Securing the Future of Care: *Trustworthy Connected Medical Devices*

Capgemini

Securing medical devices requires specialized knowledge of hardware, firmware, and software engineering coupled with a deep understanding of cybersecurity, the healthcare industry and applicable regulation.

Medical devices are becoming more connected than ever and devices that are not well protected can lead to exposure of personal health data and deterioration in the efficacy of the device's function, potentially resulting in loss of life in extreme cases. Medical device manufacturers (MDMs) are therefore under constant pressure to protect their devices against vulnerabilities, and they are complementing their traditional approaches to safety and reliability with cybersecurity measures across the entire lifecycle of the product. However, this journey is not expected to be easy and manufacturers will have to tackle numerous complexities along the way.

Navigating the complexity of medical device security: Risks and vulnerabilities

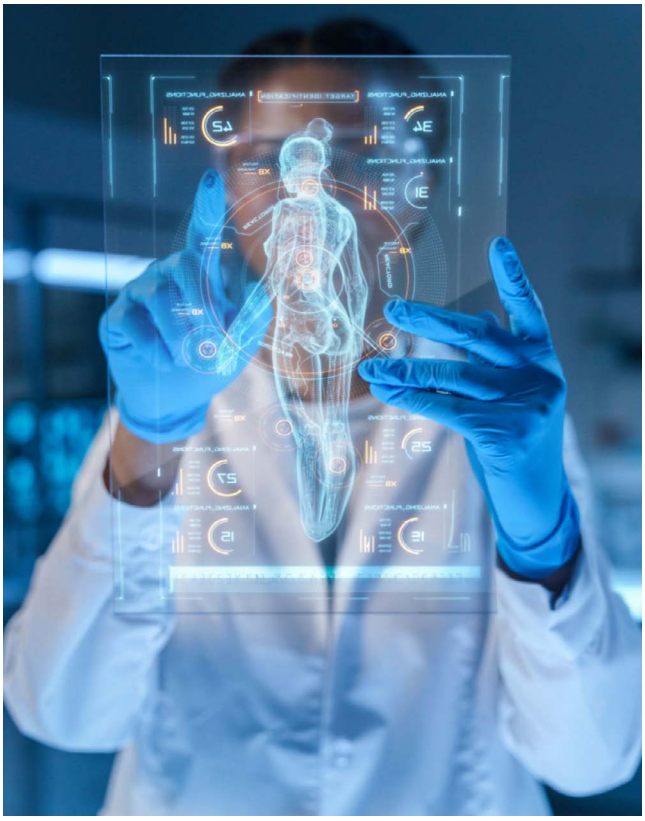
The healthcare sector has always been at the forefront of embracing newer technological advances. Medical devices are becoming increasingly interconnected and advanced; this is revolutionizing patient care and diagnostic processes. Newer technologies like AI and machine learning (ML) have been used by medical professionals for analyzing vast amounts of data and for continuous learning, thereby improving the efficiency and performance of diagnosis and clinical processes. Advances in connectivity using technologies like 5G have reduced latency and bandwidth challenges enabling medical professionals to consult and even perform surgeries remotely.

As these newer technologies make inroads into medical devices, attackers are finding ways to exploit vulnerabilities in these technologies and ultimately compromise the devices. ***A recent survey*** found that healthcare organizations with a higher percentage of connected medical devices suffer more cyberattacks with nearly half (48%) of healthcare cyberattacks impacting patient care, and two in three (67%) affecting patient data. The healthcare sector has also long been a target for ransomware attacks from cybercriminals and Ransomware-as-a-Service affiliates and operators. As per the FBI's ***Internet Crime Complaint Center (IC3) annual report 2023,*** healthcare was the most impacted sector with more than 250 reported ransomware attacks in 2023.

Medical devices also store and process sensitive patient data that include protected health information (PHI) like personal details, medical conditions, and care information. It is imperative for MDMs to safeguard patient privacy and secure data from potential misuse, unauthorized access, and data breaches. Attackers can misuse protected health information for various purposes including committing fraud, impersonation, and tampering with medical records. ***Healthcare data breaches*** in the United States hit an all-time high in 2023 with more than 133 million patient records breached, more than double the number in 2022 (51.9 million).

