IMDRF/DITTA Joint Virtual Workshop
Monday 21 Sept. 2020
Cybersecurity - Where are we today?

Cybersecurity Best Practices

Paul Chua
Regional Product Security Officer, Greater Asia for BD
Cybersecurity Trends in Healthcare

- Healthcare is the #1 target for cybercriminals.
- It’s not just about patient privacy—it’s also about patient safety.
- Cybercriminals work 24/7/365, using increasingly sophisticated techniques.
- Every hospital and every patient environment is unique, so there’s no one-size-fits-all approach.
- Regulations are different in different locations.
Business Challenges of Cybersecurity

- Legacy Devices/End of Life
- Asset Management
- Incident Response and Vulnerability Management
- Procurement
- Patch Management
Striving for products and services that are secure...

**Security by design, in use, and through partnership.**
- Promote transparency, trust, collaboration, and control.
- Build and empower a community of practice.
- Evolve with business objectives

**BY DESIGN**
- Products designed to be secure and developed with security in mind

**IN USE**
- Products secured and maintained across their lifetime of use, across all technologies and sites including end-of-life decisions

**THROUGH PARTNERSHIP**
- A culture of transparency, engagement and proactive responsiveness with customers and the security industry

**Transparency**
- Industry-accepted measures
- That are interoperable and manageable by customers

**Control**
- Providing capability to
- Meet different needs
- In different environments

Doctors
Labs
Hospitals
Patients

© 2020 BD
Cybersecurity Framework

Service Design
- Concept
- Definition
- Development
  - Design Requirements
  - Cybersecurity Requirements
  - System Requirements
  - Hardening Standards
  - Software Requirements
  - Secure Coding Standards
  - Regional and Market Cybersecurity Requirements
  - Asset, Vulnerability and Patch Management

Service Transition
- Qualification
  - Penetration Testing
  - Cybersecurity Management Plan
  - User Complaints
  - Vulnerability and Patch Management
  - Incident Response
  - Governance and Compliance Reporting
  - Cybersecurity White Paper

Service Operation
- Launch
  - Identity Access Management
  - Logging and Monitoring
  - Inventory Management
  - Decommissioning
  - Governance and Compliance Reporting

Training and Awareness
- Design Control
- Complaint Handling
- Risk Management

Formalized
Verifiable
Repeatable
Continuous
Traceable
Cybersecurity Best Practices

• **Security by design, in use and through partnership**: Consider the entire lifecycle of the device, from R&D through end of life/end of support.

• **Collaboration is essential**: Regulators, healthcare providers and medical device manufacturers must work closely together; build a community of practice.

• **Apply proven best practices**: Network segmentation, patch management, Intrusion Detection Systems, malware protection, defense in depth, principle of least privileges.

• **Never be complacent**: Evolve with the latest strategies, like Zero Trust principles.

• **Educate your workforce**: Train them to recognize social engineering and phishing attacks
Thank you!