Implementing Secure by Design Principles to Protect Against Cybersecurity Threats in Medical Devices

Dr. Jackie Kunzler

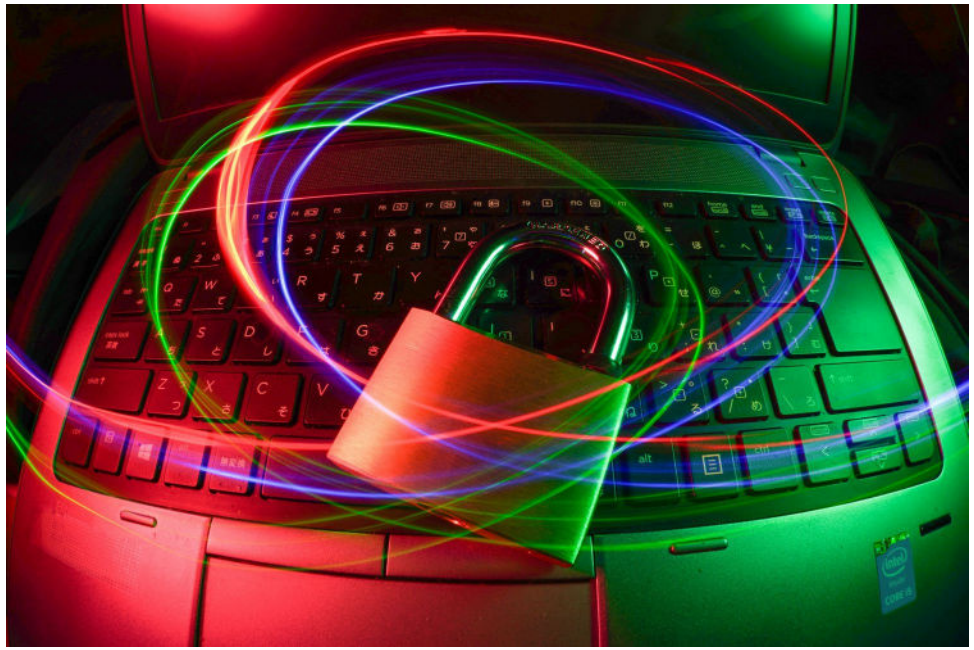
June 4, 2025

European Medical Device Summit

TERUMO

Agenda

- What Is Cybersecurity
- Types of Cybersecurity
- Why it Matters
- Security By Design
- Application to Medical Devices
- Lifecycle Management and Legacy Products
- Useful References



What is Cybersecurity and Why Do We Care?

Cybersecurity is the practice of protecting computer systems, networks, and data from unauthorized access, misuse, damage, or destruction. It encompasses a broad range of technologies, policies, and practices designed to safeguard information assets from various cyber threats.

Cybersecurity is crucial for protecting individuals, businesses, and critical infrastructure from the growing threat of cyberattacks. These attacks can result in financial loss, reputational damage, disruption of operations, and even physical harm.

Types of Cybersecurity

- **Network Security:** Protecting the infrastructure that connects devices and systems.
- **Cloud Security:** Securing data and applications hosted in the cloud.
- **Endpoint Security:** Protecting individual devices like computers and smartphones.
- **Mobile Security:** Securing mobile devices and applications.
- **Internet of Things (IoT) Security:** Protecting connected devices and their data.
- **Application Security:** Securing web applications and their underlying systems.
- **Identity and Access Management (IAM):** Managing user access and permissions to systems and data.
- **Data Security:** Protecting data from unauthorized access, use, or disclosure.
- **Physical Security:** Protecting physical infrastructure like data centers and servers.

Types of Cybersecurity Threats

1. Malware: Malicious software designed to infiltrate and damage systems, including viruses, worms, and Trojans.

2. Phishing: Deceptive emails or messages designed to trick users into revealing sensitive information like passwords or credit card details.

3. Social Engineering: Exploiting human psychology to manipulate individuals into divulging confidential information or performing actions that compromise security.

4. Man-in-the-Middle (MitM): Attacks Intercepting communications between two parties to steal data or impersonate one of them.

5. Denial-of-Service (DoS) Attacks: Overwhelming a system or network with traffic to make it unavailable to legitimate users.