With increased reliance on ***software,*** newer medical devices are increasingly the target of cyberthreats that exploit vulnerabilities and weak

configuration in software that results in risks to patient safety, privacy, and the integrity of devices. ***A recent report*** on healthcare security found that 63% of key exploitable vulnerabilities (KEVs) tracked by the Cybersecurity and Infrastructure Security Agency (CISA) can be found on healthcare networks, while 23% of medical devices have at least one known exploited vulnerability. Many of these vulnerabilities were found in imaging workstations, clinical IoT devices, picture archiving and communication systems (PACS), and medical data systems. This has led to a substantial increase in advisories and notifications issued by federal agencies like the US Food and Drug Administration (FDA) and CISA to organizations on vulnerabilities in various hardware and software components impacting several medical devices. Software ***supply chain*** security is another big concern for both the federal government and regulatory bodies. Modern-day medical devices – be they Software-as-a-Medical-Device (SaMD) or devices that contain software including firmware or programmable logic controllers – are increasingly relying on components



that consists of various commercial, third-party, and open-source code. Vulnerabilities in these software components can pose major risks to the safety and integrity of a medical device. Regulatory bodies and federal agencies have made MDMs accountable for ensuring that software used in their devices is secured against any emerging threats.

Many of the devices in the healthcare sector still rely on ***legacy devices*** that operate on outdated software. These devices are being used even beyond the manufacturer's intended and prescribed shelf life. Some of the security controls applicable to modern medical devices cannot be applied to these legacy devices. ***A recent survey*** has found that 14% of the connected medical devices operated on unsupported operating systems. Of the unsupported devices, 32% are imaging devices, including X-ray and MRI machines.

With the evolving nature of cyberthreats, MDMs are also faced with the problem of digital skill shortage due to the lack of experts and practitioners who can effectively address security for their products. Addressing cybersecurity for medical devices requires knowledge of both the medical domain and cybersecurity. This can be challenging for traditional software and hardware engineers who find it difficult to bridge the gap between these two domains of different natures. Also, regulatory experts in the healthcare sector who are traditionally accustomed to addressing safety risks using traditional fault tree analysis or failure modes and effects analysis (FMEA) methods are still learning to effectively identify cybersecurity risks that are influenced by confidentiality, integrity, and availability requirements on the device.

The diverse nature of medical devices with different technology stacks also makes it difficult for regulatory bodies to issue specific guidelines and requirements that can cater to each type or category of medical device. Regulation is therefore generic in nature and that leaves manufacturers to have their own interpretation of regulatory guidelines and to incorporate controls that may not be fully effective but just sufficient to address compliance.

Building a foundation of security: Strategies for MDMs

Healthcare manufacturers are trying to find a balance between making healthcare more patient-focused and maintaining patient safety. Any vulnerability exploited by attackers that impacts patient safety or data security can result in manufacturers facing regulatory actions that can include fines, recalls, or device usage restrictions.

To secure medical devices and ensure privacy in these devices, a comprehensive and planned strategy is needed. MDMs need to take a proactive approach rather than a reactive approach. They need to focus on training their employees (management, quality assurance, and engineers) on cybersecurity best practices, conducting regular security assessments to minimize security risks, and embedding security as part of their lifecycle processes.

