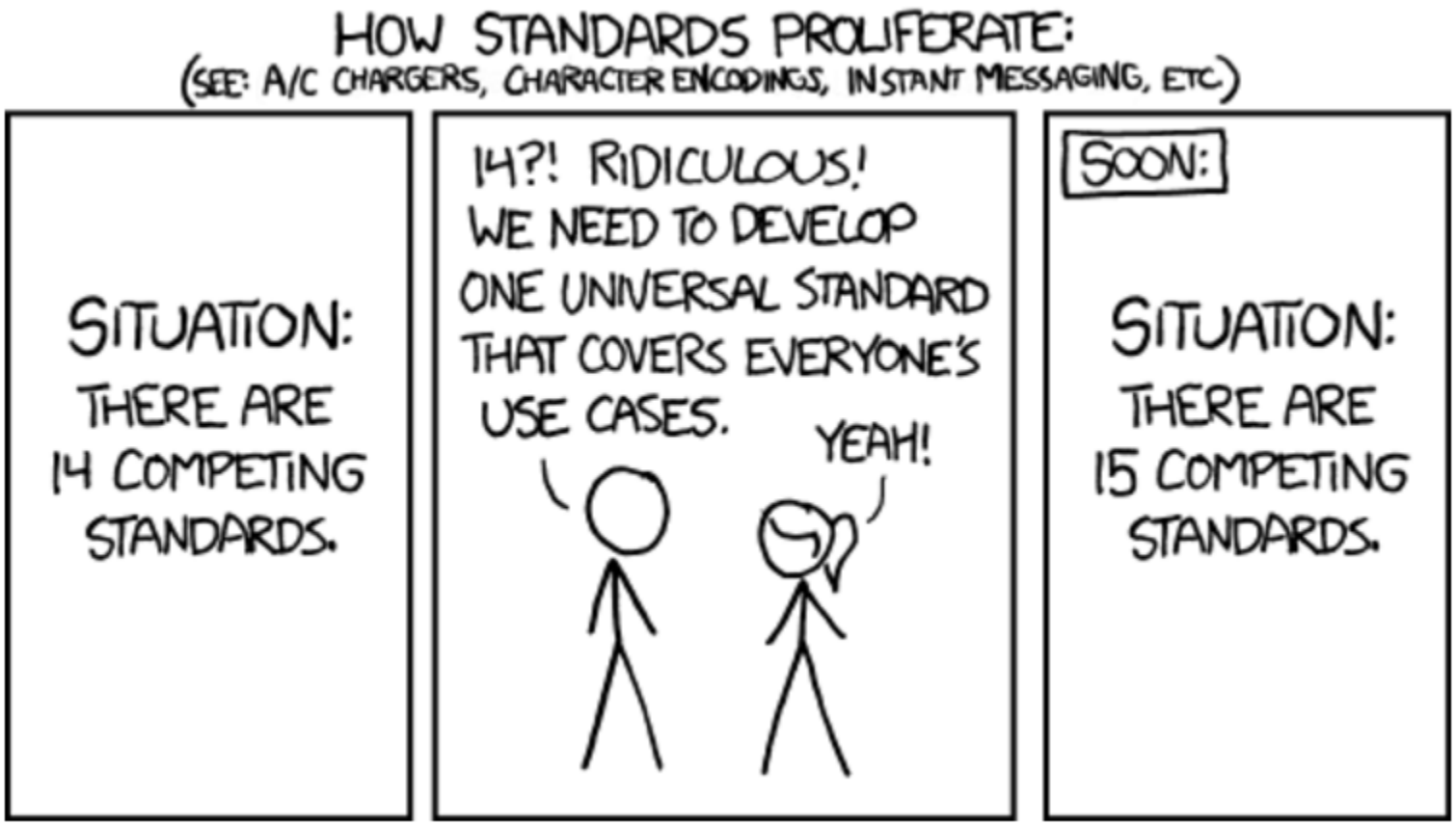
CYBER SECURITY SUMMIT 2017

Building the Future – Standards and Resources

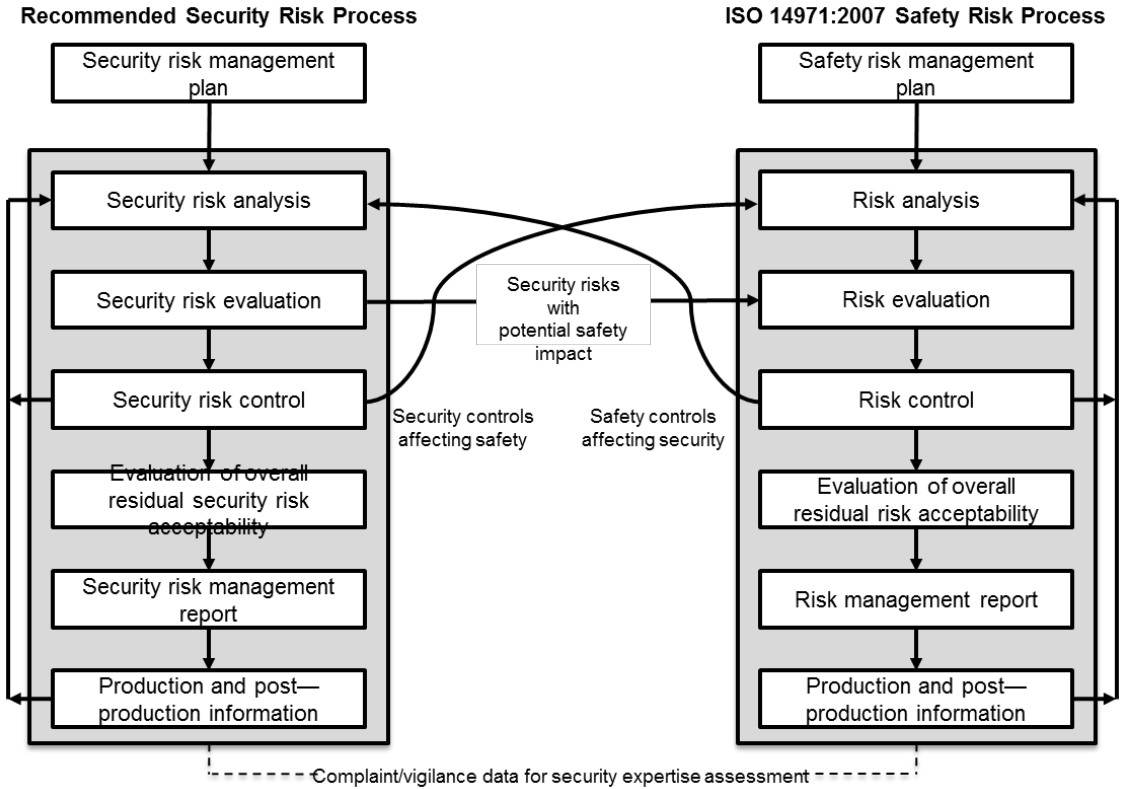
Ken Hoyme – Director, Product Security
Boston Scientific