6. Ransomware: Malicious software that encrypts a victim's data and demands payment for its release.

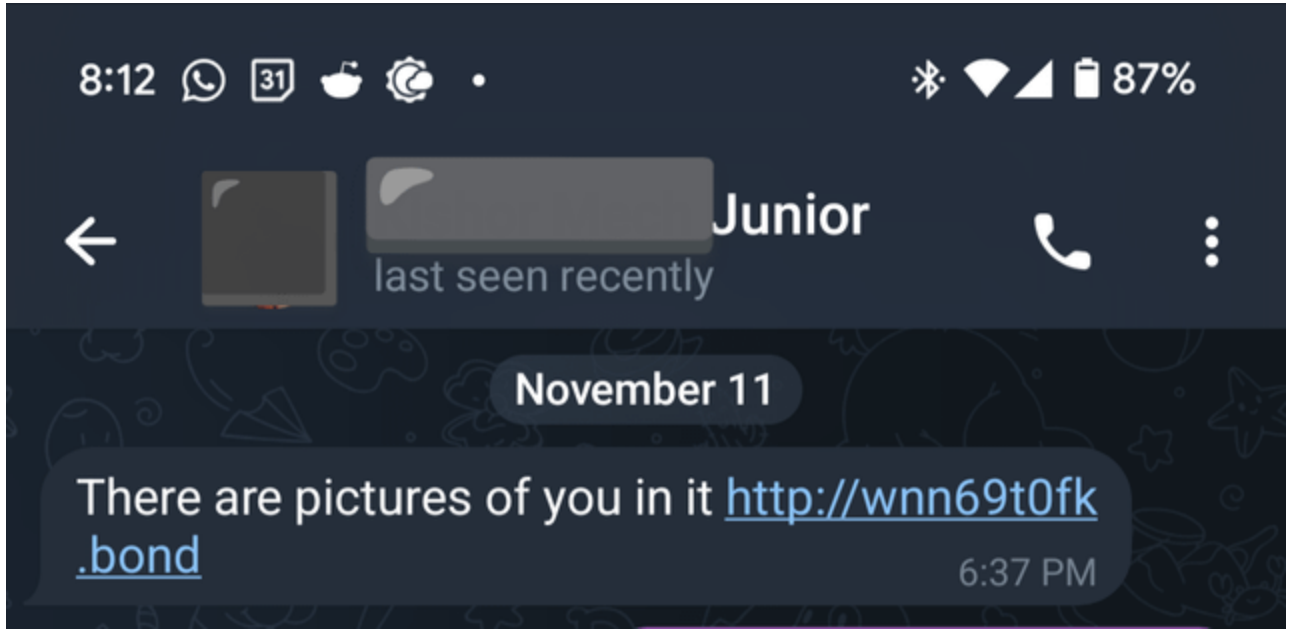
7. Advanced Persistent Threats (APTs): Sophisticated cyberattacks that can remain undetected on a system for extended periods, stealing data or compromising security.

