MEDJACKING: A LIFE OR DEATH ISSUE FOR LEADERS IN CONNECTED HEALTHCARE

Authored by:
Colin Konschak, FACHE, Divurgent
Shane Danaher, MBA, Divurgent

INTRODUCTION

When you imagine medical devices being breached by cybercriminals, your thoughts might automatically go to the horror scenario—a pacemaker being ordered to drive 800 volts into the heart of an unsuspecting politician or an infusion pump being shut off or instructed to deliver a deadly multi-dose administration. While threats like these need to be taken seriously, healthcare IT leaders are looking at bigger picture organizational threats when it comes to medical device breaches, or "medjacking" as it has come to be known.

The bigger picture looks like this: the cybercriminal finds a security vulnerability in a networked imaging machine in a large hospital, letting her into the wi-fi network, eventually providing an entry into the entire network. From there a range of damage could be done, including holding electronic health records hostage, stealing protected health information, shutting the network down, or back to the horror scenario above of causing malfunctions in medical devices hooked up to people, except on a much grander scale.

In this whitepaper we look at the risks of medjacking and identify key elements of management strategies to help mitigate those risks.

> *"We use the term medjack, or medical device hijack, to frame what we see as the attack vector of choice in healthcare. Attackers know that medical devices on the network are the easiest and most vulnerable points of entry. The medjack is designed to rapidly penetrate these devices, establish command and control and then use these as pivot points to hijack and exfiltrate data from across the healthcare institution."*
>
> --- *Moshe Ben Simon, Co-Founder & VP, TrapX Security, General Manager, TrapX Labs,* Anatomy of an Attack, 2015

Although discussion of healthcare cybersecurity tends to revolve around patient records and privacy issues, that is not where some of the greatest vulnerabilities lie. Instead, the weakest links in cybersecurity may be in surgical robots, imaging machines, infusion pumps, neurostimulators, pacemakers, and a myriad of other medical devices and equipment used in hospitals and medical clinics and implanted in or hooked up to people's bodies.

The average hospital has thousands of devices and machines with computer chips, ranging from wireless blood pressure cuffs that transmit data into EHRs, to computerized tomography (CT) scanners, magnetic resonance imaging (MRI) machines and surgical robots. Most are connected to the hospital's local access network (LAN) and the Internet. In a survey of 535 IT practitioners in healthcare organizations, 59% said their organizations had more than 300 network-connected devices (Ponemon, 2016).

The ability of nefarious agents to use these vulnerable assets for medjacking attacks calls for a new mindset among healthcare executives and IT leaders, according to Symantec Technical Architect, Axel Wirth, writing in a February 2018 blog. "In the last couple of years, cyber attackers demonstrated that healthcare's exposure goes beyond protecting data; they can actually shut down hospitals and impact care delivery," Wirth wrote. "Healthcare leaders are realizing that this was a lot more serious than the prospect of a HIPAA fine or audit. Simply put, if your clinical staff can't access data, there is a severe impact to delivering patient care. No surprise, then, to learn that 60% of healthcare providers now consider risk assessment, rather than just HIPAA compliance, their top consideration in their security investments" (Wirth, 2018).

Wirth dove a little deeper into the risk assessment aspect. "As they've learned from being on the receiving end, cyber-attacks can lead to a shutdown of equipment, thus disrupting a hospital's ability to offer clinical services. You're also starting to see the growing appreciation of the cyber security implications of an increasingly connected world. If a malicious hacker can bust in and tamper with the temperature of the hospital HVAC system, they can put operating rooms out of order and cause the cancellation of scheduled operations."

The most significant global attack to date, the WannaCry ransomware attack—attributed to North Korea—impacted 144+ countries and had a profound impact on the National Health System in the UK. This attack, which occurred in May 2017, illustrates how exploits in one part of the healthcare ecosystem, such as disabling clinicians' access to critical medical information across all types of care environments, can adversely affect care and prompt a major health crisis as well as disrupt operational workflow in all other sectors of the industry.

