RSA Conference2015
San Francisco | April 20-24 | Moscone Center

SESSION ID: TECH-F03

Medical Device Security: Assessing and Managing Product Security Risk

Russell Jones
Partner
Cyber Risk Services | Deloitte & Touche LLP

John Lu
Principal
Cyber Risk Services | Deloitte & Touche LLP

Presenter Bio

	Summary of experience
 **Russell L. Jones** Partner Cyber Risk Services Deloitte & Touche LLP	• Russell leads Deloitte's Medical Device Safety and Security (MeDSS) practice • More than 22 years of experience working with health care provider, biotechnology/Pharma, diagnostics, medical device manufacturer and public sector clients • Focus on development of cybersecurity, product security, information security, data privacy and IT risk management programs • Bachelor's degree in Management Information Systems from University of Notre Dame • Certified Information Privacy Professional (CIPP), Certified Information Systems Security Professional (CISSP), Certified Information Systems Auditor (CISA), and Certified Public Accountant (CPA) licensed in California and Maryland
 **John Lu** Principal Cyber Risk Services Deloitte & Touche LLP	• John specializes in delivering Security, Privacy, & Resiliency services for global Life Sciences organizations • Over fifteen (15) years of experience leading information technology risk management (ITRM), information security, data privacy, and third-party/vendor risk management, with a focus on Identity & Access Management (IAM) projects • Experience encompasses a broad spectrum of engagement types, ranging from project management, policy development, current state assessment, strategy and roadmap development, requirements analysis and definition, vendor evaluation and selection, architecture and design, installation and configuration, testing, and knowledge transfer • Certified Information Systems Security Professional (CISSP)

Agenda

What are we going to talk about today?

- Current medical device security landscape: Takeaways from FDA guidance
- Security risk assessment for networked medical devices: Deloitte's POV
- You've identified security risks, now what?: Possible solutions – Security By Design
- Key takeaways

Today's Objectives:

- Learn how to assess and mitigate the security risk for medical devices

Audience Poll

Your poll will show here

1

Install the app from
pollev.com/app

2

Make sure you are in
Slide Show mode

Still not working? Get help at pollev.com/app/help

or

Open poll in your web browser

Audience Poll

Your poll will show here

1

Install the app from
pollev.com/app

2

Make sure you are in
Slide Show mode

Still not working? Get help at pollev.com/app/help

or

Open poll in your web browser

Medical Device Cybersecurity Issues

Trending In the News

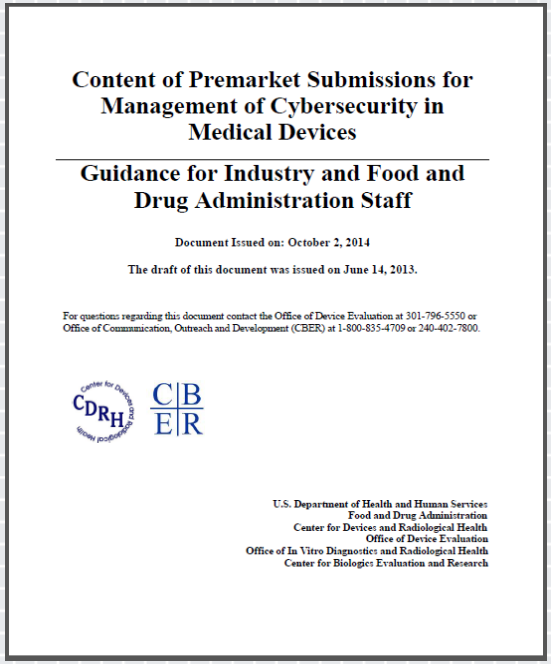
RSAConference2015

San Francisco | April 20-24 | Moscone Center

Current Medical Device Security Landscape

Current state of medical device security

Takeaways from FDA guidance



Content of Premarket Submissions for Management of Cybersecurity in Medical Devices

Guidance for Industry and Food and Drug Administration Staff

Document Issued on: October 2, 2014

The draft of this document was issued on June 14, 2013.

For questions regarding this document contact the Office of Device Evaluation at 301-796-5550 or Office of Communication, Outreach and Development (CBER) at 1-800-835-4709 or 240-402-7800.