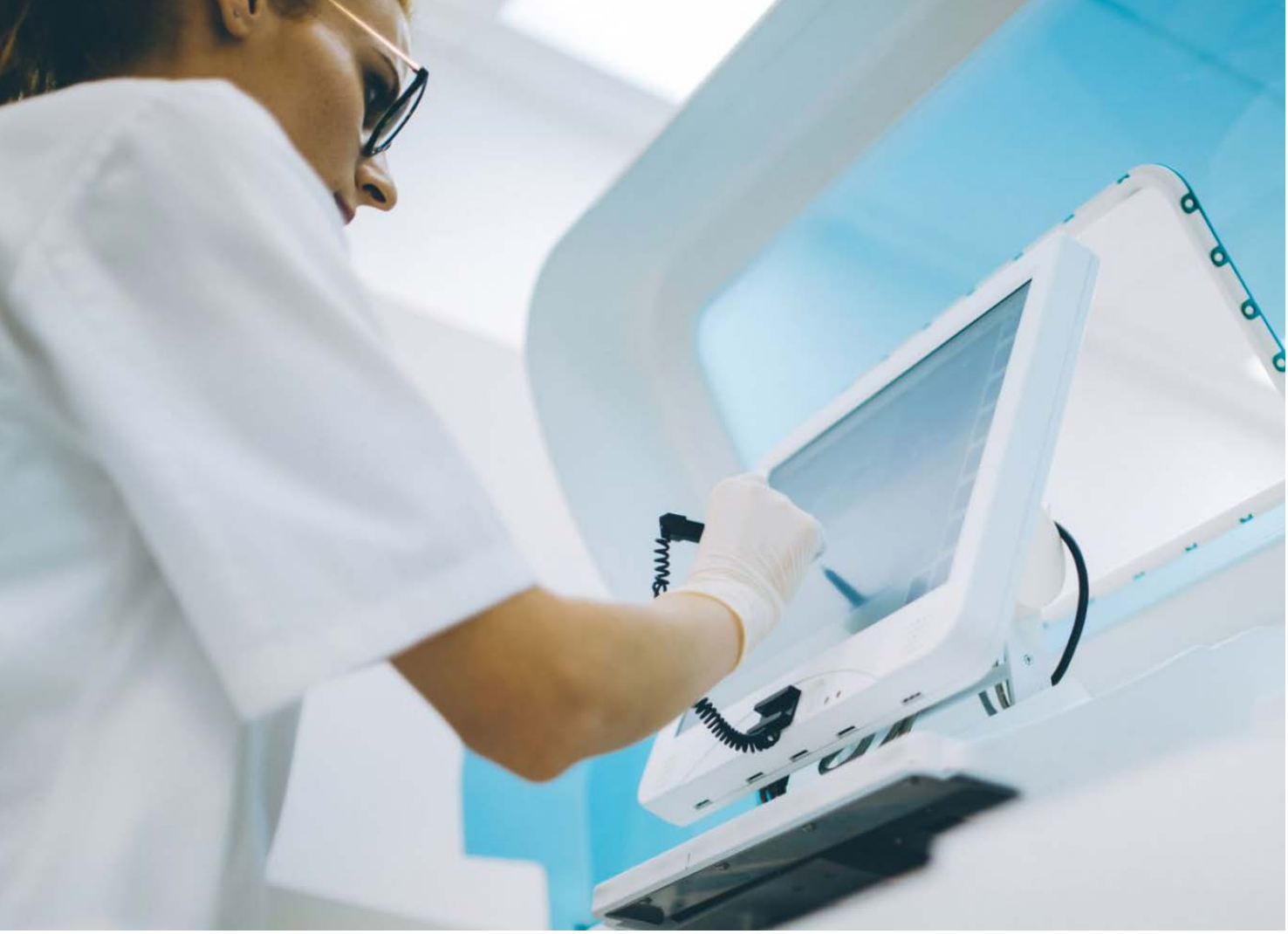
Key foundational approaches that need to be considered as part of such a strategy include:

Product lifecycle security:

MDMs need to integrate security in all phases of the product lifecycle from conception to delivery and post-market operations. Security should be baked into the product development process and should not be an afterthought. Organizations need to embrace lifecycle security approaches guided by principles defined in various internationally accepted standards and should avoid bolted-on approaches. Various standards, guidelines, and frameworks offer secure software development practices that need to be integrated into software development lifecycle (SDLC) models. For example, the FDA recommends the implementation of a Secure Product Development Framework (SPDF): a set of processes that reduce the number and severity of vulnerabilities in products throughout the Total Product Lifecycle (TPLC). The National Institute of Standards and Technology (NIST) in the US has the Secure Software Development Framework (SSDF), which defines secure software development practices and tasks for software producers. Organizations can also refer to secure lifecycle practices defined in standards used in other sectors like IEC 62443 4-1 or ISO/SAE 21434.

Risk management:

Existing risk management frameworks used by MDMs do not consider cybersecurity explicitly and are more focused on safety aspects. Organizations should develop a holistic risk management framework that includes cybersecurity besides safety risks to offer a comprehensive risk management framework. Foundational frameworks like ISO 14971 need to be complemented with standards that address security aspects like AAMI TIR57. Risk management that includes cybersecurity risk evaluation and mitigation should be applied across the entire product lifecycle including development, testing, manufacturing, and post-market activities.