According to McAfee Chief Scientist Raj Samani: "Whether it disrupts an MRI scanner, forces a hospital to cancel surgeries or prevents a doctor from finding patient information, ransomware can impede healthcare treatment and risk patient well-being" (Hayes, 2017).

WHERE ARE THE THREATS?

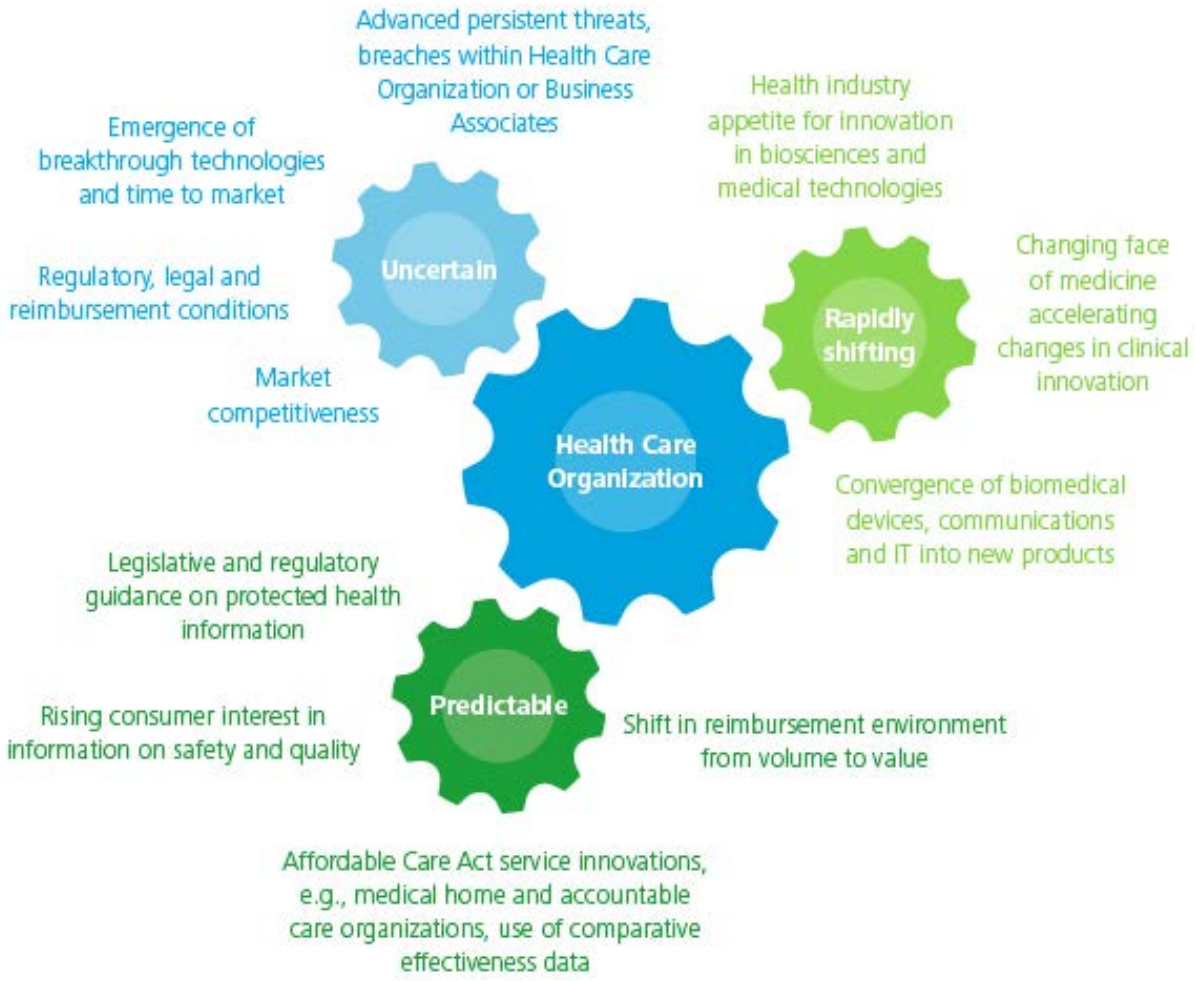
Consultants at Deloitte Center for Health Solutions interviewed stakeholders from nine healthcare organizations about medical device security in 2012, just as concern about the vulnerability of medical devices was emerging. They highlighted the rapidly shifting landscape for medical device security, as depicted in Figure 1 (Deloitte, 2012).

