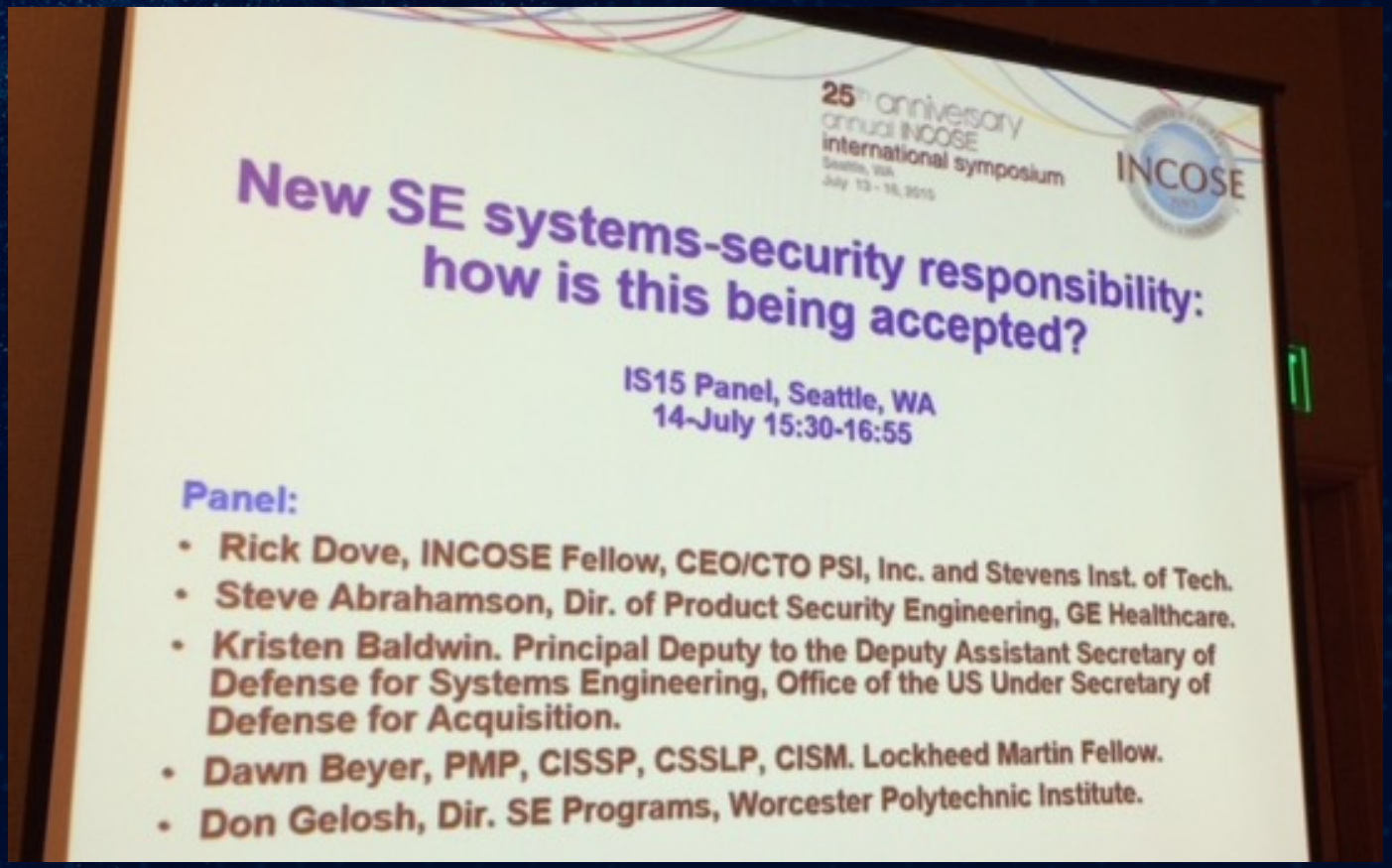
INCOSE
Healthcare
Working Group
5th Annual Systems Engineering in Healthcare Conference
May 1-2, 2019
Minneapolis, MN

INCOSE

Quality Cyber Security for Medical Devices

Steve Abrahamson
Sr. Director, Product Cyber Security GE Healthcare



Steve Abrahamson, BSME, MBA, CEM

AAMI Clinical Engineering Symposium – Long Beach, June 2018

TIME	DESCRIPTION	SPEAKERS/PANELISTS
7:00 a.m.–7:10 a.m.	Welcome, Introduction	**Arif Subhan**, MS, CCE, CHTM, FACCE, ACCE President
7:10 a.m.–7:55 a.m.	The Security Risks Associated with an Evolving Ecosystem	**Axel Wirth**, CPHIMS CISSP HCISSP, Distinguished Technical Architect, Symantec Corporation
7:55 a.m.–8:40 a.m.	Security Risk Management Processes in the New Environment	**Steve Grimes**, FACCE FAIMBE FHIMSS, Principal Consultant, Strategic Healthcare Technology Associates, LLC
8:40 a.m.–8:55 a.m.	BREAK	
8:55 a.m.–9:40 a.m.	Manufacturing Secure Products for the New Environment	**Steve Abrahamson**, BSME MBA CEM, Senior Director, Product Cyber Security, GE Healthcare
9:40 a.m.–10:30 a.m.	Panel Discussion—Healthcare Providers Discuss Migrating and Adapting Security Practices to the New Environment	**Steve Abrahamson** **Steve Grimes** **Inhel Rekik**, MS, Georgetown University Hospital **Priyanka Upendra,** MSE, CCMS. SSLP, CHTM, Intermountain Healthcare **Axel Wirth**