Standards Monotonically Increase



AAMI TIR57

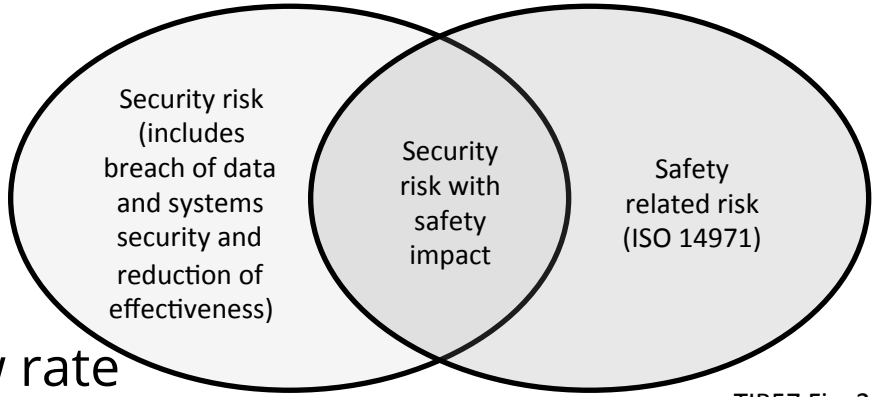
- Addresses security risk management in the context of 14971.
- Creates clear linkages between the consideration of safety and security.
- Recognized by the FDA and referenced in their recent post-market guidance.



Alignment with 14971

- Defining device security is inherently a Risk Management activity.
  - Risks that may lead to patient harm.
  - Risks that may lead to breach of PHI.
- Medical device manufacturers already have a risk management process for safety risk.
- We decided to introduce security risk management in a 14971 context.
  - To the point that the main body of TIR 57 parallels the section structure of 14971.

Security and Safety Risks



TIR57 Fig. 2

- Security risks that impact safety
  - Hacked pump changes drug flow rate
- Security risks that don't impact safety
  - PHI exposed
- Safety risks unassociated with security
  - Power supply failure

ISO/TC 215 – Health Informatics

- IEC 80001 Standard Series
  - Application of risk management for IT-networks incorporating medical devices
  - Guidance for hospitals to configure safe and secure IT networks
- Not imposed by FDA on device vendors
  - But will provide insight into what the hospitals may require

80001-1

- “Part 1: Roles, responsibilities and activities”
- Define a risk management approach for those integrating devices on networks
- Concept of “responsibility agreements”
  - Negotiated between hospital and device vendor

IEC/TR 80001-2-2

- Part 2-2: Guidance for the disclosure and communication of medical device security needs, risks and controls
- Organized around 19 “Security Capabilities”

Automatic Logoff	Audit Controls	Authorization	Configuration of Security Features
Cyber Security Product Upgrades	Data Backup and Disaster Recovery	Emergency Access	Health Data De-identification
Health Data Integrity and Authenticity	Health Data Storage Confidentiality	Malware Protection/ Detection	Node Authentication
Person Authentication	Physical Locks on Devices	Security Guides	System & Application Hardening
Third Party Components in Product Lifecycle Roadmaps	Transmission Confidentiality	Transmission Integrity	

IEC/TR 80001-2-8

- “Part 2-8: Application guidance -- Guidance on standards for establishing the security capabilities identified in IEC 80001-2-2”
- Maps 80001-2-2 security capabilities to several standards
  - NIST SP 800-53
  - ISO 27799
  - IEC 62443
  - ISO/IEC 27002
  - ISO/IEC 15408
- The mappings are not intended to be an exhaustive set of controls for each capability but rather guidance for the selection of controls for each capability

HIMSS/NEMA MDS2 Form

- MDS2 – Manufacture Disclosure Statement for Medical Device Security
  - http://www.nema.org/standards/Pages/Manufacturer-Disclosure-Statement-for-Medical-Device-Security.aspx
- Discloses the use/management of private data in the device
- Discloses security capabilities of the device
  - Terminology aligned to IEC/TR 80001-2-2
- Expect this form to be requested as part of contract negotiations for network connected devices