Medical Device Security Standards

EU-US eHealth Marketplace & Conference
October 22, 2014

Mark Coderre, National Practice Director – Security Services

Regulatory Impact on Security and Innovation

- Heavier regulations can carry risks too:
  - Organizations shift resources from design and testing to audit response.
  - Regulatory frameworks are slow to change relative to rapid changes in threat tactics and targets – are we even testing the most relevant controls?
  - Assessment processes can look for presence of controls but are they deployed appropriately – are we looking for quality or quantity?
  - Tend to focus on confidentiality and availability – but what about integrity controls?

- However, accountability and good faith intent must be in place!
  - Risk management "built in" to governance (release management, product planning)
  - Security reviews of the architecture as well as the product
  - The organization must practice *mature* Risk Management including threat modeling and business impact analysis
  - A trust mark representing the safety of the product is desirable

FDA Guidance as of October 2, 2014

- ✓ General Principles include risk management phases
  - o Identification, inherent risk, controls, residual risk
  - o References to best practices
- ✓ Cites the basics which are still important
  - o Strong Authentication, Authorization, Privileged User
  - o Code signatures and configuration management procedures for trustworthiness
  - o Encryption of data in motion
  - o Event logging and Incident Analysis & Response
  - o Assume the device can be compromised and still protect critical functions
- ✓ Present top risks and be transparent about analysis
  - o Map controls to risks, patch management, delivery protection, environmental controls

Source: "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices" fda.gov