Career Path

HARM

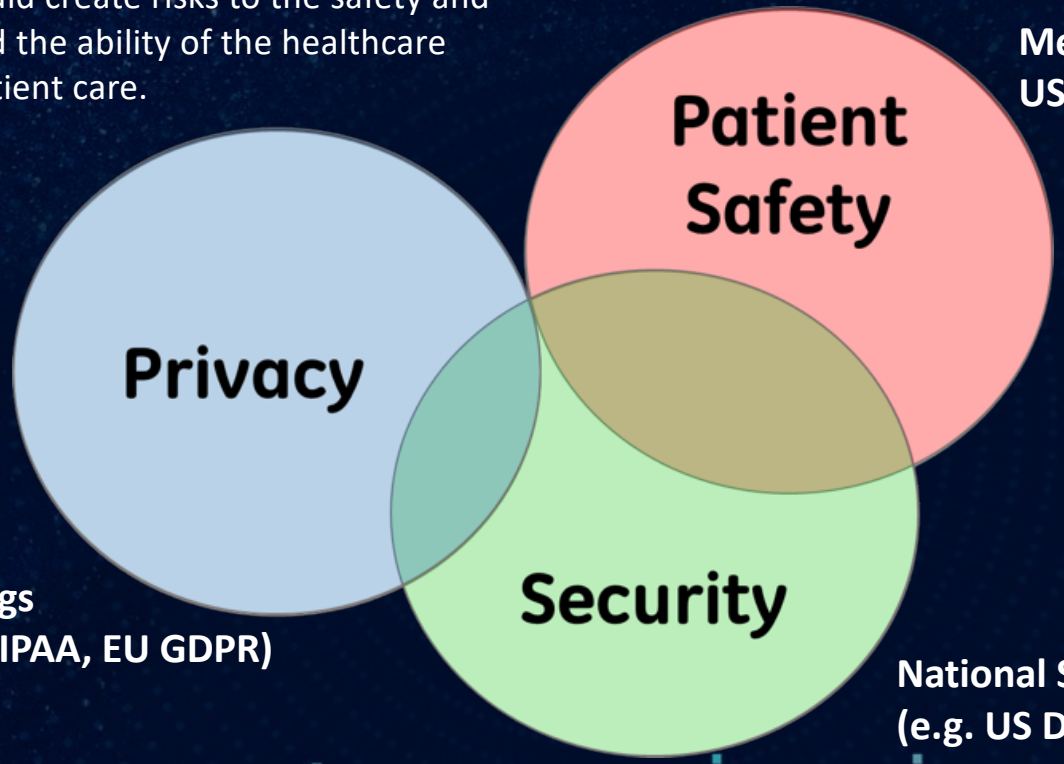
Preventing Harm

Cyber Security – Security in “Cyberspace”, a term coined by author William Gibson

“Cyberspace. A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts... A graphic representation of data abstracted from banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data. Like city lights, receding...”
— William Gibson, *Neuromancer (1984)*

Medical Device Cyber Security

Protecting medical devices and device data flows from threats to their integrity, confidentiality, and availability, where such threats could create risks to the safety and privacy of patients, and the ability of the healthcare provider to provide patient care.



Med Device Regulations (e.g. US FDA)

Privacy Regs (e.g. US HIPAA, EU GDPR)

National Security (e.g. US Dept of Homeland Security)

GE Healthcare

Safety Risk

BloombergBusinessweek
15 August 2013

Bloomberg.com | Businessweek.com | Bloomberg TV | Premium

BloombergBusinessweek
Technology

Global Economics | Companies & Industries | Politics & Policy | Technology | Markets & Finance | Innovation & Design | Lifestyle

Security

Medical Hacking Poses a Terrifying Threat, in Theory

By Joshua Brustein | August 15, 2013

SEND TO kindle

Privacy Risk

Medscape 15 October 2018

Medscape Monday, October 15, 2018

NEWS & PERSPECTIVE DRUGS & DISEASES CME & EDUCATION ACADEMY V

News > Medscape Medical News

Healthcare Providers Are Common Source of Data Breaches

Tinker Ready
September 28, 2018

22 Read Comments

Note: US Data

More than 176 million confidential health records were breached between 2010 and 2017, including 37.1 million records controlled by healthcare providers, according to a study published online in *JAMA* this week.

Availability Risk (+ safety risk + privacy risk)

The Guardian – 12 May 2017

sign in | become a supporter | subscribe | search

jobs | US edition

theguardian

US | politics | world | opinion | sports | soccer | tech | arts | lifestyle | fashion | business | travel | environment | browse all sections

home › tech

Cybercrime

Massive ransomware cyber-attack hits nearly 100 countries around the world

More than 45,000 attacks recorded in countries including the UK, Russia, India and China may have originated with theft of 'cyber weapons' from the NSA

- Global cyber-attack - live updates
- 'Accidental hero' finds kill switch to stop spread