U.S. Department of Health and Human Services
Food and Drug Administration
Center for Devices and Radiological Health
Office of Device Evaluation
Office of In Vitro Diagnostics and Radiological Health
Center for Biologics Evaluation and Research

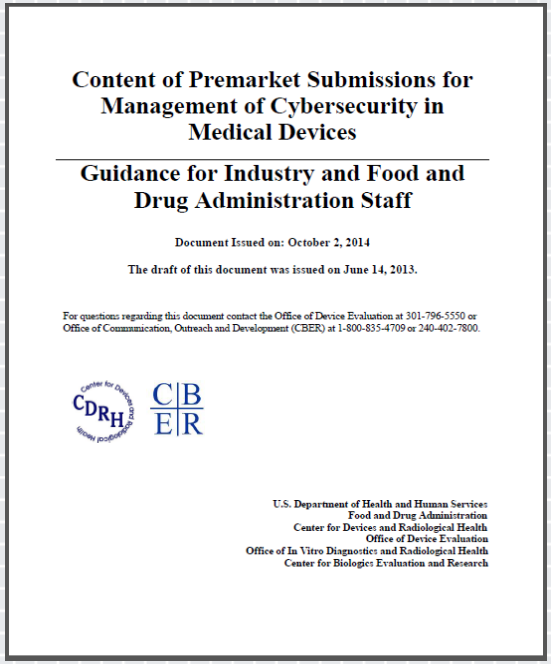
Source:
http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM356190.pdf

Key takeaways from the FDA's guidance (the Guidance):

- **Manufacturers should address cybersecurity during the "design and development" of the medical device**
- **The Guidance leverages NIST's Cybersecurity Framework**
- **The scope of the Guidance covers the following:**
  - 510k, de novo submissions, Premarket Approval Applications (PMAs), product development protocols, and humanitarian device exemption

Current state of medical device security (Contd.)

Takeaways from FDA guidance



Content of Premarket Submissions for Management of Cybersecurity in Medical Devices

Guidance for Industry and Food and Drug Administration Staff

Document Issued on: October 2, 2014

The draft of this document was issued on June 14, 2013.

For questions regarding this document contact the Office of Device Evaluation at 301-796-5550 or Office of Communication, Outreach and Development (CBER) at 1-800-835-4709 or 240-402-7800.

U.S. Department of Health and Human Services
Food and Drug Administration
Center for Devices and Radiological Health
Office of Device Evaluation
Office of In Vitro Diagnostics and Radiological Health
Center for Biologics Evaluation and Research

Source:
http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM356190.pdf

Key takeaways from the FDA's guidance (the Guidance) (Contd.):

- **The FDA is looking for the following in their review of the above types of submissions:**
  - A specific list of all cybersecurity risks (**both intentional and unintentional**) that were considered in the design of the device and a list, and justification for all cybersecurity controls that were established for the device;
  - A "traceability matrix" that links the actual cybersecurity controls to the cybersecurity risks that were considered;
  - A summary describing the plan for providing validated software updates and patches as needed throughout the lifecycle of the medical device to continue to assure its safety and effectiveness;
  - A summary describing controls that are in place to assure that the medical device software will remain free of malware from the point of origin to the point at which that device leaves the control of the manufacturer; and
  - Device instructions for use and product specifications related to recommended cybersecurity controls appropriate for the intended use environment.

Current state of medical device security

A first of its kind medical device security workshop was held on October 21 – 22, 2014

FDA's CENTER FOR DEVICES & RADIOLOGICAL HEALTH, THE DEPARTMENT OF HOMELAND SECURITY (DHS) C³ VOLUNTARY PROGRAM AND THE DEPARTMENT OF HEALTH AND HUMAN SERVICES (HHS) CRITICAL INFRASTRUCTURE PROTECTION PROGRAM PRESENT A PUBLIC WORKSHOP:

