devices." [Internet] [cited August 2013]. Available from: http://www.darkreading.com/vulnerability/getting-root-on-the-human-body/231300312.

3 Paul N, Kohno T, Klonoff DC. "A Review of the Security of Infusion Pump Systems." *J Diabetes Sci Technol.* 2011;5(6):1557-1562.

4 Kramer DB, Baker M, Ransford B, Molina-Markham A, Stewart Q, Fu K, et al. "Security and Privacy Qualities of Medical Devices: An Analysis of FDA Postmarket Surveillance." *PLoS ONE* 7(7) 2012. [Internet] [cited August 2013].

5 U.S. Food and Drug Administration. Overview of medical device regulation. [cited August 2013]. Available from: http://www.fda.gov/medicaldevices/deviceregulationandguidance/overview/classifyyourdevice/ucm051512.htm.

6 U.S. Food and Drug Administration. MDDS Rule [cited August 2013]. Available from: http://www.fda.gov/MedicalDevices/ProductsandMedicalProcedures/GeneralHospitalDevicesandSupplies/MedicalDeviceDataSystems/ucm251897.htm.

7 U.S. Government Accountability Office. Medical Devices: FDA Should Expand its Consideration of Information Security For Certain Types of Devices. Washington D.C.: 2012.

8 U.S. Food and Drug Administration. FDA Safety Communication: Cybersecurity for Medical Devices and Hospital Network 2013 [cited August 2013]. June 14: Available from: http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm356423.htm.

9 McClain. J.P. "Time to Upgrade. New telemetry standards call for a new generation of wireless equipment no date." [cited August 2013] Available from: http://www.ashe.org/resources/WMTS/pdfs/timetoupgrade.pdf.

10 Keckley PH, Coughlin SL, Gupta S. *Privacy and Security in Health Care: A fresh look.* Washington, DC: Deloitte Center for Health Solutions, 2011.

11 U.S. Department of Homeland Security. National Cybersecurity and Communications Integration Center. Attack Surface: Healthcare and Public Health Sector [cited August 2013]. Available from: http://info.publicintelligence.net/NCCIC-MedicalDevices.pdf.

12 Sun LH, Dennis B. "FDA, facing cybersecurity threats, tightens medical-device standards. *Washington Post*" [cited August 2013] Available from: http://www.washingtonpost.com/national/health-science/facing-cybersecurity-threats-fda-tightens-medical-device-standards/2013/06/12/b79cc0fe-d370-11e2-b05f-3ea3f0e7bb5a_story.html.

13 Nelson Mullins Riley & Scarborough LLP. FDA Safety Communication: Cybersecurity for Medical Devices and Hospital Networks. [cited August 2013] Available from: http://www.nelsonmullins.com/DocumentDepot/FDA_Cybersecurity_Docs.pdf.

Deloitte Center
for Health Solutions

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.

About the Deloitte Center for Health Solutions
The Deloitte Center for Health Solutions is the health services research arm of Deloitte LLP. Our goal is to inform all stakeholders in the health care system about emerging trends, challenges, and opportunities using rigorous research. Through our research, roundtables, and other forms of engagement, we seek to be a trusted source for relevant, timely, and reliable insights.

Copyright © 2013 Deloitte Development LLC. All rights reserved.

Member of Deloitte Touche Tohmatsu Limited