In its research, Deloitte identified numerous potential risks with regard to networked medical devices, including:

- Electromagnetic interference
- Untested or defective software and firmware
- Theft or loss of networked medical devices (external or portable)
- Security and privacy vulnerabilities

- Misconfigured networks or poor security practices
- Failure to install timely manufacturer security software updates and patches to medical devices, and concerns about causing service disruptions to functional devices
- Uncontrolled distribution of passwords, such as employee carelessness in leaving a password unattended in public, disabled passwords, or hard-coded passwords for software intended for privileged medical device access (e.g., to administrative, technical, and maintenance personnel)
- Unauthorized device-setting changes, reprogramming, or infection via malware
- Targeting mobile health devices using wireless technology to access patient data, monitoring systems, and implanted medical devices

Figure 1: The Landscape for Medical Device Security



Source: Networked Medical Device Cybersecurity and Patient Safety. (2012). Deloitte Center for Health Solutions.

2018 Threat Predictions for Connected Care

In its report titled, Threat Predictions for 2018, global cybersecurity firm, Kaspersky Lab, predicted the 2018 threats to connected healthcare. Medjacking plays a part in several of those predictions, which are:

- "Attacks targeting medical equipment with the aim of extortion, malicious disruption or worse, will rise.
- There will also be a rise in the number of targeted attacks focused on stealing data.
- There will be more incidents related to ransomware attacks against healthcare facilities.
- The concept of a clearly-defined corporate perimeter will continue to "erode" in medical institutions.
- Sensitive and confidential data transmitted between connected 'wearables,' including implants, and healthcare professionals will be a growing target for attack.
- National and regional healthcare information systems that share unencrypted or otherwise insecure patient data between local practitioners, hospitals, clinics and other facilities will be a growing target for attackers looking to intercept data beyond the protection of corporate firewalls.
- The growing use by consumers of connected health and fitness gadgets will offer attackers access to a vast volume of personal data that is generally minimally protected.
- Disruptive attacks—whether in the form of denial of service attacks or through 'ransomware' that simply destroys data (such as WannaCry) – are a growing threat to increasingly digital health care facilities.
- Emerging technologies such as connected artificial limbs, implants for smart physiological enhancements, embedded augmented reality etc. designed both to address disabilities and create better, stronger, fitter human beings will offer innovative attackers new opportunities for malicious action and harm unless they have security integrated from the very first moment of design."

Source: Kaspersky Lab. (2017). Kaspersky Lab Threat Predictions for 2018. Retrieved at: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07164714/KSB_Predictions_2018_eng.pdf

The biggest threats currently relating to the medjacking issue are the medical devices themselves and their inherent vulnerabilities. These problems have been raised for several years now as these attacks intensify, using medical equipment in hospitals as the breaching mechanism for bad actors. Manufacturers have been under increasing pressure to step up to the security challenges. So how bad is it?

In one frightening scenario, TrapX Security tested the protection of medical devices in more than 60 hospitals. Within six months, numerous devices had been infected with malware. While the hackers weren't manipulating the devices themselves, they were using them as a portal to infiltrate the rest of the hospital's systems to steal patient data. The security experts also found ransomware software on some machines, suggesting that the cyberattackers could have taken

the machines "hostage," threatening patients unless the hospitals met their demands. In three hospitals, X-ray equipment, picture archives (used to store radiologic images), communications systems, and blood gas analyzers were compromised (TrapX Labs, 2015).

