DELL EMC

WHITE PAPER
Medical Device Security

ADDRESSING THE EVOLVING THREAT LANDSCAPE OF MEDICAL DEVICE CYBERATTACKS

TABLE OF CONTENTS

CONNECTED MEDICAL DEVICES

A brave new world of Internet of Things (IoT), or Internet of Medical Things (IoMT), is taking shape in healthcare. The industry is experiencing an explosion of connected medical devices, ranging from evermore networked systems within the health system to remote monitoring, wearable, and implantable devices. If anything, the proliferation of medical devices is expected to accelerate, with some reports estimating the market will reach $117 billion by 2020.[1]

Growth is driven by value-based incentives, cost-and-care objectives, digitization, miniaturization, and plummeting technology price points. The promise of connected medical devices sharing data in real time is great. They can play an important role in improving health outcomes, patient experience, provider productivity, and cost efficiencies. In a report issued by Goldman Sachs, researchers estimated that the total savings opportunity of IoMT could reach $305 billion, with chronic disease management representing almost two-thirds of that savings, at $200 billion.[2]

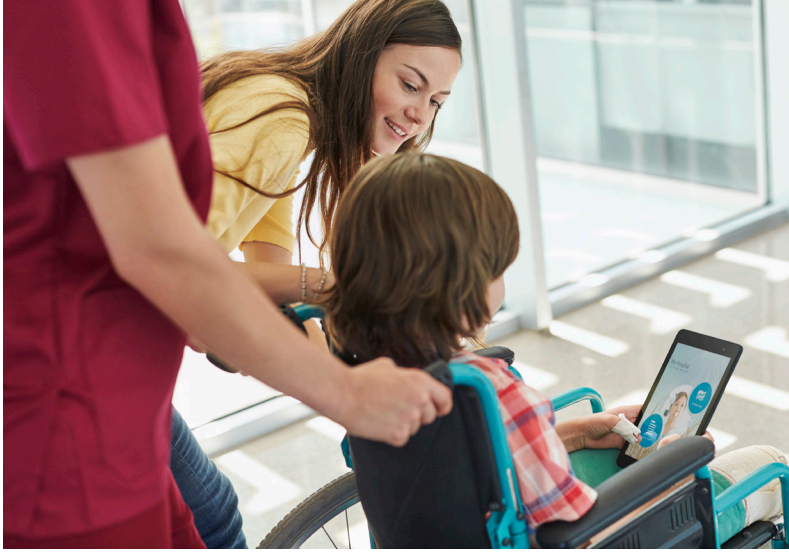
GROWING VULNERABILITY

With increased use of connected devices, however, comes greater vulnerability. Until recently, medical devices were siloed, feeding data to a local screen or monitor and not connected to larger networks. Now, with a growing web of interconnections among devices and systems across multiple networks and with data transmitted across the Internet, the entire health industry—providers, patients, payors, and government agencies—needs to address a rapidly changing threat landscape for cyberattack.

The growing threat of cyberattack in healthcare overall is well documented. As cases such as Hollywood Presbyterian, Medstar Health, and Methodist Hospital show, cyberattacks are increasingly sophisticated and well funded. An astonishing 88 percent of reported ransomware attacks have been targeted at hospitals.[3] Although attacks can often result in an exchange of payment for return of access to intact systems, some hackers are mining for personal health information (PHI). This information is now estimated to be ten times as valuable on the black market as credit-card information.[4]

Medjacking: Beyond data to physical harm

The increased targeting of healthcare systems has even helped coin a new word for these cyberattacks: "medjacking." Medjacking can do more than gain access to a patient's medical records, however. Vulnerabilities in medical devices could be putting patients' health, if not their lives, at risk.



Implantable medical devices (IMDs), for example, such as pacemakers and infusion pumps, could fall prey to malicious hackers who wish to cause harm to a particular person or create chaos for a particular health system.

By taking over control, a hacker can cause a device to malfunction or fail, with serious consequences to the physical wellbeing of the patient. A hack into an IV pump last year, where hackers were reported to have gained access and control over the device, was enough to spur the FDA into action. The agency issued guidelines on medical device cybersecurity in early 2016. Just recently, a Reuters report provided warning from Johnson & Johnson regarding security vulnerabilities in its Animas OneTouch Ping insulin pump, stating that "a hacker could exploit to overdose diabetic patients with insulin, though it describes the risk as low."[5]

Black boxes and weak links

Healthcare organizations face unique challenges in securing data and devices. While other industries are in the process of creating the intelligent, connected "things" in their emerging IoTs, health organizations are already filled with medical devices that operate essentially as special-purpose computers.