Regulations and standards:

As regulatory bodies like the US Food and Drug Administration (FDA) and the European Union Medical Device Regulation (EU MDR) mandate similar cybersecurity requirements to be met for premarket submissions, it is important for MDMs to have a harmonized quality management system (QMS) process and procedures that align with key requirements from various regulatory bodies in key markets (US, EU). The US regulatory body FDA mandates manufacturers to have processes in place for the secure design and development of medical devices, along with processes and procedures to monitor and patch post-market cybersecurity vulnerabilities.

Privacy:

MDMs need to protect the privacy of data, including patient health information in accordance with various local and regional regulations (GDPR, CCPA, HIPAA). Privacy aspects should consider how data is stored, transmitted, and disposed. Manufacturers need to incorporate privacy by design principles and implement key controls like data encryption at rest, access control, and secure disposal to ensure the protection of data privacy.

Regular assessment:

To identify and mitigate security vulnerabilities in software and hardware, manufacturers need to undertake regular security assessments and penetration testing. Security vulnerabilities in coding need to be identified using static code analysis and mitigated using secure coding practices. Vulnerabilities in operating systems, libraries, and configurations in network-connected devices need to be regularly identified using network-based active scanning tools.

Secure by design:

Manufacturers need to incorporate secure by design principles that include enforcing strict access control mechanisms to prevent unauthorized access to devices and data. Manufacturers also need to have the right controls to ensure data during transit and storage are secured using encryption. These controls need to be based on the network capabilities, data storage, and transmission features. To minimize risks due to compromise in hardware, manufacturers need to augment software security measures with physical security measures that include secure enclosures, access control mechanisms, and tamper-resistant seals.

Software bill of material (SBOM):

The FDA now mandates manufacturers of all "cyber devices" to provide an SBOM in a machine-readable format, with an inventory of all commercial, open-source, and off-the-shelf components, as part of the pre-market review process. Manufacturers need to provide an assessment of the various vulnerabilities in the software components listed in the SBOM along with the current level of support and the support end date. The recent executive order (EO) 14028 has emphasized the need to include best practices for software supply chain security as part of product security.

Security in hardware:

To design devices resistant to cyberattacks, manufacturers are also encouraged to offload security operations to hardware leveraging hardware crypto modules, Trusted Platform Module (TPM) and trust zones that are supported in most modern-day hardware.

Legacy Devices:

To mitigate risks to patients from legacy devices, manufacturers are advised to follow guidance from the International Medical Device Regulators Forum (IMRDF) on applying total product lifecycle (TPLC) to legacy devices. The recommendations include effective communication and implementation considerations for MDMs and health care providers (HCP) and the implementation of compensating controls after the end of support.

Training:

Manufacturers should foster a culture of regular cybersecurity training programs for staff members in different roles. For example, training for software developers should focus on topics like secure coding and static code analysis, and training for quality assurance specialists should cover compliance documentation and risk assessment.

Charting the course for secure and innovative medical devices

In an increasingly connected healthcare ecosystem, MDMs are under increased pressure to offer commitment to their customers on delivering patient safety and protection for personal data. With technology making faster inroads into healthcare and medical devices becoming more advanced, cybersecurity needs to be interwoven with traditional safety measures. This demands an increased collaboration and synergy between traditional risk management and new-age cybersecurity iteratives. Organizations need to adopt security across product lifecycles based on guiding principles from various industry-accepted standards to strengthen their defenses against cyberattacks and to maintain continuity of care.

Authors

Kiran Gurudatt
Director,
Cybersecurity
Cloud Infrastructure Services
kiran.gurudatt@capgemini.com

Aarthi Krishna
Global Head,
Intelligent Industry Security
Cloud Infrastructure Services
aarthi.krishna@capgemini.com

About Capgemini

Capgemini is a global business and technology transformation partner, helping organizations to accelerate their dual transition to a digital and sustainable world, while creating tangible impact for enterprises and society. It is a responsible and diverse group of 340,000 team members in more than 50 countries. With its strong over 55-year heritage, Capgemini is trusted by its clients to unlock the value of technology to address the entire breadth of their business needs. It delivers end-to-end services and solutions leveraging strengths from strategy and design to engineering, all fueled by its market leading capabilities in AI, cloud and data, combined with its deep industry expertise and partner ecosystem. The Group reported 2023 global revenues of €22.5 billion.

Get the future you want | www.capgemini.com

GIS_042024_SC

Copyright © 2024 Capgemini. All rights reserved.