Imagine a critical emergency during which clinicians receive wrong information about a patient's status because the blood gas analyzer had been medjacked!

Government healthcare entities are far from immune to the risk. A 2013 *Wall Street Journal* investigation found that malware had infected at least 327 devices at Veterans Administration hospitals, including x-ray machines and equipment in a catheterization lab, forcing the lab to temporarily close. Several IT executives at the hospitals affected said they weren't even aware of the problems or the potential for such infections (Weaver, 2013).

Researchers from the University of South Alabama found that even the medical mannequins used to train medical students can put an entire system at risk. They armed fourth-year medical students with open-source software and a mannequin, and watched as they easily gained access to the device and launched a denial of service attack. Few had any significant technical expertise in computers (Glisson, Andel, McDonald, Jacobs, M., et al., 2015).

Medical devices, particularly those integrated into a system's network or implanted in the body, are a huge attack vector for numerous reasons (TrapX Labs, 2015; GAO, 2012):

- Most were approved without appropriate safeguards. Updating them now, manufacturers argue, would require additional FDA approvals (even though the agency has said that devices do not need to be recertified).
- Most are closed systems that are often inaccessible to in-house IT staff, with only the manufacturer's representatives able to access them. This makes it nearly impossible for hospitals to identify malware and other breaches, and to run the type of security software they use to protect computers and the IT network.
- Most hospital devices run on ancient software, including operating systems dating back to Windows 2000 and Windows XP, neither of which is still supported.
- Adding updates/patches without manufacturer approval and testing could void the warranty, after which manufacturers may refuse to continue servicing the devices.
- Most devices (particularly implanted devices like pacemakers) are in use 24 hours a day, seven days a week, making updates difficult.
- Implanted devices have limited battery capacity. New security features could further drain the battery. They are also vulnerable to attacks designed specifically to drain the battery.
- Most devices, external and internal, can be remotely accessed.
- Most devices transfer unencrypted data to external portals like the EHR.
- There are limited or nonexistent authorization processes. In other words, they don't discriminate between authorized and non-authorized access. Adding such features, however, could limit the ability of health professionals to provide care in an emergency situation.

- They are extremely difficult to secure. An investigation by security firm TrapX found significant delays in addressing security breaches in hospital devices. Even after the malware was removed, the company reported, it was easy to reinfect it. “There was no real protection offered by most cyber defense suites that could run within the medical devices,” the company wrote in a report.

Manufacturers argue that if hospitals had stronger firewalls, attackers couldn’t break into the devices, while hospitals argue that it is up to the manufacturer to provide secure devices (Reel & Robertson, 2015; O’Brien & Khanna, 2014).

On this point hospitals are correct. Firewalls are nearly useless against networked devices. Devices could be infected prior to shipment to the hospitals or get infected during maintenance processes.

Most healthcare organizations say they are only in the planning stages for medical device security (Symantec, 2016). A 2016 survey of more than 500 healthcare IT professionals found that although 77% viewed unsecured medical devices as a serious threat, just a third said their organization has the security of those devices as part of their cybersecurity strategy (Ponemon, 2016).

MEDICAL DEVICE VULNERABILITIES CONTINUE

Recent government advisories provide examples of the types of problems there are, and how an attack on security flaws like these could be executed and the kinds of damage they can cause.

In late March 2018, the Department of Homeland Security’s Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) issued security advisories noting that Dutch healthcare technology giant Philips had reported vulnerabilities in its iSite and IntelliSpace PACS medical imaging archiving communications systems as well as its Alice 6 polysomnography system. The advisory stated:

> "If exploited, these vulnerabilities could impact or compromise patient confidentiality, system integrity, and/or system availability. The vulnerabilities may allow attackers of low skill to provide unexpected input into the application, execute arbitrary code, alter the intended control flow of the system, access sensitive information, or potentially cause a system crash" (ICS-CERT, 2018, March 29).