8. Insider Threats: : Security breaches caused by authorized individuals, either intentionally or unintentionally.

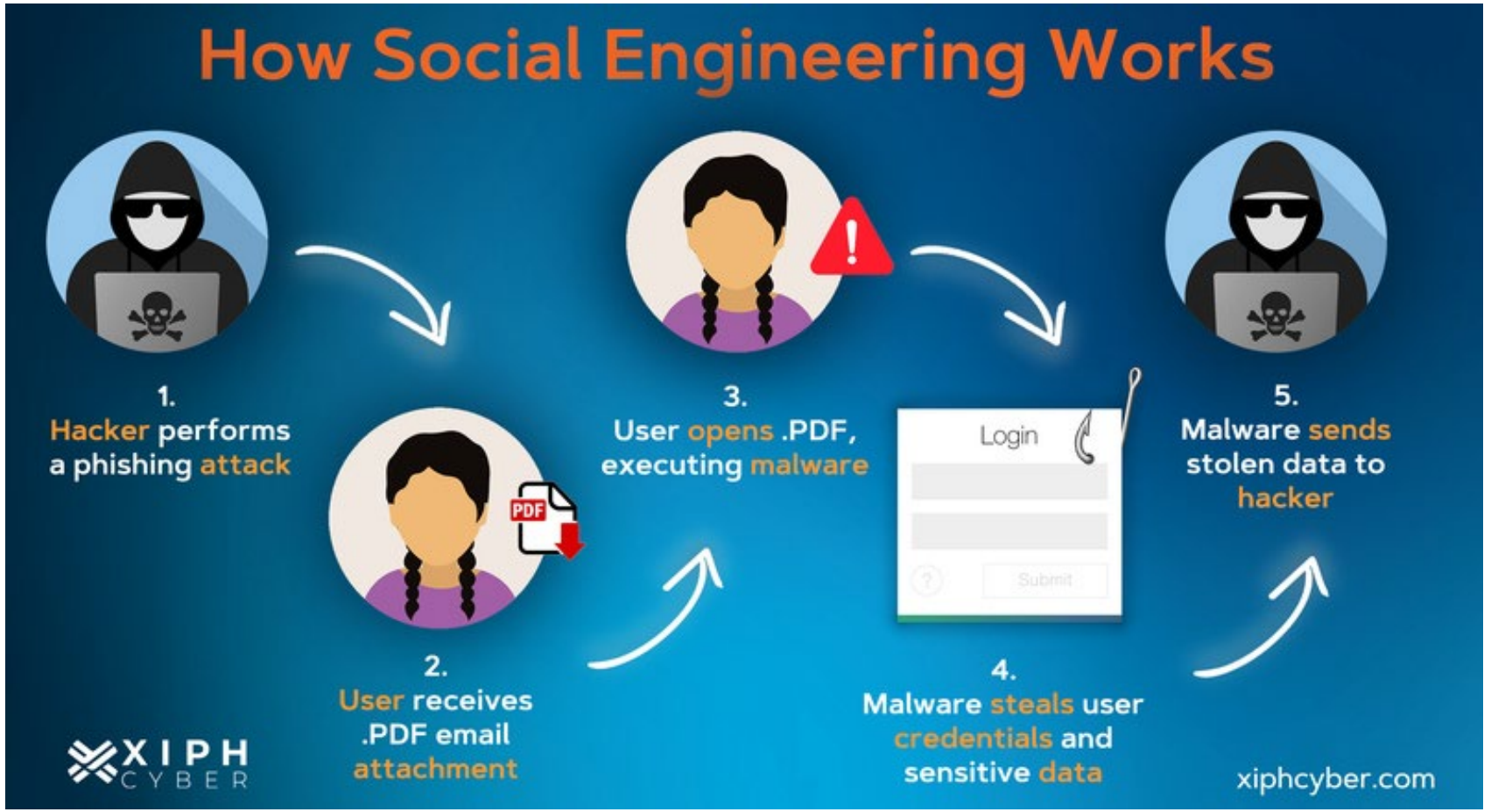
9. Data Breaches: Unauthorized access to sensitive data, often resulting in the theft or exposure of confidential information.

10. Cloud Security Threats: Attacks targeting data, applications, and services hosted in the cloud, including data breaches, system vulnerabilities, and identity theft.

Phishing



Social Engineering



What Makes Medical Devices so Challenging?

- Long Lifecycles
- Significant Number of Interconnections
- Impact on Patient Safety
- Evolving Regulatory Requirements
- Relatively slow development cycles so the “patch” mentality that works in other industries is not fast enough

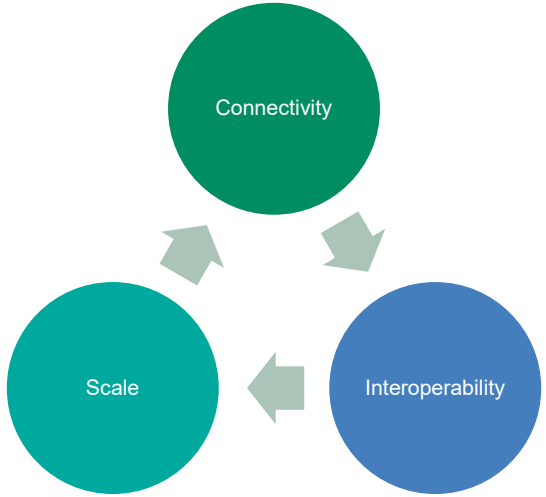
Increasing Importance of Cybersecurity

Increased usage of connected and interoperable care devices are rapidly expanding the threat landscape and attack surfaces

- 7 million Internet of Medical Things (IoMT) deployed at Healthcare Delivery Organizations as of 2026

- Typical US hospital has between 10 and 15 medical devices per bed, excluding lab equipment
  - 63% of the vulnerabilities in the (CISA) Known Exploited Vulnerabilities (KEV) Catalog can be found on healthcare networks.