Collaborative Approaches for Medical Device and Healthcare Cybersecurity

October 21-22, 2014

National Intellectual Property Rights Coordination Center

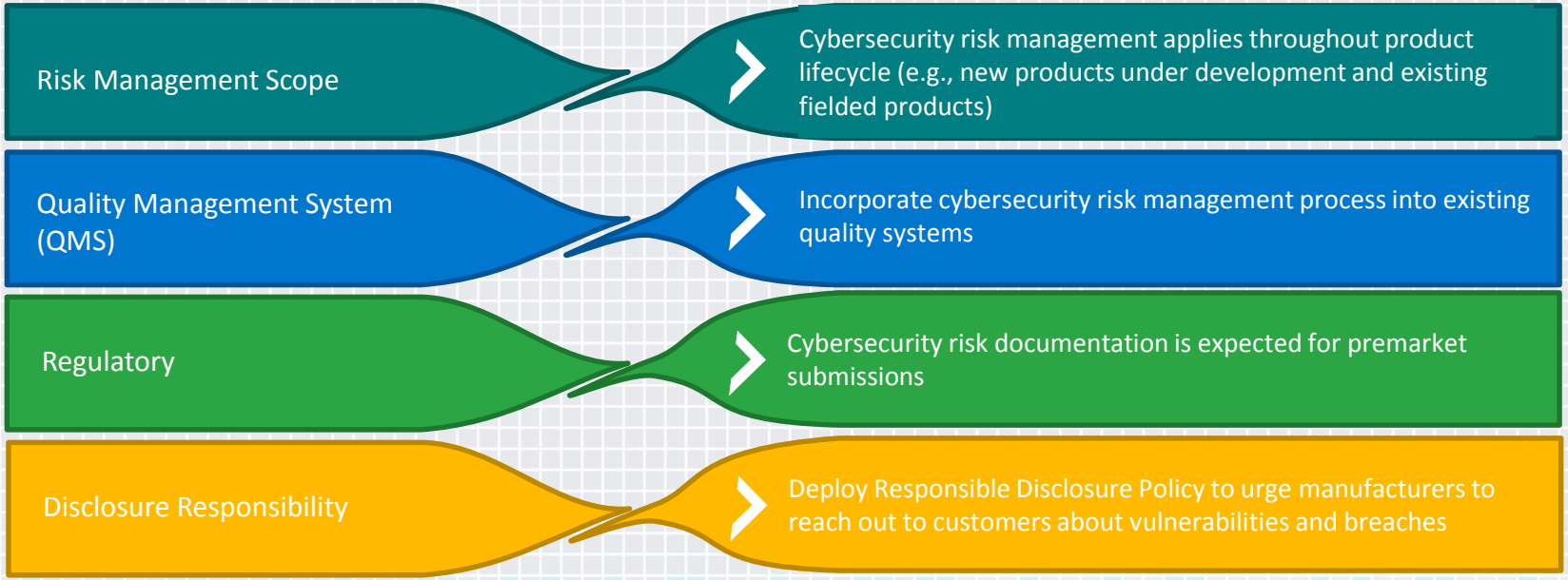
Arlington, VA

FDA

Key takeaways from the FDA's Cybersecurity Workshop

Developing a scalable and repeatable Security Risk Assessment Framework for medical devices

FDA guidance provides recommendations for manufacturers to consider for effective cybersecurity risk management of the medical devices they design, develop, and/or manage.



RSAConference2015

San Francisco | April 20-24 | Moscone Center

Security Risk Assessment for Networked Medical Devices: Deloitte's POV

High Risk Networked Medical Devices: Infusion pumps

How can you exploit a medical device?

An infusion pump is a medical device that infuses fluids, medication or nutrients into a patient's circulatory system. Infusion pumps are one of the most **ubiquitous** medical devices in the world.

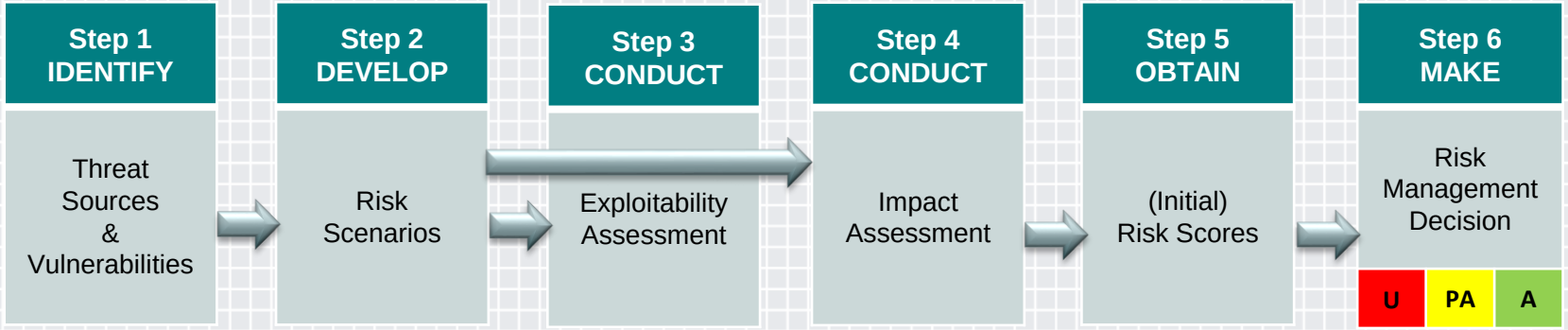
Infusion Pump

Illustrative Cyberattack Scenario: Infusion Pump

Security Risk Assessment for Medical Devices

Adopting a broad risk assessment approach

The Security Risk Assessment Process uses a six-step approach to calculate the risk rating using the Medical Device Security Risk Framework and the risk calculator. The risk ratings can be used by management to prioritize identification and adoption of mitigating controls.