Indeed, HIMSS reports that "hospitals and similar healthcare organizations typically have 300% to 400% more medical equipment than IT devices."[6] Most of these devices operate as black boxes using their own specialized software and hardware. Because healthcare IT organizations are typically unaware of the technology stack used in medical devices, these devices do not undergo routine security testing and simulation, and even when IT tests software vulnerabilities in the network, the vulnerabilities of black-box devices remain unknown to IT staff.

Another weak link in the healthcare industry's cybersecurity armor is the wide variety of legacy devices in system networks. These devices can expose organizations through

security vulnerabilities from outdated operating systems, such as Windows XP or NT; a lack of cybersecurity features such as updates, patches, encryption, and protocols; and outdated coding standards. These devices commonly have hard-coded passwords, redundant or unused code bases, and other software vulnerabilities. In addition, most systems have inadequate access controls and weak passwords. Often these legacy devices remain untouched and not updated due to the fear of disrupting workflow.

The human factor

Finally, a culture of security is lacking, which can open a backdoor for hackers to gain access undetected. In general, comprehensive security policies and protocols at all levels, with the proper governance and training, are still rare in the healthcare industry, as many still lack basic security hygiene. It's not unusual, for example, for users to post the username and password on a sticky note on a medical device. A study by Deloitte of European hospitals noted that more than half of those surveyed used medical devices with hard-coded or default passwords.[7]

In addition to improving the security practices within the health system, the growing use of connected, remote, wearable, and implanted devices requires new kinds of oversight and education for home health professionals and patients as well.

GROWING AWARENESS

The good news is that the leaders in healthcare are becoming more aware of risks and vulnerabilities. According to the Harvey Nash / KPMG CIO Survey 2016, CIOs and other IT leaders who believed that their systems can identify and respond effectively to attacks has decreased from nearly one-third in 2014 to one-fifth in 2016.[8]

The bad news is that in a Ponemon Institute study, only 27 percent of IT officials surveyed included medical device security as part of their cybersecurity planning.[9] Limited resources play a part in keeping healthcare organizations from staying on the cutting edge of cybersecurity. Another Ponemon Institute study discovered that only 37 percent of healthcare organizations had "sufficient resources to prevent or detect unauthorized patient data access, loss or theft"[10] for all cybersecurity, not just security related to medical devices.

THE NEED FOR END-TO-END SECURITY

Protecting medical device safety and reducing the risk to healthcare networks, systems, data, and patients require a multilayered approach that goes beyond traditional security hygiene. Security risks must be assessed and addressed at all levels: device, system, network, data, access, education, and governance—across, as well as beyond, the health system (Figure 1).

Device-level security

Cybersecurity at the device level must address all components in the software and hardware stack. In addition to up-to-date patching and configuration management, data encryption on the device itself is a must for data protection and advanced malware protection at the endpoint.

That said, encryption and malware protection on devices pose their own set of unique challenges. Medical devices