This article is 2 months old

7,179

Julia Carrie Wong and Olivia Solon in San Francisco

Friday 12 May 2017 15.57 EDT

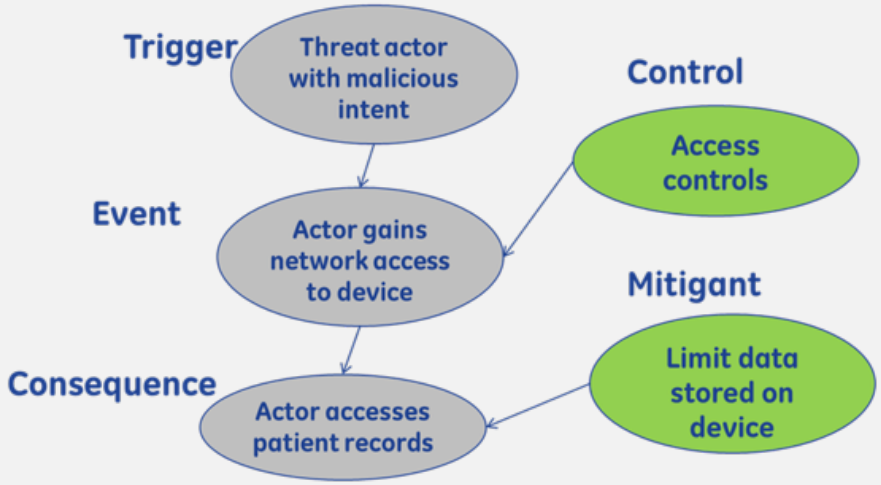
Understanding Security Risk Management

Risk = f (asset x threats x vulnerabilities) – controls

Asset = data, device
Threats = malicious actions, malware
Vulnerabilities = exploitable weaknesses in design
Controls = security safeguards to block exploits

Security Controls
- Access
- Authentication
- Accountability/audit
- Media protection
- Others

A simple network model for risk assessment:



A New Perspective on Risk

Safety Risk Management:

Protecting people from malfunctioning devices

Security Risk Management:

Protecting devices from malfunctioning people

FDA Quality System Regulation – 21 CFR Part 820

Current good manufacturing practice (CGMP) requirements are set forth in this quality system regulation…The requirements in this section are intended to ensure that finished devices will be safe and effective and otherwise in compliance with the Federal Food, Drug, and Cosmetic Act…

Quality System = Safe and Effective Devices with minimal risk to patient harm

GE Healthcare

US FDA Involvement – 03 August 2015

Infusion Pump Case

Citing hacking risk, FDA says Hospira pump shouldn't be used

Monday, 3 Aug 2015 | 7:22 AM ET The Associated Press – CNBC

The federal government says health care facilities should stop using Hospira's Symbiq medication infusion pump because of its vulnerability to hacking.

The Food and Drug Administration said Friday it's the first time it has warned caregivers to stop using a product because of a cybersecurity risk. It comes at a time of rising concerns about breaches of products that connect to the Internet. A week ago, automaker Fiat Chrysler recalled 1.4 million vehicles because of a flaw that made them vulnerable to hackers.

The FDA says the computerized pumps could be accessed remotely through a hospital's network, but it doesn't know of any cases where that has happened. In recent months cybersecurity experts and the Department of Homeland Security have warned that the device could be hacked and remotely controlled, possibly allowing an intruder to change the amount of medication a patient received.

Medtronic Defibrillator Vulnerability

TechCrunch - 22 March 2019

Homeland Security has issued a warning for a set of critical-rated vulnerabilities in **Medtronic** defibrillators that put the devices at risk of manipulation.

…Most modern devices come with wireless or radio-based technology to allow patients to monitor their conditions and their doctors to adjust settings without having to carry out an invasive surgery.

But the government-issued alert warned that Medtronic's proprietary radio communications protocol, known as Conexus, wasn't encrypted and did not require authentication, allowing a nearby attacker with radio-intercepting hardware to modify data on an affected defibrillator.

Homeland Security gave the alert a 9.3 out of 10 rating, describing it as requiring "low skill level" to exploit.

What is Quality

GE Healthcare

Quality Defined

Quality means the totality of features and characteristics that bear on the ability of the device to satisfy fitness for use, including safety and performance.

Quality (business) ... Consumers may focus on the specification **quality** of a **product**/service, or how it compares to competitors in the marketplace. Producers might measure the conformance **quality**, or degree to which the **product**/service was produced correctly.

The group of features and characteristics of a saleable good which determine its desirability and which can be controlled by a manufacturer to meet certain basic requirements. Most businesses that produce goods for sale have a product quality or assurance department that monitors outgoing products for consumer acceptability.

The extent to which a product meets its specifications.

Quality Gurus

W. Edwards Deming

Statistical Process Control built upon the work of Walter Shewhart

Deming's 14 Principles led to "Total Quality Management"

"Improve constantly and forever the system of production and service"

"If you can't describe what you do as a process, you don't know what you are doing."

"It is not enough to do your best; you must know what to do, and then do your best."