To fix the vulnerabilities regarding the iSite and IntelliSpace products, Philips recommended that product users enroll in its monthly patching program and update firmware. In addition, users can upgrade to IntelliSpace PACS 4.4.55x with Windows 2012, which addresses product hardening. The company estimated that the three steps together should take care of 99.9 percent of known vulnerabilities in the products.

With regard to the Alice 6, the following were the possible impacts:

> "Successful exploitation may allow an attacker to gain visibility to usernames/passwords and personal data. Insufficient encryption and cryptographic integrity checks can lead to altered, corrupted, or disclosed sensitive data. Disclosure of personal data can occur by replacing a trusted node with a malicious node"(ICS-CERT, 2018, March 27).

The ICS-CERT advisory regarding the Alice 6 vulnerabilities stated that Philips is scheduled to release a new product version and supporting product documentation in December 2018. For all users of the Alice 6 System product, version R8.0.2 or prior, Philips will update the devices to R8.0.3. In the meantime, Philips recommends that customers "Ensure that network security best practices are implemented and limit network access to Alice 6 in accordance with product documentation."

Earlier in March 2018, ICS-CERT issued an advisory about the use of default or hard-coded credentials in GE Healthcare medical imaging software, systems, and workstations, affecting a total of 23 of its products. The advisory said an independent researcher had discovered the use of default or hard-coded credentials by GE Healthcare, which increases the risk that attackers could guess the password to access these systems. GE has produced product updates that are available upon request, which replace default or hard-coded credentials with custom credentials for all but three of the affected products (ICS-CERT, 2018, March 13).

And the advisories continue. Healthcare IT personnel can keep track of the latest advisories, at https://ics-cert.us-cert.gov/advisories.

Working with the Manufacturers

The Food and Drug Administration (FDA) has endured criticism for years for not doing enough to ensure cybersecurity in medical devices. In December 2017, the American Hospital Association recommended that the FDA increase oversight of medical device manufacturers (Thompson, 2017). In a letter to the FDA, AHA Senior Vice President Public Policy Analysis and Development Ashley B. Thompson wrote:

> *"The recent global ransomware attack underscores the cybersecurity risks hospitals and health systems face and the importance of strong cybersecurity protections. More than 200,000 computers in more than 150 countries were infected with the WannaCry ransomware worm, which locked down systems and demanded a ransom payment to have them restored. While this attack was waged against all sectors, the health sector drew attention from the media and federal officials because of the critical nature of the services we provide and the widespread impact of the attack on the United Kingdom's National Health Service. There are reports that WannaCry hit some American hospitals and health systems – and medical devices with embedded, outdated software likely were the vector.*

> *"Thus, this recent ransomware attack highlighted the extent to which medical devices are vulnerable and can create high-risk areas for the security of hospitals' overall information systems. The FDA must provide greater oversight of medical device manufacturers with respect to the security of their products. Manufacturers must be held accountable to proactively minimize risk and continue updating and patching devices as new intelligence and threats emerge. They share responsibility for safeguarding confidentiality of patient data, maintaining data integrity and assuring the continued availability of the device itself. While the FDA has released both pre- and post-market guidance to device manufacturers on how to secure systems, the device manufacturers have yet to resolve concerns, particularly for the large number of legacy devices still in use."*

The FDA has always required that manufacturers report all incidents in which their devices may have contributed to a medical incident or death or have malfunctioned and *could* have contributed to harm or death. However, such reporting is not required to be time-sensitive, and that oversight has led to late-reported incidents and underreporting. There is also no requirement that security vulnerabilities be reported.

It wasn't until 2014 that the agency finally released guidance to the industry for an effective cybersecurity risk management framework for premarket submissions. The guidelines recommended that manufacturers develop a set of cybersecurity controls to ensure medical device cybersecurity and maintain medical device functionality and safety but did not mandate such a move or include any regulatory enforcement (FDA, 2014).