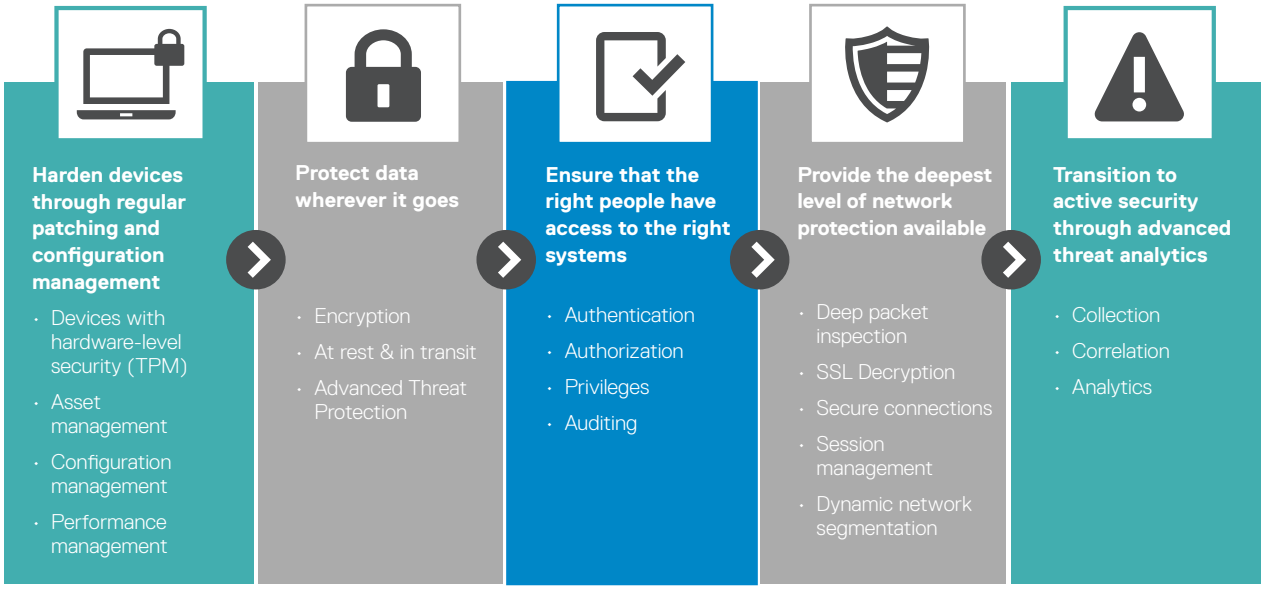


Figure 1: End-to-end medical device security

have varying levels of computing power, and as a result encryption and malware-protection software might adversely impact performance. Selecting the right strategy that is able to balance performance requirements with security is critical. Traditional antivirus software is not enough. Proactive detection methods using machine learning and artificial intelligence are important new capabilities in the security toolbox. Security should also be embedded as part of the software-development life cycle of a medical device. Organizations like the Open Web Application Security Project (OWASP) and the SANS Institute provide guidance on cybersecurity best practices for DevOps.

System-wide security

System-wide security must include the deepest level of network protection available. This includes enhanced perimeter-based protection using next-generation firewalls that can scan every packet of data, including SSL-encrypted traffic and network segmentation to isolate threats and prevent lateral spread within the data center. Technologies such as network virtualization and host-based firewalls can help to protect virtual machines and plug the gaps that traditional network security creates in an increasingly virtualized data center. VPN-based access with multi-factor authentication for remote users and applications further beefs up security for a mobile and connected workforce.

Unfortunately, you can never be 100 percent secure. There are no security measures for unknown and zero-day threats. Therefore, you need to be prepared to detect and respond. Security professionals must continually collect and analyze data and threat intelligence from multiple sources to increase detection and plan effective responses. Even so, gathering and analyzing data from disparate systems and devices, identifying threats, and initiating timely, effective defenses are daunting challenges.

When it comes to securing an IoMT environment, one approach to helping address these challenges is the use of an intelligence gateway or threat intelligence gateway. A fixed-function gateway at the network edge can take on much of the work of continual data gathering, integration, and analysis. It can help identify potential threats and present possible options for how to manage the threat through a dashboard interface, helping security professionals launch a customized response based on the threat and the nature of the target.

In addition to detecting threats, gateways can help manage security protocols. For example, gateways can apply encryption, perform analytics, and provide hardware-level security. They can validate data (ensure data has not been corrupted or compromised and is coming from the correct device) and aggregate data from multiple sources. Once the gateway has analyzed and validated information at the edge, the data can be further screened at back-end firewalls for viruses and other anomalies.

Strategy and governance

Strategy and governance programs are a critical part of inculcating a culture of security.

Best practices, education, and training must be ongoing and based on the following:

- Efficient and timely security updates
- Vulnerability detection and reporting
- Periodic risk assessments and audits
- Forensics and incident-response planning
- Penetration testing and simulations
- Business continuity and resiliency planning
- User authorization and access control
- Continuous threat intelligence and security monitoring
- State of security updates to business leaders

SHARED RESPONSIBILITY

The problem of medical device security is complex, widespread, and growing. To address these challenges, responsibility cannot lie with just any one entity. Device manufacturers, healthcare providers, security experts, patients, and governing bodies must work together on both immediate remediation and longer-term protection.

Device manufacturers

According to FDA guidelines, device manufacturers must remain "vigilant in communicating risks and hazards associated with their devices."[11] HIMSS and NEMA have come together to provide a standardized form for manufacturers to make this communication easier and more efficient. The initiative, called the Manufacture Discloser Statement for Medical Device Security (MDS^2),[12] assists healthcare professionals responsible for security-risk assessment in weighing risks and taking note of specific use-case vulnerabilities for specific devices of interest. For manufacturers, such transparency leads to critical feedback needed to improve the design and testing of new devices as well as more robust life-cycle protocols.