Source: "Security Risk Assessment Framework for Medical Devices", MDPC, September 26, 2014

Legend:

A	Acceptable
PA	Potentially Acceptable
U	Unacceptable

Ability to Exploit Vulnerability – illustrative example

Defining the threat factors

The Ability to Exploit Vulnerability (in lieu of "likelihood") is calculated for identified risk/threat scenarios using the table below

	High (Easy to Exploit)	Medium	Low (Difficult to Exploit)	Validated
Threat Agent Factors				
Skill	• Minimal Technical Skills • Default Configuration	• Advanced Technology Skills • Common Configuration	• Advanced Technology Skills	Nearly impossible and/or merely theoretical for a highly skilled attacker with advanced equipment to succeed
Motive	• Financial or other identifiable gain exits	• Some financial or other identifiable gain exits	• No financial or other identifiable gain exits	
Opportunity & Resources	• No physical access required	• Some physical access required • Requires access rights	• Full physical access required	
Vulnerability Factors				
Ease of Discovery & Awareness	• Easily discoverable	• Knowledge of vulnerability exists publicly with no technical details	• Difficult to discover	Nearly impossible to exploit and/or merely theoretical even with advanced and/or commercial grade equipment
Ease of Exploiting	• Easy to exploit	• Difficult to exploit	• Nearly impossible to exploit	
Intrusion Detection	• Unauthorized access is not logged or monitored	• Unauthorized access is logged and monitored but no automated alerts	• Unauthorized access is logged and monitored and immediately detected	
Effectiveness of Applied Security Controls	• Security controls are not designed or implemented effectively	• Security controls are well defined but limited in strength and effectiveness	• Security controls are well defined and multi-layered	Controls developed and implemented should: provide a high degree of confidence that they are complete, consistent and correct

Source: Adapted from "Security Risk Assessment Framework for Medical Devices", MDPC, September 26, 2014

Risk rating

Determining the risk ranking

The risk calculator takes as its inputs the Ability to Exploit Vulnerability and Impact. The combination of impact and ability to exploit results in the risk score, which is either Acceptable, Potentially Acceptable, or Unacceptable (defined below).

Illustrative Example of Risk Score Definitions

Product Device	
Acceptable (A)	No further evaluation or controls are necessary regarding the Acceptable risk scenario
Potentially Acceptable (PA)	It is highly recommended that manufacturers consider additional security controls or strengthen existing mitigating controls
Unacceptable (U)	Additional security controls and/or strengthened mitigating controls must be applied unless a decision is made to decommission the device/project

Illustrative Example of the MDPC Security Risk Calculator

EXPLOITABILITY VALUE	IMPACT VALUE				
	1 (Negligible)	2 (Minor)	3 (Major)	4 (Critical)	5 (Catastrophic)
3 (High)	Potentially Acceptable	Unacceptable	Unacceptable	Unacceptable	Unacceptable
2 (Medium)	Acceptable	Potentially Acceptable	Potentially Acceptable	Unacceptable	Unacceptable
1 (Low)	Acceptable	Acceptable	Acceptable	Potentially Acceptable	Potentially Acceptable
0 (Validated)	Acceptable	Acceptable	Acceptable	Acceptable	Acceptable

Source: "Security Risk Assessment Framework for Medical Devices", MDPC, September 26, 2014

Scenario – Drug infusion pump

Applying the risk ranking

- IDENTIFY
  Threat Sources & Vulnerabilities
- DEVELOP
  Risk Scenarios
- CONDUCT
  Exploitability
- OBTAIN
  Risk Scores
- MAKE
  Risk Management Decision
- OBTAIN
  RESIDUAL Risk Scores

Vulnerability:

Device is not password protected and allows easy access to the multi-file system, custom binary files, registry settings, and pump control

Risk Scenario:

The attacker:

1. Target is attached to a wireless infusion pump and is using web security.
2. The device is not password protected and provides easy access to pump control.
3. Executes the native pump accessible to embedded operating system.

Ability to Exploit	Confidentiality		Patient Safety	
	Impact	Current Risk Score	Impact	Current Risk Score
2-Medium	4-Critical	Unacceptable	5-Catastrophic	Unacceptable

Remediation:

Mitigate risk through advice given in US-Cert ICS-Alert-13-164-01, including additional network security and segmentation controls and monitoring, working with the product vendor to apply device specific patches.

Ability to Exploit	Confidentiality		Patient Safety	
	Impact	Residual Risk Score	Impact	Residual Risk Score
1-Low	4-Critical	Potentially Acceptable	5-Catastrophic	Potentially Acceptable

Note: Information is an example of a vulnerability scenario and is not specific to one device or company.