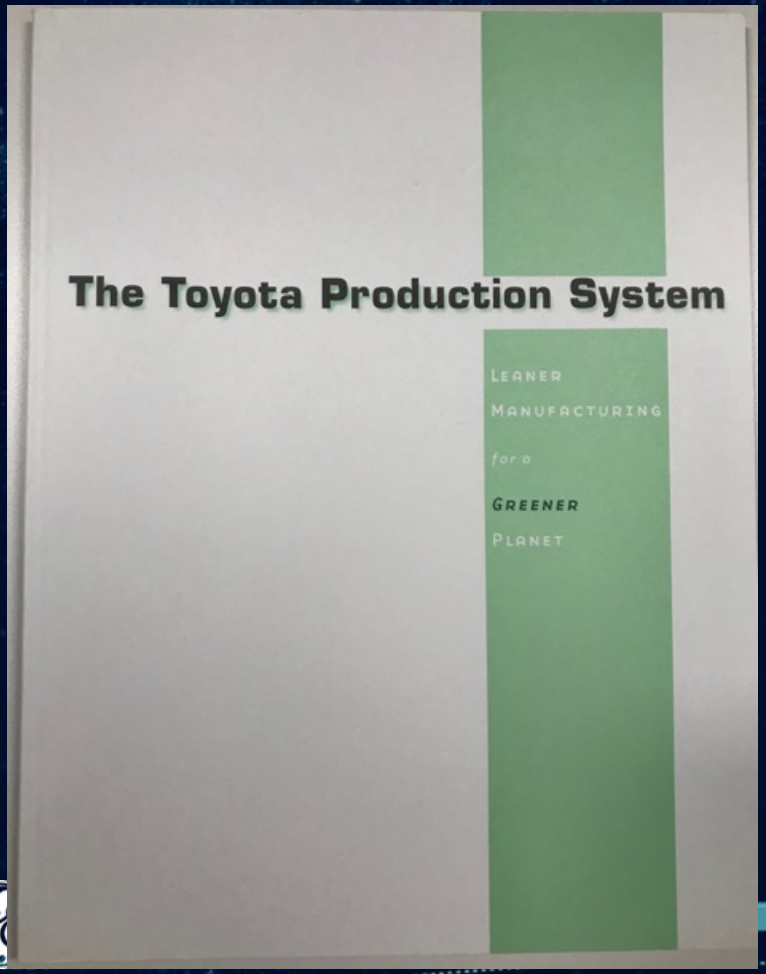
Joseph Juran

Quality Management: Planning, Control, Improvement

Management speaks the language of money

The "Pareto Principle"

The Toyota Production System



Productivity: It's a matter of Life and Death!

Companies that are more efficient than their competitors in providing customers with high-quality goods and services will thrive. Companies that are less efficient than their competitors will perish.

Of course, all companies must provide customers with world-class quality. And they must provide prompt delivery and service. Customers won't accept anything less. The globalization of markets means they don't have to accept anything less.

The Toyota Production System is a framework of concepts and methods for enhancing corporate vitality. It enables companies to achieve continual gains in **productivity** while satisfying customers' expectations for **quality** and **prompt delivery**.

Eliminating waste (and thereby raising quality)

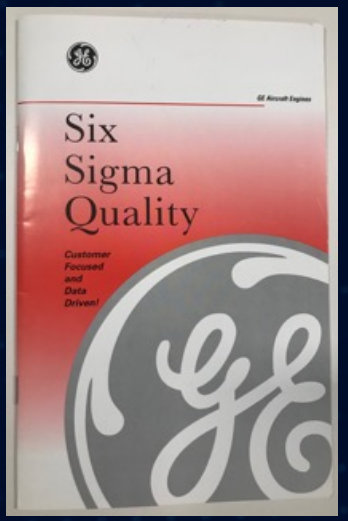
Basically, the Toyota Production System provides for **eliminating waste** in the ways that companies employ human resources, equipment, and material. Managers and employees learn to question the need for every work-sequence motion, for every item of in-process stock, for every second that people, material, or machines spend idle. By eliminating waste in those and other categories, companies concentrate resources on making and delivering only what the customer wants, only when the customer wants it, and only in the amount the customer wants.

Quality rises along with productivity when people learn to identify and eliminate waste. That is because a big part of eliminating waste consists of preventing defects. Defective products entail a grievous waste of human resources, equipment, and material. And measures for eliminating waste by preventing defects are a definitive feature of the Toyota Production System.

By identifying waste and eradicating it, companies can reduce their **costs**. Managers formerly regarded costs as a "given" that was largely beyond their control and prices as a variable that they could adjust to accommodate fluctuations in costs. But in the intensely competitive global markets of today, buyers—rather than sellers—are the arbiters of price. The only way for companies to survive and

Six Sigma

Steve Abrahamson, BSME, MBA, CEM, CSSBB, CSSMBB



Six Sigma - for Process Improvement (developed by Motorola)

Six Sigma is an organizational structure that concentrates on continuous improvement…to achieve goals and objectives **set** by the organization…keeping costs and defect rate at a minimal point.

Six Sigma success is based on five key **principles**: Focus on customer requirements, understanding sources of variation, eliminating variation, and continually improving the process.

"S**ix sigma quality**" = 3.4 defects per million opportunities (DPMO).

Design for Six Sigma - for Product Design Improvement (developed by Texas Instruments)

Determining the needs of customers and the business, and driving those needs into the product solution…gaining a deep insight into customer needs and using these to inform every design decision and trade-off.

DFSS seeks to avoid manufacturing/service process problems by designing products such that they are aligned with process capabilities, to increase product and service effectiveness in the eyes of the customer.

Quality in a Regulated Industry

FDA Quality System Regulation – 21 CFR Part 820

Current good manufacturing practice (CGMP) requirements are set forth in this quality system regulation…The requirements in this section are intended to ensure that finished devices will be safe and effective and otherwise in compliance with the Federal Food, Drug, and Cosmetic Act…

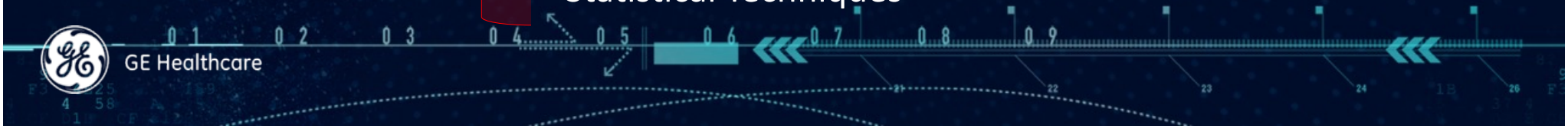
Quality System = Safe and Effective Devices with minimal risk to patient harm

GE Healthcare

Sections in the FDA Quality System Regulation

Relevant to
Good Cyber Practices
(GCP) ?