The controls, the FDA wrote, should include risk assessment during the design and development phase of the device, as well as establishing a "cybersecurity vulnerability and management approach" as part of the software validation and risk analysis already required. This includes:

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

The agency extended that guidance with draft cybersecurity guidelines for medical devices released in January 2016. (FDA, 2016) The guidelines recommend that cybersecurity information be provided "throughout a product's lifecycle, including during the design, development, production, distribution, deployment, and maintenance of the device."

The rules also call on companies to have a structured and systematic approach to risk management and quality management systems, including (FDA, 2016):

- Applying the 2014 NIST Framework for Improving Critical Infrastructure Cybersecurity, which includes the core principles of "Identify, Protect, Detect, Respond and Recover"
- Monitoring cybersecurity information sources for identification and detection of cybersecurity vulnerabilities and risk
- Maintaining robust software lifecycle processes that include mechanisms for:
    - Monitoring third party software components for new vulnerabilities throughout the device's total product lifecycle
    - Design verification and validation for software updates and patches that are used to remediate vulnerabilities, including those related to off-the-shelf software
- Understanding, assessing and detecting presence and impact of a vulnerability
- Establishing and communicating processes for vulnerability intake and handling
    - The FDA has recognized ISO/IEC 30111:2013: Information Technology – Security Techniques – Vulnerability Handling Processes.
- Using threat modeling to clearly define how to maintain safety and essential performance of a device by developing mitigations that protect, respond and recover from the cybersecurity risk
- Adopting a coordinated vulnerability disclosure policy and practice
    - The FDA has recognized ISO/IEC 29147:2014: Information Technology – Security Techniques – Vulnerability Disclosure which may be a useful resource for manufacturers.
- Deploying mitigations that address cybersecurity risk early and prior to exploitation

The agency stressed that the majority of steps required to improve device security do not require any advance notification to the FDA. The agency only needs to be informed of the "small subset" of vulnerabilities and exploits that may compromise the essential clinical performance of a device and present a reasonable probability of serious adverse health consequences or death. If the vulnerability is quickly addressed in a way to reduce the risk of harm to patients, the FDA won't enforce urgent reporting of the vulnerability (FDA, 2016).

A FRAMEWORK FOR MANAGING RISK IN HEALTHCARE

The first recommendation for medical device manufacturers above is that they apply the National Institute for Standards and Technology (NIST) Cybersecurity Framework (CSF), which provides a guide for businesses seeking to adopt and implement a robust cybersecurity program. Many cybersecurity firms recommend that hospitals and other healthcare organizations do the same.

In a February 2018 blog, Senior Strategist for Symantec Global Government Affairs, Ken Durbin, wrote: "At first glance, the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) may seem daunting. With 98 subcategory outcomes spread across five

core Functions, each designed to target a specific cybersecurity risk category, the thought of implementing this framework into an established healthcare system could serve as a deterrent. But, it's not as difficult a task as one might perceive, and the benefits far outweigh the repercussions of not having a formal security baseline in place" (Durbin, 2018).

Figure 2: The Core of the NIST Cybersecurity Framework

Source: NIST Cybersecurity Framework. https://www.nist.gov/cyberframework

Focused on risk management, the "core" of the Framework focuses on five elements: identify, protect, detect, respond, and recover—the complete span of experiencing a cybersecurity incident. These are detailed below (NIST, 2014):

- "**Identify**—Develop an organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities. The activities in the Identify Function are foundational for effective use of the Framework. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs. Examples of outcome Categories within this Function

include: Asset Management; Business Environment; Governance; Risk Assessment; and Risk Management Strategy.

