An Infographic

Internet of Medical Things (IoMT) Cybersecurity Readiness

ecfirst | Culinda

IoMT Facts: FBI

- The number of IoMT devices is projected to grow to 50 billion in 2020.
- Deficient security capabilities, legacy operating systems, difficulties in patching vulnerabilities and a lack of security awareness are significant risks to both IoMT devices themselves and the networks to which they connect.
- Unsecure or poorly secured IoMT devices can leave networks open to Distributed Denial of Service (DDoS) attacks.

Source: FBI Alert I-101717a-PSA

Explosion of IoMT devices increases pressure for significantly improved cyber defense against incursions that threaten patients and cause costly disruptions

Myth	Fact
The FDA is the only federal government agency responsible for the cybersecurity of IoT devices.	The FDA works closely with other federal government agencies, such as the U.S. Department of Homeland Security (DHS), but also works with members of the private sector, IoMT device manufacturers, healthcare delivery organizations, security researchers, and end users to increase the security of critical cyber infrastructure.
IoMT device manufacturers can't update IoMT devices for cybersecurity.	IoMT device manufacturers can always update a IoMT device for cybersecurity. In fact, the FDA does not typically need to review IoMT device updates implemented solely to strengthen cybersecurity.
The FDA tests IoMT devices for cybersecurity.	The FDA does not conduct premarket testing for medical products. Testing is the responsibility of the medical product manufacturer.

Number of IoMT devices in a hospital can be more than twice the number of traditional networked devices, such as laptops and smartphones

IoMT Business Risks

- Disruption of patient care.
- Loss of Protected Health Information (PHI) and Personally Identifiable Information (PII).
- Loss of revenue.

Asset management of IoMT devices is typically incomplete

Dept. of Homeland Security issued 30 advisories about cybersecurity vulnerabilities in IoMT devices

IoMT Cybersecurity Services

Identify IoMT Devices Asset Management

Categorize IoMT Devices

Prioritize IoMT Device Cyber Risk

Remediate Anomalies

Assess IoMT Device HIPAA Compliance

Policy Ensure Policy Developed to Appropriately Secure Devices

Process Procedures Aligned with Policy to Ensure Consistent Configuration of Devices

Evidence Implementation Verified to Validate Process for Securing IoT Devices

Measure and Monitor IoMT Device Security Framework Effectiveness

IoMT devices typically run legacy operating system with known vulnerabilities waiting to be exploited

Readiness Assessment

The ecfirst IoMT cybersecurity report includes an asset inventory, which identifies specific IoMT device information such as:

- IP Address
- Hostname (if resolvable or successfully authenticated)
- Operating System (if discoverable or successfully authenticated)
- Open Ports
  - Potentially Active Services
- Installed Software

Healthcare organizations typically have minimal visibility into managing and monitoring IoMT devices

IoMT Cybersecurity Checklist

- **Cybersecurity Framework** Determine the cybersecurity framework that will establish the foundation for your security program requirements for IoMT devices.
- **Policy** Develop a cybersecurity policy specific to IoMT devices. Ensure the policy is reviewed by associated and impacted departments/business units, approved by senior leadership, and communicated to the workforce.
- **Security Risk Assessment** Ensure IoMT devices are within the scope of enterprise cybersecurity risk assessment exercises. Perform a vulnerability assessment to determine IoMT device security gaps. Examine the security architecture and identify opportunities to possibly segregate IoMT devices (i.e. determine application of segregation for IoMT devices).
- **Business Associate Agreements (BAA)** Review third-party vendors (business associates) and their security practices to ensure HIPAA, FDA, and other mandates are appropriately addressed.
- **Configuration Management** Ensure each type of IoMT device is configured consistently, and addresses the appropriate security capabilities to secure PHI and PII.
- **Encryption** Examine options to encrypt PHI and PII stored, processed or transmitted by IoMT devices.
- **Risk Management** Based on the findings of the risk assessment, establish a plan for risk management of IoMT devices. Ensure formal remediation is performed on a regular schedule (e.g. monthly).

60% of IoMT devices are at end-of-life stage, with no patches or upgrades available

IoMT devices in use by hospitals and other healthcare organizations average 20+ years of use per device, making them prime hacker targets

Bottomline

Lack of IoMT device cybersecurity = patient safety risk

Lack of IoMT device cybersecurity = disruptive business risk

Challenge Every hospital and health system must improve its cyber capabilities to monitor and manage IoMT devices to ensure patient life is not threatened and healthcare operations are not disrupted.

Solution AI-based Culinda provides deeper visibility and integrated capabilities to mitigate by continuously monitoring and managing IoMT devices.

Gartner predicts that by 2020, more than 25% of cyberattacks in healthcare delivery organizations will involve the IoT

15-20 connected IoMT devices in a typical hospital room, and an average of 6.2 vulnerabilities on each IoMT device

Kris Laidley | Kris.Laidley@ecfirst.com | www.ecfirst.com

Reimagining Cyber Defense

Code: MEDIoTIG0008