- Design Controls
- Document Controls
- Purchasing Controls
- Identification and Traceability
- Production Processes and Controls
- Acceptance Activities
- Non-Conforming Product
- Labeling and Packaging Control
- Handling, Storage, Distribution, and Installation
- Records (including Complaint files)
- Servicing
- Statistical Techniques



Key Cyber Interfaces with the Med Device QMS

Pre-Market:

- Design Inputs
- Risk Management
- V&V

Implications of Agile?

Post Market:

- Surveillance

Enough?

FDA Cybersecurity Guidance – Premarket (02 October 2014)

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

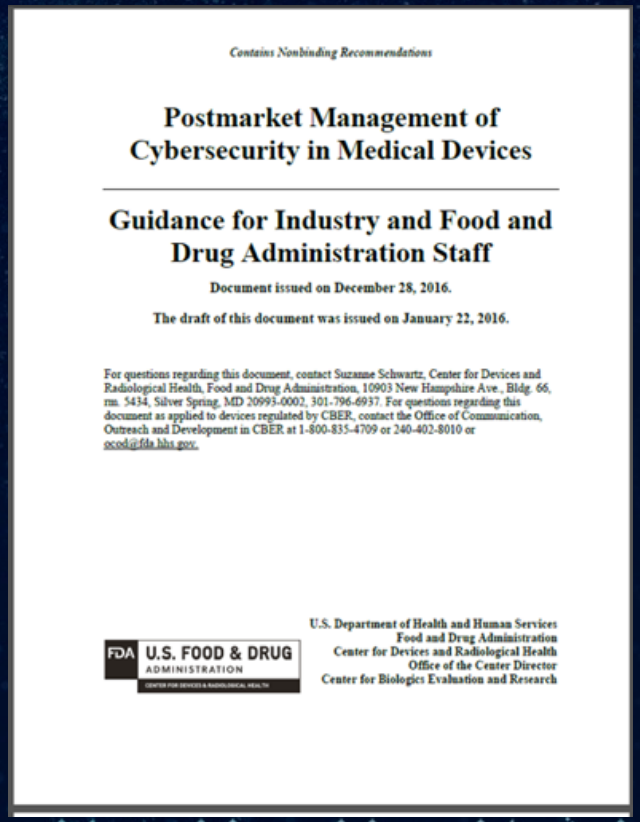
The draft of this document was issued on June 14, 2013.

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

The need for effective cybersecurity to assure medical device functionality and safety has become more important with the increasing use of wireless, Internet- and network- connected devices, and the frequent electronic exchange of medical device-related health information. This guidance has been developed by the FDA to assist industry by identifying issues related to cybersecurity that manufacturers should consider in the design and development of their medical devices as well as in preparing premarket submissions for those devices.

FDA Cybersecurity Guidance – Postmarket
(28 December 2016)



Contains Nonbinding Recommendations

Postmarket Management of Cybersecurity in Medical Devices

Guidance for Industry and Food and Drug Administration Staff

Document issued on December 28, 2016.

The draft of this document was issued on January 22, 2016.

For questions regarding this document, contact Suzanne Schwartz, Center for Devices and Radiological Health, Food and Drug Administration, 10903 New Hampshire Ave., Bldg. 66, rm. 5434, Silver Spring, MD 20993-0002, 301-796-6937. For questions regarding this document as applied to devices regulated by CBER, contact the Office of Communication, Outreach and Development in CBER at 1-800-835-4709 or 240-402-8010 or ocod@fda.hhs.gov.

FDA U.S. FOOD & DRUG ADMINISTRATION

U.S. Department of Health and Human Services
Food and Drug Administration
Center for Devices and Radiological Health
Office of the Center Director
Center for Biologics Evaluation and Research

A growing number of medical devices are designed to be networked to facilitate patient care. Networked medical devices, like other networked computer systems, incorporate software that may be vulnerable to cybersecurity threats. The exploitation of vulnerabilities may represent a risk to health and typically requires continual maintenance throughout the product life cycle to assure an adequate degree of protection against such exploits. Proactively addressing cybersecurity risks in medical devices reduces the overall risk to health.

This guidance clarifies FDA's postmarket recommendations and emphasizes that manufacturers should monitor, identify, and address cybersecurity vulnerabilities and exploits as part of their postmarket management of medical devices.