- **Protect**—Develop and implement appropriate safeguards to ensure delivery of critical infrastructure services. The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event. Examples of outcome Categories within this Function include: Identity Management and Access Control; Awareness and Training; Data Security; Information Protection Processes and Procedures; Maintenance; and Protective Technology. Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.
- **Detect**—The Detect Function enables timely discovery of cybersecurity events. Examples of outcome Categories within this Function include: Anomalies and Events; Security Continuous Monitoring; and Detection Processes.
- **Respond**—Develop and implement appropriate activities to take action regarding a detected cybersecurity incident. The Respond Function supports the ability to contain the impact of a potential cybersecurity incident. Examples of outcome Categories within this Function include: Response Planning; Communications; Analysis; Mitigation; and Improvements.
- **Recover**—Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident. The Recover Function supports timely recovery to normal operations to reduce the impact from a cybersecurity incident. Examples of outcome Categories within this Function include: Recovery Planning; Improvements; and Communications."

The full framework may be found at: https://www.nist.gov/cyberframework

In the blog mentioned above, Durbin, who focuses on compliance and risk management in the critical infrastructure business sectors, provided the following recommendations from Symantec for healthcare organizations who might be taking the first step in using the NIST Cybersecurity Framework (Durbin, 2018):

- "Create a security controls policy, which provides a high-level description of objectives along with the framework for those impacted.
- Document roles and responsibilities so each team or department knows who is responsible for what aspect of implementation.
- Document standard operating procedures that explain how the different controls should be implemented. They need to be filtered by team and department and document how they should be done, as well as when and what artifacts will be kept once completed.
- Document detailed task lists for each team and department, including who is responsible for each task and when it needs to be done.
- Assign tasks. Standard operating procedures and scripts can be adjusted following the original implementation for future use to improve the process."

The following case study demonstrates how some of the core principles of the NIST Cybersecurity Framework might be used in managing the risk of networked medical devices (Upendra P, Prasad P, Jones G, et al., 2015).

Case Study: Securing Networked Medical Devices

Who: Stanford Children's Health, a 400-bed tertiary care medical center in Palo Alto, California.

Personnel involved: Information technology, information security, materials management, buyers, clinical technology and biomedical engineering, senior leadership, and manufacturers

How long: Seven-and-a-half months

What did they do?

1. **Inventoried network-connected medical equipment** using the hospital's computerized maintenance management system, then exported it into an Excel spreadsheet with details on every piece of equipment including status (active, retired, out for service). Total active equipment: 23,756 devices. All model numbers and model names verified and hospital rounds and audits confirmed the number of devices.
2. **Identified vulnerabilities.** The team contacted every manufacturer and asked for the Manufacturer Disclosure Statement for Medical Device Security (MDS2). Very few manufacturers even responded initially and even fewer understood what the MDS2 was. Some responded with inaccurate information on the devices. This was one of the most time-consuming and frustrating parts of the process.
3. **Mitigated risks.** This included antivirus software installation on devices with Windows operating systems; putting each device through a detailed security process including a thorough review of all manuals; verifying usage in patient areas; ensuring full-disk encryption software that supported AES 128 or 256, operating system patches; and approved user name and passwords authentication. The hospital granted some remote access to manufacturers through a two-step authentication.
4. **Standardized procurement process.** The new process requires collecting the MDS2 in the purchasing packet or during the request-for-information phase, and a review of security features before any purchase.
5. **Developed processes to maintain cybersecurity of devices.** This included cybersecurity upgrades and educating clinical technology and information security on current literature and best practices. The hospital also assigns someone to perform daily checks on cybersecurity updates from the manufacturer, distributors, suppliers, and other resources, and conducts periodic audits to assess the value of connecting medical devices to the hospital network.

Lessons learned:

- Collaboration with different teams is essential.
- It is important to establish strong coordination and communication with nurses and physicians so they will accept and accommodate equipment downtimes and patient monitoring during upgrades and installations.
- It is important to confirm the information presented in the MDS2 by reviewing the equipment performance, security needs, MDS2, and manufacturer-recommended installations during daily team meetings.
- A designated employee should hold daily and weekly follow-up meetings with the manufacturers to speed up the security process.

While in the case study above it is not clear whether the NST Cybersecurity Framework was explicitly used as the guide for the Stanford efforts, the process certainly reflects many of the core elements and categories of the Framework.