RSAConference2015

San Francisco | April 20-24 | Moscone Center

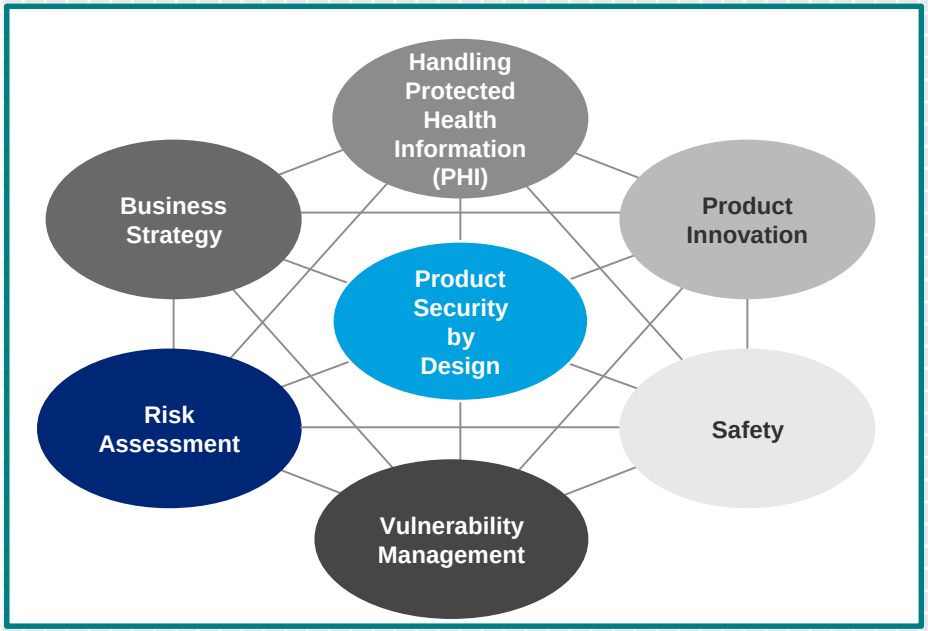
You've Identified Security Risks, Now What?: Possible solutions– Security By Design

Security by Design- Deloitte's Point of View

Building security into the medical device on the front-end

Security by Design is becoming **a key requisite within the product development lifecycle for medical devices**. A risk-based approach that integrates Research & Development (R&D) innovation with the security considerations of regulatory agencies and patients and the business strategy of the firm must be undertaken.

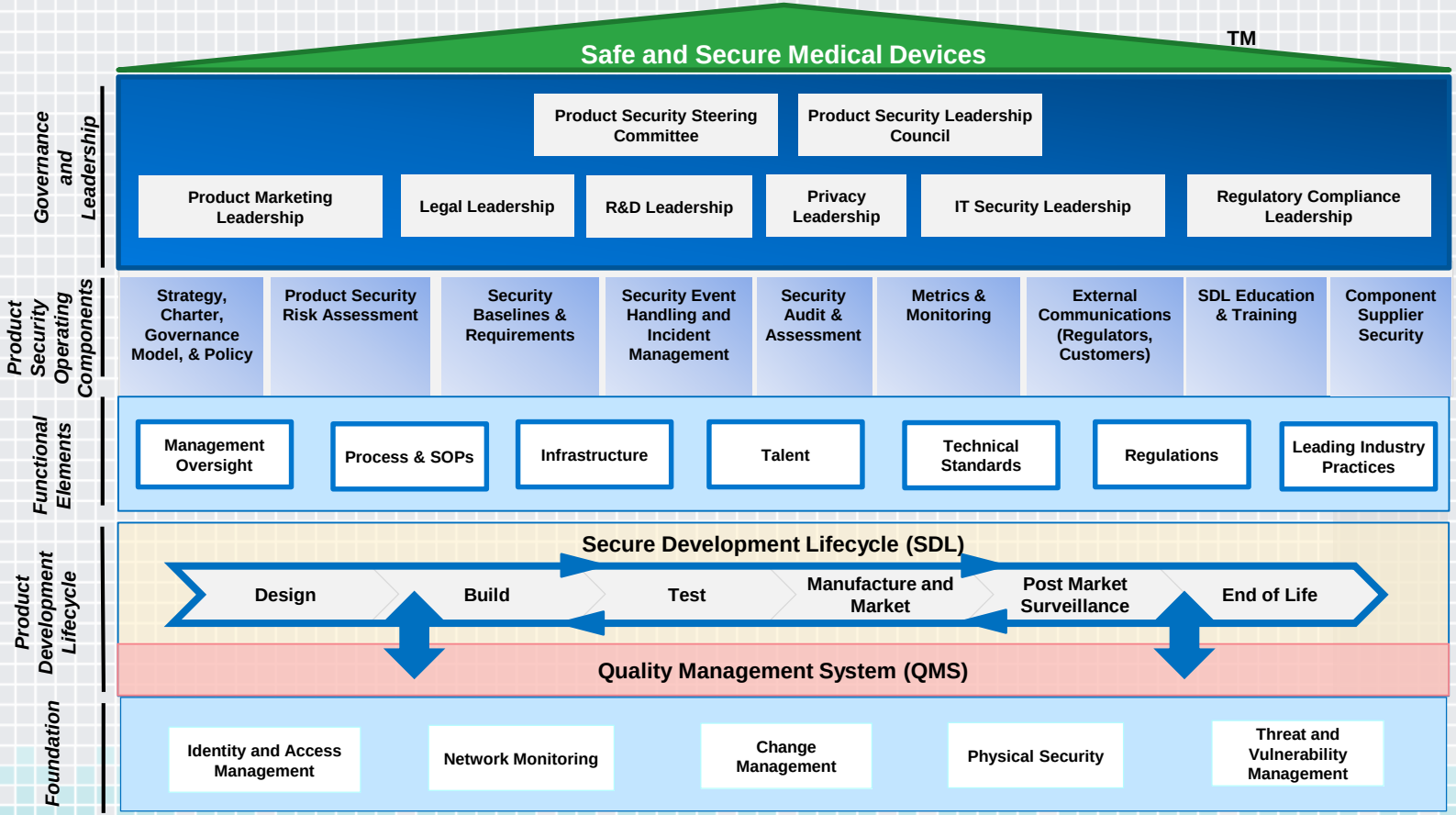
Handling PHI	➢ Design must incorporate and maintain confidentiality of sensitive patient information
Product Innovation	➢ Design must not compromise the creativity of the development team and thus maintain competitive advantage for the firm
Safety	➢ Design must comply with safety requirements and consider potential safety implications
Vulnerability Management	➢ Design must be continuously monitored for potential vulnerabilities at an early stage
Risk Assessment	➢ Design related risks must be identified, tracked and mitigated throughout the product lifecycle
Business Strategy	➢ Design must align with the business strategies and market objectives of the firm