Revisiting Total Quality and Security

GE Healthcare

Product Cyber Security: What Customers Want

Built-in Product Security

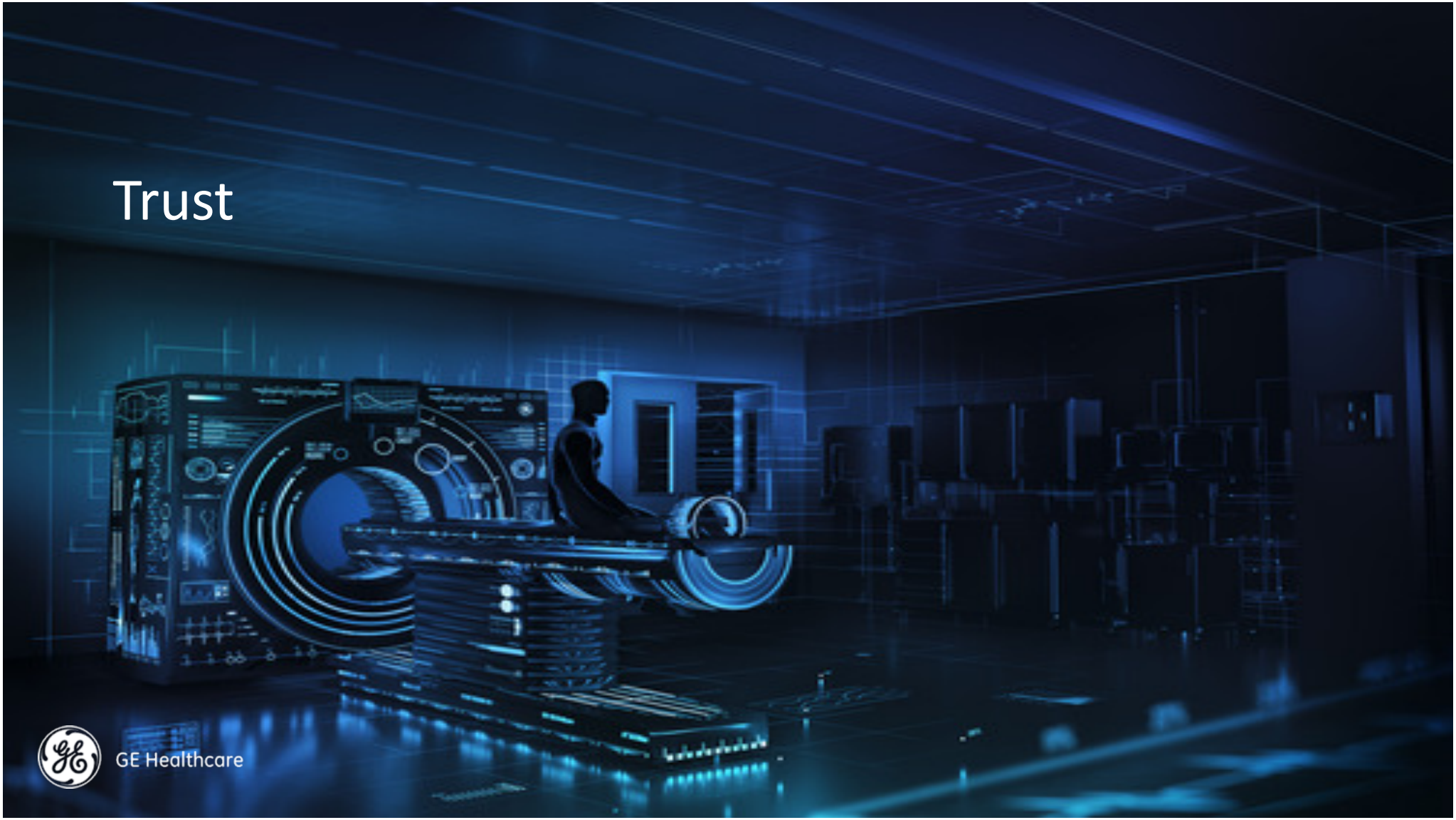
- Security Control Features
- Hardened Devices / Free of Vulnerabilities

Security Awareness within Contract

- Data Transparency
- Defined Roles and Obligations

Operational Support Plan

- Enable and Support Secure Operation
- S/W Updates and Patches for Vulnerabilities


Trust
GE Healthcare

Security and Trust

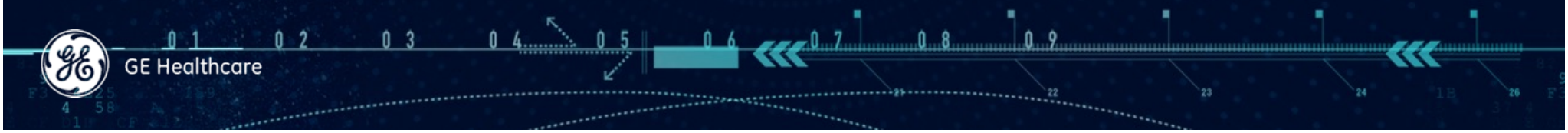
Trust is the firm belief in the reliability, truth, ability, or strength of someone or something.

"relations have to be built on trust"

Quality is about Trust

Security is about Zero Trust

Security must be considered part of Quality to establish Trust between Health Delivery Organizations and Medical Device Manufacturers



From FDA DRAFT Guidance:

Content of Premarket Submissions for Management of Cybersecurity in Medical Devices