REFERENCES

Deloitte Center for Health Solutions. (2013). Networked medical device cybersecurity and patient safety: Perspectives of health care information cybersecurity executives.

Food and Drug Administration. (2014, October 2). Content of Premarket Submissions for Management of Cybersecurity in Medical Devices.

Food and Drug Administration (2016, December 28). Postmarket Management of Cybersecurity in Medical Devices for Industry and Food and Drug Administration Staff.

General Accountability Office. (2012) FDA Should Expand Its Consideration of Information Security for Certain Types of Devices.

Glisson WB, Andel T, McDonald T, Jacobs, M., et al. (2015) Compromising a Medical Mannequin. Americas Conference on Information Systems (AMCIS). Puerto Rico. Available at http://aisel.aisnet.org/amcis2015/HealthIS/GeneralPresentations/5/

Hayes, J. (2017). WannaCry ransomware impact on patient care could cause fatalities. *Engineering and Technology*. https://eandt.theiet.org/content/articles/2017/05/wannacry-and-ransomware-impact-on-patient-care-could-cause-fatalities/

ICS-CERT. (2018, March 29) Advisory (ICSMA-18-088-01). Philips iSite/IntelliSpace PACS Vulnerabilities. Washington, DC: U.S Department of Homeland Security. Retrieved at: https://ics-cert.us-cert.gov/advisories/ICSMA-18-088-01.

ICS-CERT. (2018, March 27). Advisory (ICSMA-18-086-01). Philips Alice 6 Vulnerabilities. Washington, DC: U.S Department of Homeland Security. Retrieved at: https://ics-cert.us-cert.gov/advisories/ICSMA-18-086-01

ICS-CERT. (2018, March 13) Advisory (ICSMA-18-037-02). GE Medical Devices Vulnerability. Washington, DC: U.S Department of Homeland Security. Retrieved at: https://ics-cert.us-cert.gov/advisories/ICSMA-18-037-02

Kaspersky Lab. (2017). Kaspersky Lab Threat Predictions for 2018. Retrieved at: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07164714/KSB_Predictions_2018_eng.pdf

National Institute for Standards and Technology. Cybersecurity Framework. https://www.nist.gov/cyberframework/framework.

O'Brien G, Khanna G. National Cybersecurity Center of Excellence. December 18, 2014.

Ponemon Institute. (2016). The State of Cybersecurity in Healthcare Organizations in 2016. Retrieved at http://business.eset.com/cybersecurity-healthcare-survey/.

Reel M, Robertson J. It's Way Too Easy to Hack the Hospital November 2015. http://www.bloomberg.com/features/2015-hospital-hack/.

Symantec. Addressing Healthcare Cybersecurity Strategically. 2016.

Thompson, AB. (2017, December 7) RE: Docket Number FDA-2017-N-5093, Review of Existing General Regulatory and Information Collection Requirements of the Food and Drug Administration; Proposed Rule (Vol. 82, No. 42506) September 8, 2017. American Hospital Association. Retrieved from https://www.aha.org/system/files/advocacy-issues/letter/2017/171207-let-aha-fda-regulation-device-security.pdf

TrapX Labs. (2015). Anatomy of an Attack: Medjack (Medical Device Hijack). Retrieved at: https://securityledger.com/wp-content/uploads/2015/F06/AOA_MEDJACK_LAYOUT_6-0_6-3-2015-1.pdf

Upendra P, Prasad P, Jones G, et al. (2015). Operationalizing medical device cybersecurity at a tertiary care medical center. *Biomed Instrum Technol.* 49(4):251-258.

Weaver C. (2013, June 13) Patients put at risk by computer viruses. *The Wall Street Journal*. Retrieved at: https://www.wsj.com.

Wirth, A. (2018, February 28) Healthcare cyber security: Is that light at the end of the tunnel? [Web blog]. Symantec. Retrieved at: https://www.symantec.com/blogs/feature-stories/healthcare-cyber-security-light-end-tunnel