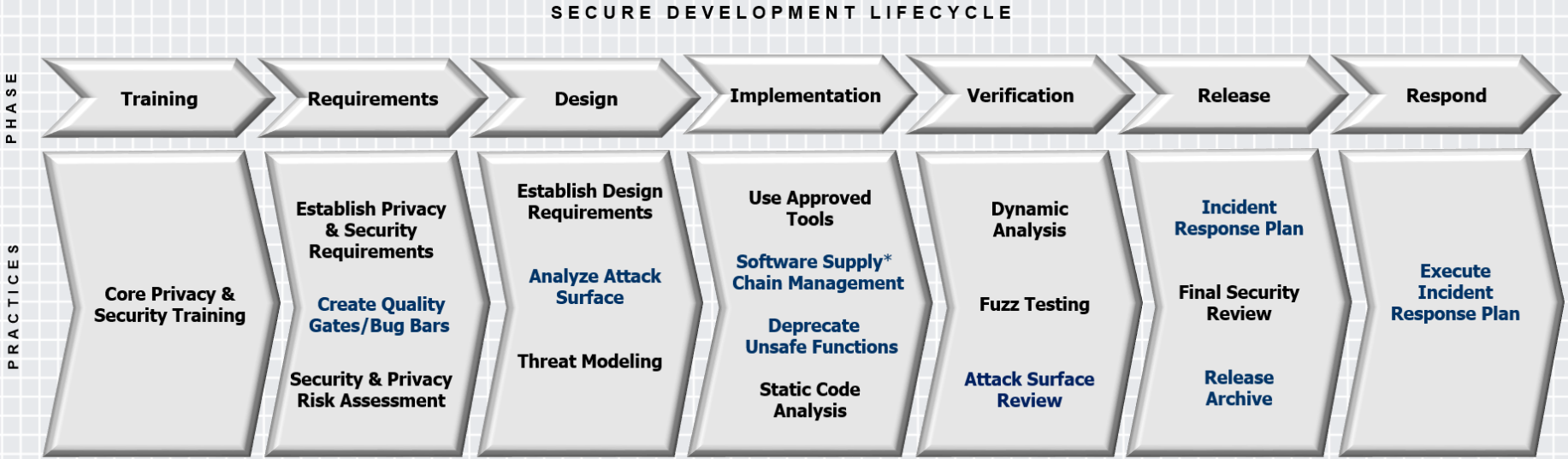
Implementing "Security by Design" requires a programmatic approach

Deloitte Product Security Program Framework (TM)

Leveraging Product Security Program Framework



Implement A Secure Development Lifecycle (SDL)



Source: adapted from : "Microsoft SDL', http://www.microsoft.com/security/sdl/process/

PHASE 1: Training

Training and Education is foundational for building better software and applications and include secure design, threat modeling, secure coding, security testing, and privacy leading practices.