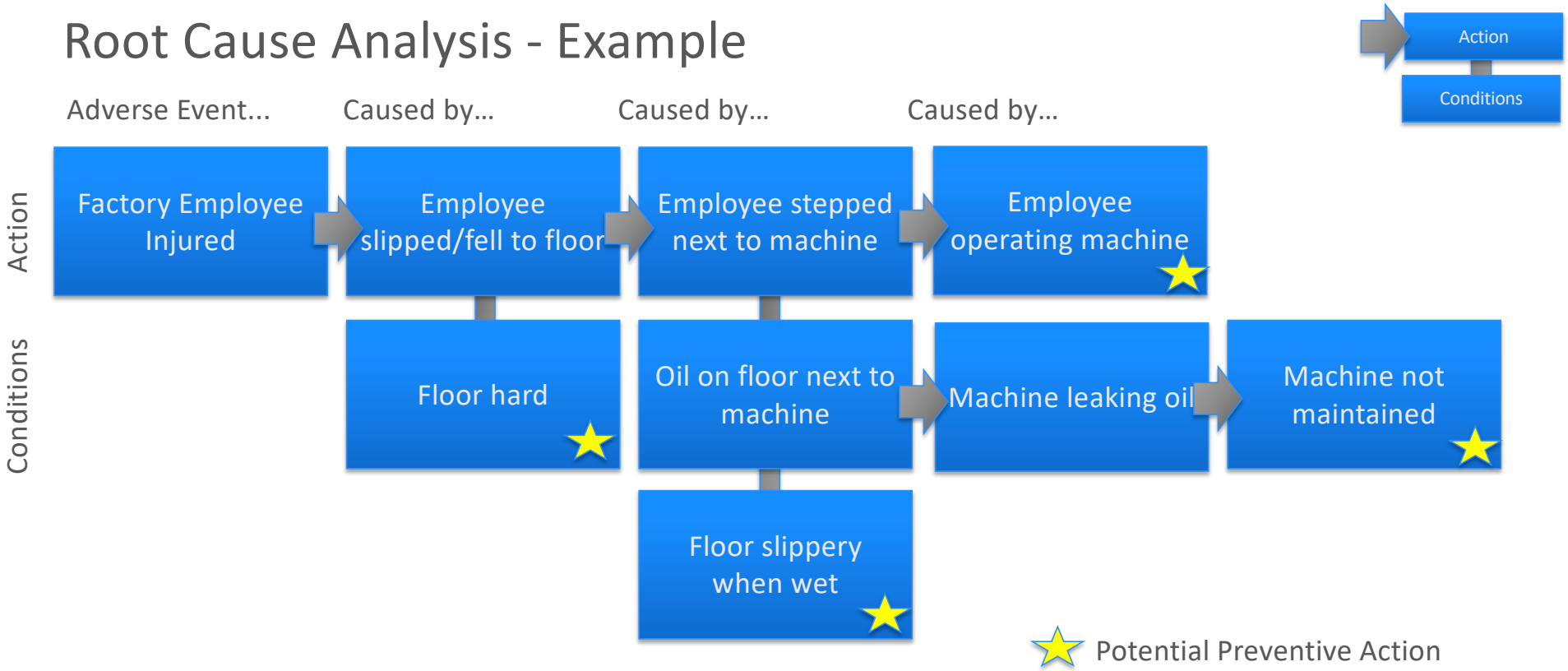
V. Designing a Trustworthy Device: Application of NIST Cybersecurity Framework

As mentioned in Section IV, for software devices, documentation related to design controls, and specifically design validation and software validation and risk analysis in 21 CFR 820.30(g), is often necessary to provide a reasonable assurance of safety and effectiveness in a premarket submission. For devices with cybersecurity risks, we recommend that manufacturers design devices that are trustworthy because trustworthy devices may be more likely to meet their applicable statutory standard for premarket review and because trustworthy devices are more likely to remain safe and effective throughout their life-cycle. Trustworthy devices: (1) are reasonably secure from cybersecurity intrusion and misuse; (2) provide a reasonable level of availability, reliability, and correct operation; (3) are reasonably suited to performing their intended functions; and (4) adhere to generally accepted security procedures. In addition, documentation demonstrating the trustworthiness of a device will help FDA more quickly and efficiently assess the device's safety and effectiveness with respect to cybersecurity.