  - 14% of medical devices are running an unsupported or end-of-life operating system



➢ ***Collaboration between Medical Device Manufacturers and Healthcare Delivery Organizations is essential for maintaining and improving security across the ecosystem***

[1] IoMT devices in smart hospitals to exceed 7M by 2026
[2] 63% of Known Exploited Vulnerabilities Can be Found in Hospital Networks

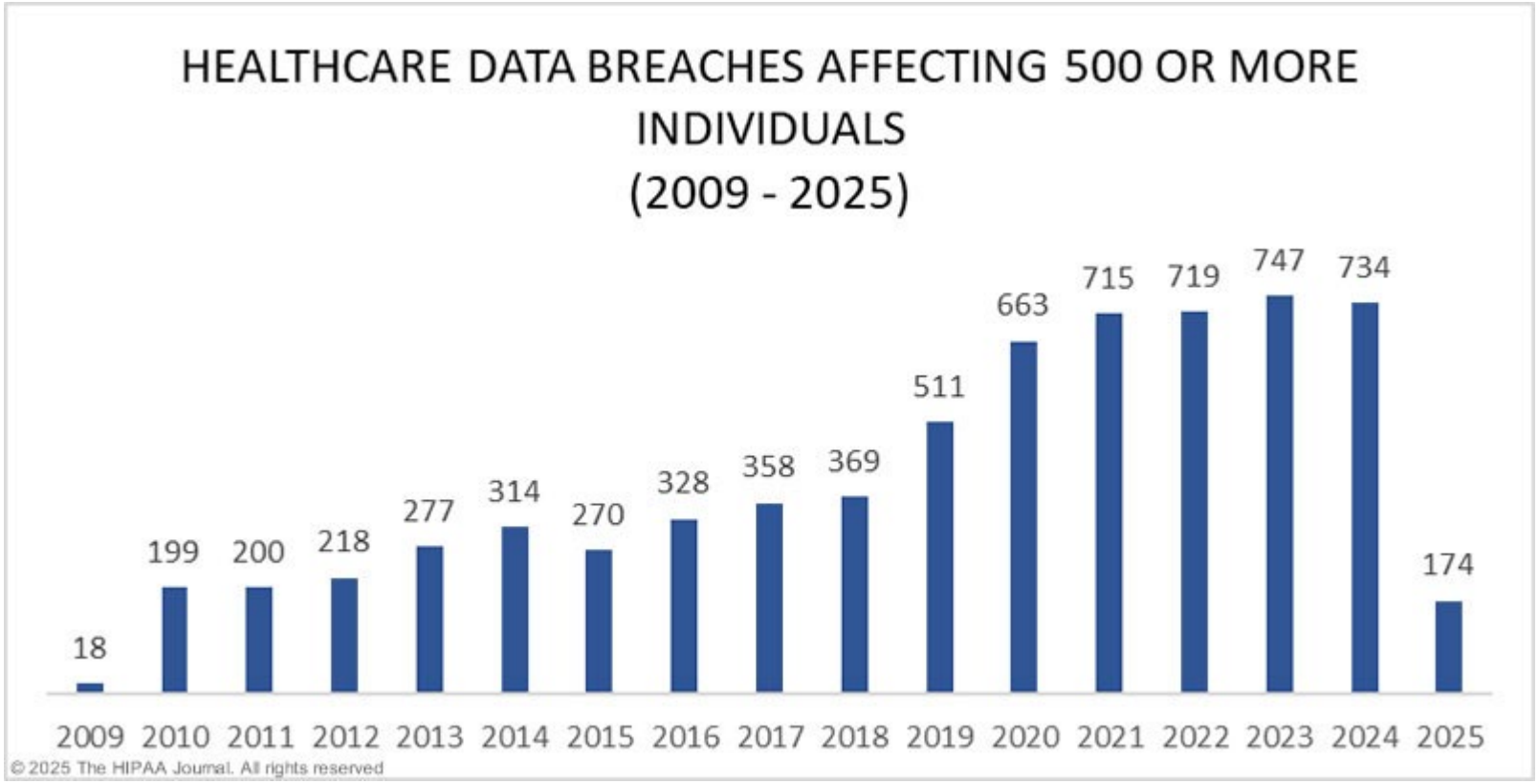
Why Security by Design Matters

Lurie Children's Hospital[1]

792k patients affected
3.5 months to restore access

Change Healthcare[2]

190,000,000 individuals affected
Care delivery and financial consequences



[1] January 2024 Cyberattack on Lurie Children's Hospital Affects 792K Individuals
[2] Change Healthcare Cyberattack Underscores Urgent Need to Strengthen Cyber Preparedness for Individual Health Care Organizations and as a Field | AHA
[3] Healthcare Data Breach Statistics

Security by Design Principles

Products designed with Secure by Design principles prioritize the security of customers as a **core business requirement**, rather than merely treating it as a technical feature.