Healthcare providers

The first priority for all healthcare providers is to objectively evaluate both risks and the state of existing security measures across people, processes, and technologies. A gap analysis, comparing the current state to requirements, helps drive action and focuses efforts on making the most critical changes first.

In addition to implementing updates and improvements to close gaps and fortify security procedures and protocols, health systems should move to role-based access controls that automatically limit access to different network levels, systems, applications, and data based on profile authorizations.

Role-based access needs to be supplemented with ongoing education and training for staff at all levels, to help all users understand, recognize, and stay up to date on security threats.

Finally, the establishment of clear policies, procedures, and protocols must be combined with governance and oversight to cultivate a culture of security throughout the health system.

Patients

Patients are becoming active players in the digital healthcare ecosystem. With a rapid expansion in the individual consumer market for connected medical devices—projected to be upwards of $612 billion by 2024[13]—patients must also be educated on security best practices.

In the area of chronic disease management alone, health systems are increasingly connecting to medical devices in the home to help patients monitor symptoms for better health outcomes, lower costs, and fewer in-hospital stays. Because the devices patients use to manage their care and communicate with their care team operate outside of the health system's secure network, government agencies and healthcare providers will need to cooperate in efforts to better regulate the security of devices, make patients aware of security threats, and equip them with proper training and tools to protect their health and medical data.

Governing bodies

Governing bodies are charged with providing industry-wide standards, policy guidelines, and oversight. The FDA, in combination with the US Department of Homeland Security, has established the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT).

ICS-CERT is responsible for reducing the risk of security breaches in "all critical infrastructure sectors."[14] It coordinates efforts between multiple entities, including law enforcement, state and local governments, the federal government and Native American tribal governments, and owners and operators of critical infrastructure sectors.

A recent public service announcement issued by the FBI states, "Patients should be informed about the capabilities of any medical devices prescribed for at-home use…If the device is capable of remote operation or transmission of data, it could be a target for a malicious actor."

Currently, the FDA is recommending that organizations follow the National Institute of Standards and Technology (NIST) cybersecurity framework, which was developed to simplify and standardize network security, while also allowing for customization by individual entities. NIST estimates that 50 percent of US companies will be using the framework by 2020.[15]

The FDA also now requires a unique device identification (UDI) for every medical device and model, with UDIs listed in a public database. The National Committee on Vital and Health Statistics (NCVHS), which is an advisory committee on health information policy to the Secretary of the US Department of Health and Human Services, recently held hearings to identify the benefits and drawbacks of implementing a UDI in administrative healthcare transactions. NCVHS further identified possible improvements to current policies and procedures, as well as possible long-term changes to assist in adoption of UDIs.

Security experts

In addition to governmental oversight, IT cybersecurity experts offer consultation and monitoring for newly emerging security risks posed by medical devices. They can share knowledge gained and techniques developed by other industries, such as the financial sector, which some estimate has a multi-year head start in understanding, developing, and applying cybersecurity measures that enable the delivery of secure services to a variety of consumer devices.

Security experts play an important role as the "white hats," helping to discover vulnerabilities and working with both healthcare providers and device manufacturers to communicate issues and fixes. For instance, the National Health Information Sharing and Analysis Center (NH-ISAC) provides strategies to protect against or minimize the effects of a threat. It provides assistance to all "healthcare stakeholders," including nonprofit and for-profit entities. NH-ISAC members contribute to the exchange of information and its continuing operation. Other healthcare security groups or committees include the "I Am The Cavalry" movement, which has developed a new Hippocratic Oath related to cybersecurity in healthcare and is helping to increase awareness.

MOVING FORWARD

Because of the complexity of the systems and the magnitude of the threat, taking action to address growing vulnerabilities in areas such as medical device cyberattacks can seem overwhelming. As a result, organizations can find themselves stuck in a kind of panicked paralysis, rather than beginning to take purposeful action that can greatly reduce risk.

Fortunately, there are concrete, proven steps healthcare organizations can take to move forward to protect themselves and their patients. One practical tool is a securities capability maturity model (Figure 2) that helps organizations benchmark where they are—and where they need to be—in terms of overall security.