Core Privacy & Security Training

Software development technical roles such as developers, testers, and program managers should consider **attending at least one security training class each year.**

Source: adapted from : "Microsoft SDL', http://www.microsoft.com/security/sdl/process/

PHASE 2: Requirements

The objective of this phase is to consider foundational security and privacy issues and to analyze how to align quality and regulatory requirements with costs and business needs.

Establish Security and Privacy Requirements

Define and integrate security and privacy requirements early to identify key milestones and deliverables and minimize disruptions to plans and schedules.

Create Quality Gates/Bug Bars

Define minimum acceptable levels of security and privacy quality at the start. This can help the team understand risks associated with security issues, identify and fix security bugs during development, and apply the standards throughout the project

Perform Security and Privacy Risk Assessments

Analyze software and application design based on regulatory requirements that can help to identify which portions of a product will require threat modeling and security design reviews.

Source: adapted from : "Microsoft SDL', http://www.microsoft.com/security/sdl/process/

PHASE 3: Design

This phase is critical for establishing leading practices around design and functional specifications and performing risk analysis that will help mitigate security and privacy issues throughout a project

Establish Design Requirements

Analyze design specifications against a functional specification to involve accurate and complete design specifications, including minimal cryptographic design requirements and a specification review

Perform Attack Surface Analysis/Reduction

Reduce the opportunities for attackers to exploit a potential weak spot or vulnerability requires **thoroughly analyzing overall attack surface and includes disabling** or restricting access to system services, applying the principle of least privilege, and employing layered defenses wherever possible.

Use Threat Modeling

Apply **a structured approach to threat scenarios during design to help a team more effectively and less expensively** identify security vulnerabilities, determine risks from those threats, and establish appropriate mitigations.

Source: adapted from : "Microsoft SDL', http://www.microsoft.com/security/sdl/process/

PHASE 4: Implementation

The focus of this phase is to help the end user to make informed decisions about the secure ways to deploy the software. It's also the time to establish leading practices for detecting and removing security issues from the code.

Use Approved Tools

Publish a list of approved tools and associated security checks to help automate and enforce security practices easily at a low cost.

Deprecate Unsafe Functions

Analyze project functions and APIs and ban those determined to be unsafe, to help reduce potential security bugs with very little engineering cost.

Perform Static Analysis

Analyze the source code prior to compilation to provide a scalable method of security code review and to help determine that secure coding policies are being followed.

Source: adapted from : "Microsoft SDL', http://www.microsoft.com/security/sdl/process/

PHASE 5: Verification

This phase involves a comprehensive effort to determine that the code addresses the security and privacy tenets established in the previous phases.

Perform Dynamic Analysis

Perform run-time verification of the software to check functionality using tools that monitor application behavior for memory corruption, user privilege issues, and other critical security problems

Perform Fuzz Testing

Induce program failure by **deliberately introducing malformed or random data to an application to help reveal potential** security issues prior to release while requiring modest resource investment.

Conduct Attack Surface Review

Review attack surface upon code completion to help determine that design or implementation changes to an application or system have been taken into account, and that new attack vectors created as a result of the changes have been reviewed and mitigated including threat models.

Source: adapted from : "Microsoft SDL', http://www.microsoft.com/security/sdl/process/

PHASE 6: Release

The focus of this phase is readying a project for public release, including planning ways to effectively perform post-release servicing tasks and address security or privacy vulnerabilities that may occur later.

Create an Incident Response Plan

Prepare an Incident Response Plan to address new threats that can emerge over time. It includes **identifying** appropriate security **emergency contacts** and establishing **security servicing plans** for code inherited from other groups within the organization and for licensed third-party code.

Conduct Final Security Review

Review security activities that were performed to help determine software release readiness.

The Final Security Review (FSR) usually includes examining threat models, tools outputs, and performance against the quality gates and bug bars defined during the Requirements Phase.

Certify Release and Archive

Certify software prior to a release helps determine security and privacy requirements were met.

Archive pertinent data for performing post-release servicing tasks and to help lower the long-term costs associated with sustained software engineering. .