Applying Secure Design Principles - FasterCapital

Medical Device and Software Product Security

Effective cybersecurity starts in design and extends through the useful life of the product

Pre-Market Activities

- Secure-by-design
- Privacy by design
- **Threat modeling**
- **Penetration testing**

Post-Market Activities

- Threat Intelligence Monitoring
- Vulnerability Management
- **Patch Management**
- Coordinated Vulnerability Disclosure

Customer Information

Manufacturer Disclosure Statement for Medical Device Security (MDS^2)

As processes mature, shift efforts to the pre-market side of the process

Vulnerabilities and Mitigations-Medical Devices

Vulnerability	Mitigation
Login	Changing Passwords, characters, lockouts etc
Stored Data	Authentication and Encryption
Data in Transit	End to End Encryption
Device Firmware	IEC 62304, PEN Testing, Encryption

Incorporating cybersecurity at the start of the product lifecycle

Design for security	• Adopt a threat-risk methodology • Harden device and incorporate security capabilities • Create secure by default configuration
Design for the product lifecycle	• Understand the expected device lifecycle • Consider hardware, CPU, and OS supportability cycle differences • Make frequent software maintenance (patching) automatic or easy
Implement secure software development lifecycle (SDLC)	• Adopt a secure SDLC framework and measure conformance • Implement security testing in each phase (static, dynamic, SCA) • Remediate vulnerabilities and security risks during development
Implement secure product lifecycle	• Monitor emerging threats, vulnerabilities, and EOM/EOS • Release regular, timely security updates • Implement coordinated vulnerability disclosure (CVD)

Stages of Device Cybersecurity Lifecycle Management

- Design and Development-Secure by Design, Secure by Default, Secure by Demand Principles
- Production and Distribution-Preventing Tampering
- Deployment and Maintenance-Software updates, vulnerability patching, threat monitoring
- End of Life-Secure decommissioning and disposal eliminating all data

Key Development Tenets:

- Compliance to Legal, Regulatory and Industry Standards (HIPAA, GDPR, CCPA, CISA)
- Integrating Security Requirements Analysis, Design and Architecture, Secure Coding, Testing, Monitoring and Incident Response procedures
- Utilizing Code Reviews, Assessment Tools, Penetration Testing and Regular Audits to Challenge the System

Legacy Device Cybersecurity Conundrum

Medical device manufacturers and healthcare organizations have to work together to manage cyber threats

- Hundreds of thousands of on-market devices that are decades old
- Because devices are still able to run, appetite for replacement is low
- Lack of inventory/traceability of connected devices at medical institutions
- Mismatches between hardware (OS), software, and cybersecurity evolution
- New cybersecurity patches can shut down interoperability

Strategies for Healthcare Organizations to Deal with Legacy Devices

- Define a Risk Management Strategy
- Define a Lifecycle Management Plan (including EOL and EOS)
- Establish a Coordinated Vulnerability Disclosure Program
- Network Segmentation of vulnerable devices
- Deploy Security Monitoring Tools
- Limit Access to Systems based on roles
- Use firewalls and other intrusion controls
- Use AI-driven anomaly detection and zero-trust security models

Key Takeaways

Design for the lifecycle

- Understand the expected useful life
- Defined lifetime and lifecycle stages
- Make future software upgrades easy

Regular Monitoring and Response

- Monitor software (open source, off the shelf, and in-house) and hardware for vulnerabilities
- Have a response plan in place
- Proactive plan for updates and upgrades

Proactively define responsibilities

- Ensure ownership of security on all sides
- Pre-plan processes for upgrades and patching
- Regular disclosure and communication

References

Guidance and Regulation to support effective implementation

Secure By Design https://www.cisa.gov/sites/default/files/2023-10/SecureByDesign_1025_508c.pdf

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

Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities https://csrc.nist.gov/pubs/sp/800/218/final

IEC 81001-5-1 IEC 81001-5-1:2021 - Health software and health IT systems safety, effectiveness and security — Part 5-1: Security — Activities in the product life cycle

Regulation (EU) 2017/745 (EU MDR) EUR-Lex - 02017R0745-20250110 - EN - EUR-Lex

Regulating medical devices in the UK Regulating medical devices in the UK - GOV.UK

Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions Guidance for Industry and Food and Drug Administration Staff September 27, 2023. Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions

Thank You!