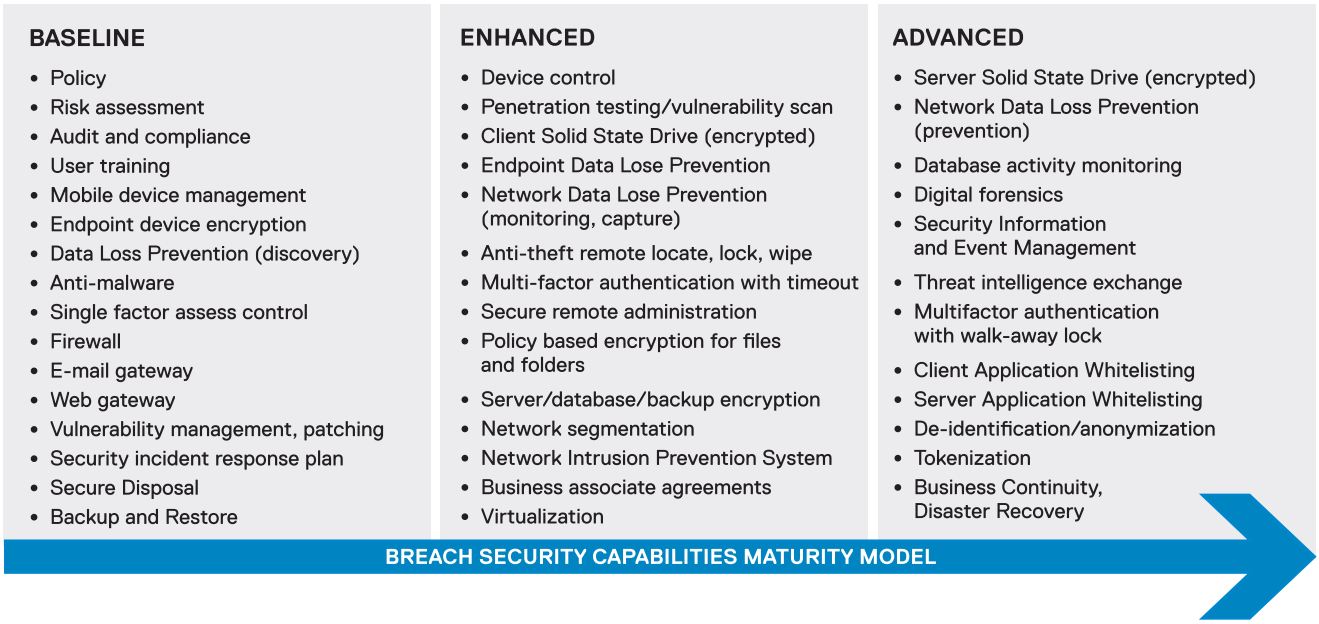


Figure 2: The security capabilities maturity model helps organizations assess their security readiness and provides a systematic framework for them to use to migrate from baseline to advanced.

Dell EMC Healthcare offers proven industry-leading expertise, methodologies, and tools to reduce risk and strengthen security in the healthcare environment. Our cybersecurity experts understand the unique challenges of protecting patients and their data and work with you to devise cost-efficient "secure by design" clinical, operational, and financial solutions that span devices, the network from edge to core, the data center, and cloud.

For more information on developing your organization's security maturity model, visit *Dell.com/healthcare*

1. $117 Billion Market For Internet of Things In Healthcare By 2020. April 22,2015. http://www.forbes.com/sites/tjmccue/2015/04/22/117-billion-market-for-internet-of-things-in-healthcare-by-2020/#4eccf1042471
2. Equity Research, Goldman Sachs Global Investment Research: The Digital Revolution comes to US Healthcare Technology. Internet of Things, Vol. 5 JUNE 29, 2015.
3. The Solutionary Security Engineering Research Team (SERT) Quarterly Threat Report for Q2 2016.
4. Reuters Technology News: Your medical record is worth more to hackers than your credit card. September 24, 2014.
5. Reuters Technology News: J&J warns diabetic patients: Insulin pump vulnerable to hacking. October 4, 2016.
6. http://www.himss.org/medical-device-security
7. Deloitte Medical Device Security Survey: Cyber security of network-connected medical devices in (EMEA) Hospitals 2016.
8. Harvey Nash/KPMG CIO Survey 2016. www.hnkpmgciosurvey.com
9. Ponemon Institute Research Report, sponsored by ESET: The state of cybersecurity in healthcare organizations in 2016. February, 2016.
10. Ponemon Institute Research Report, sponsored by ID Experts: Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data. May, 2016.
11. http://www.fda.gov/MedicalDevices/DigitalHealth/ucm373213.htm
12. http://www.himss.org/resourcelibrary/MDS2
13. Grand View Research Report: Connected Health and Wellness Devices Market Worth $612 Billion by 2024. August 2016.
14. https://ics-cert.us-cert.gov/
15. https://www.nist.gov/cyberframework