Source: adapted from : "Microsoft SDL', http://www.microsoft.com/security/sdl/process/

PHASE 7: Response

This post-release phase centers on the development team being able and available to respond appropriately to reports of emerging software threats and vulnerabilities

Execute Incident Response Plan

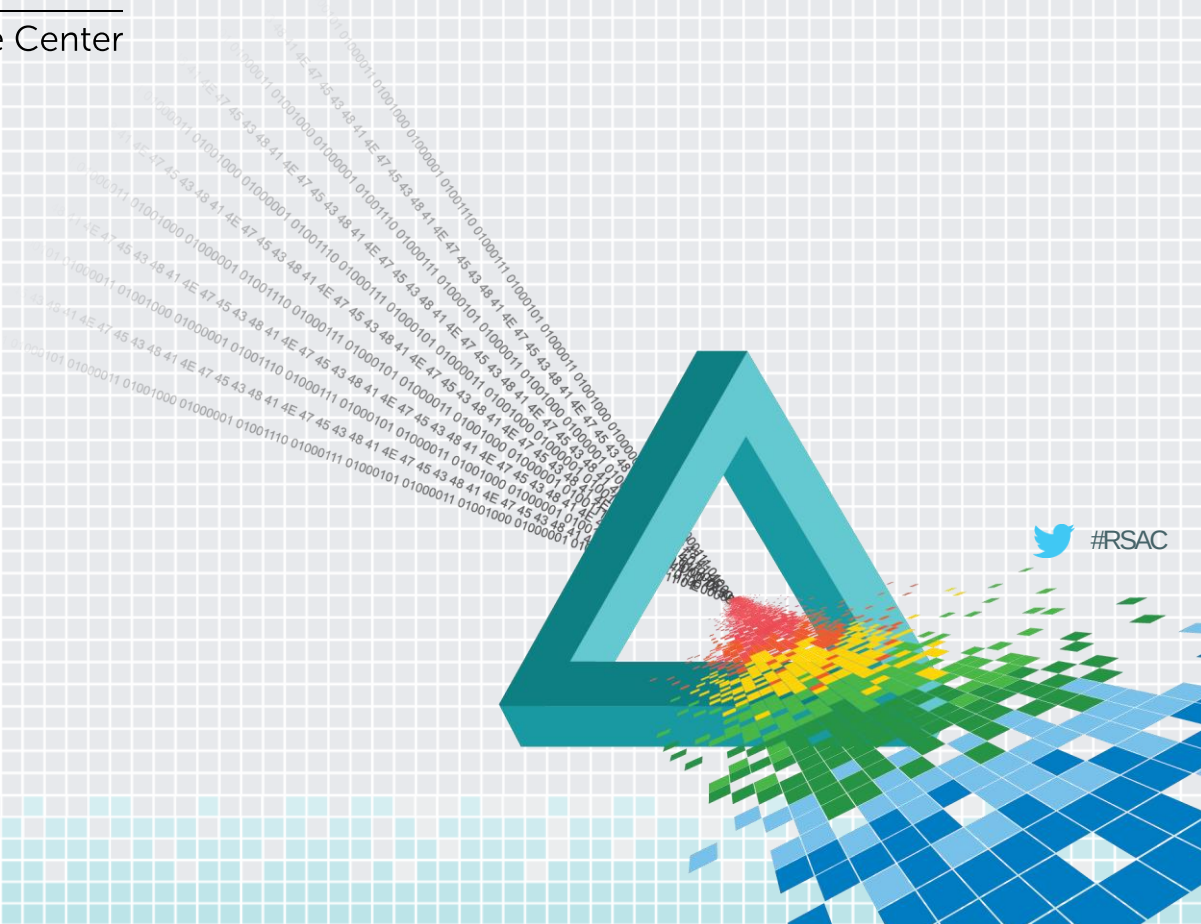
Implement the Incident Response Plan instituted in the Release phase to help protect customers from software security or privacy vulnerabilities that emerge.

Source: adapted from : "Microsoft SDL', http://www.microsoft.com/security/sdl/process/

RSAConference2015

San Francisco | April 20-24 | Moscone Center

Key Takeaways



Key Takeaways

Some key actions you need to own

1. **Get involved with key medical device/mHealth driven consortiums/standard setting bodies**
   Proactively shape the security standards that will result in medical devices that are ready for the 21st century cyber risk environment and help you meet your regulatory compliance requirements.

2. **Get involved with the NH-ISAC**
   Sharing of key cyber threat intelligence about fielded networked medical devices will be critical in understanding the current threat environment and modeling the future cyber threat landscape. The FDA and NH-ISAC have established an agreement that will allow sharing of cyber threat intelligence. Consider getting involved with NH-ISAC to both benefit from this knowledge and shape the protocols and standards that come out of it.

3. **Monitor the FDA's direction on medical device security**
   Currently, the FDA is leading the way regarding medical device security; other international regulatory agencies will most likely follow suit. Continue to monitor the FDA's direction and additional guidance on cybersecurity that may be forthcoming.

4. **Adopt A Secure Development Lifecycle (SDL)**
   "Build-in" security in the early Requirements/Design phases of new medical devices (or new indications of existing medical devices); embed SDL into the "DNA" of your product development teams.

This presentation contains general information only and Deloitte is not, by means of this presentation, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This presentation is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this presentation.