A "Trustworthy Device" works as intended, and is designed for security

Root Cause Analysis

Root Cause Analysis - Example

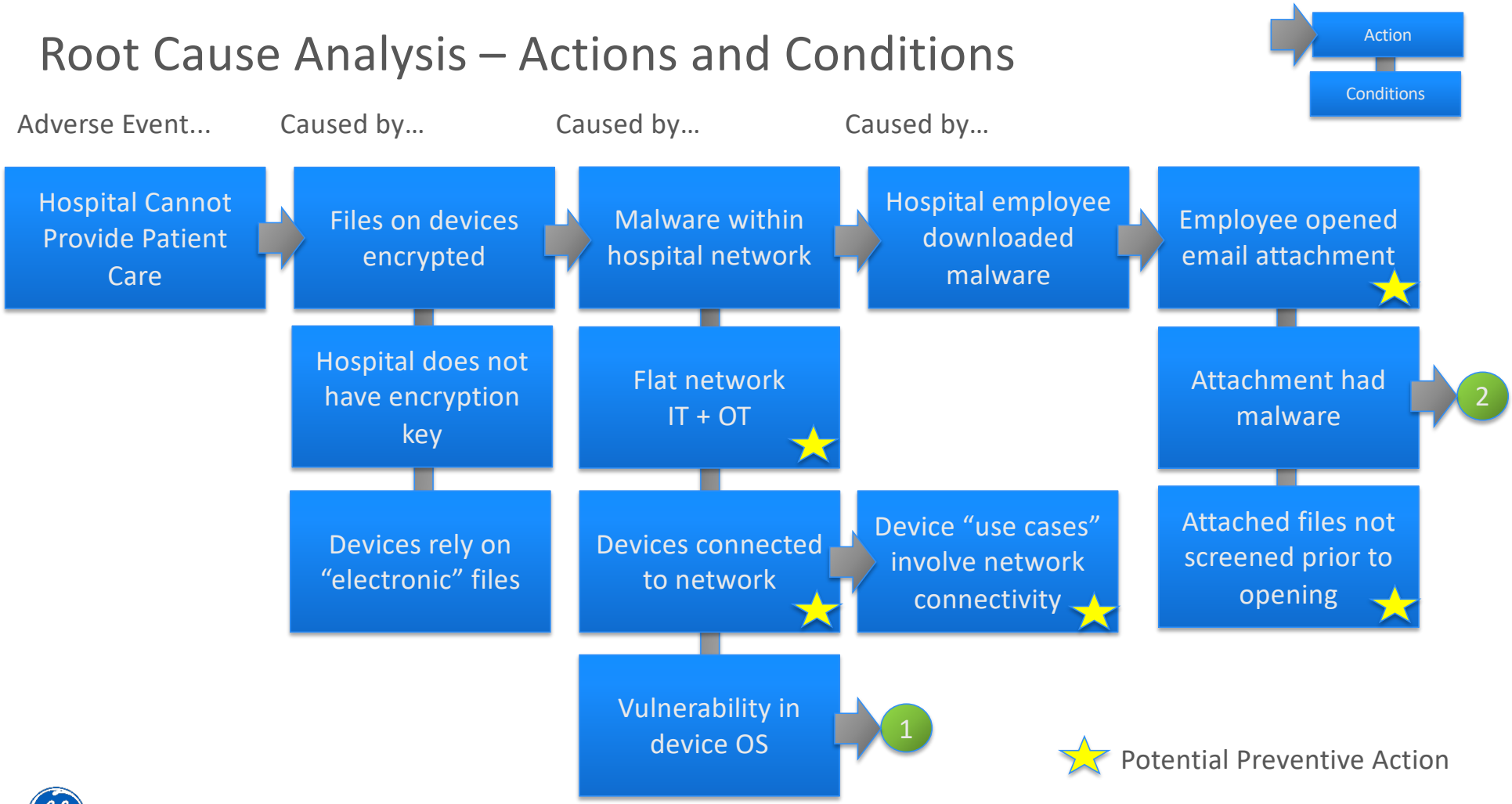


Note: Consider Action and Conditions - easier to fix conditions than to control actions!

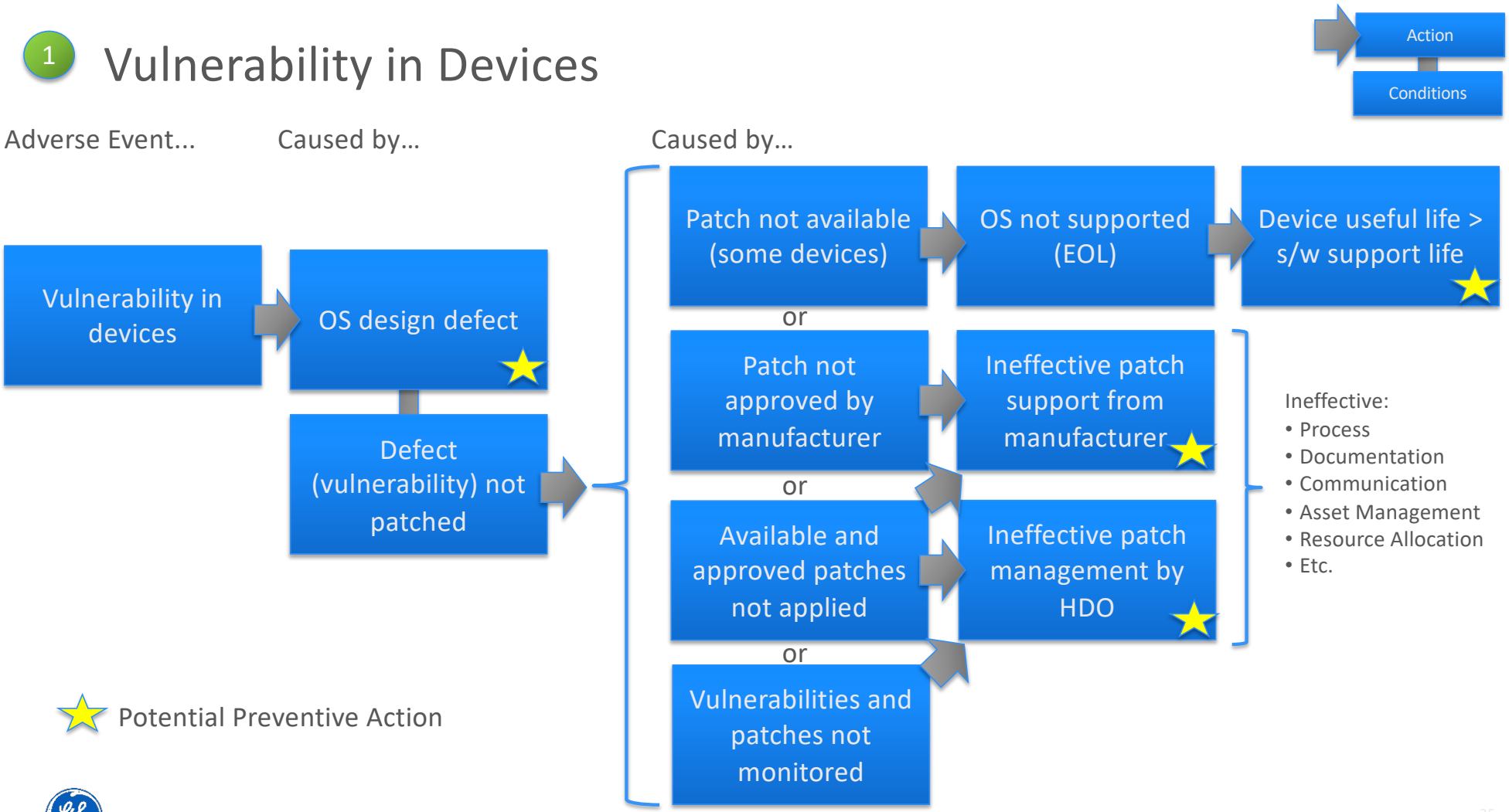
Scenario

- Hospital Operations are Shut Down Due to a Ransomware Attack
- All file on devices and in network storage are encrypted
- Malicious Threat Actors demand payment for key
- Hospital is forced to cease patient care operations until resolution

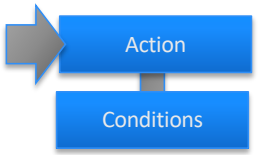
Root Cause Analysis – Actions and Conditions



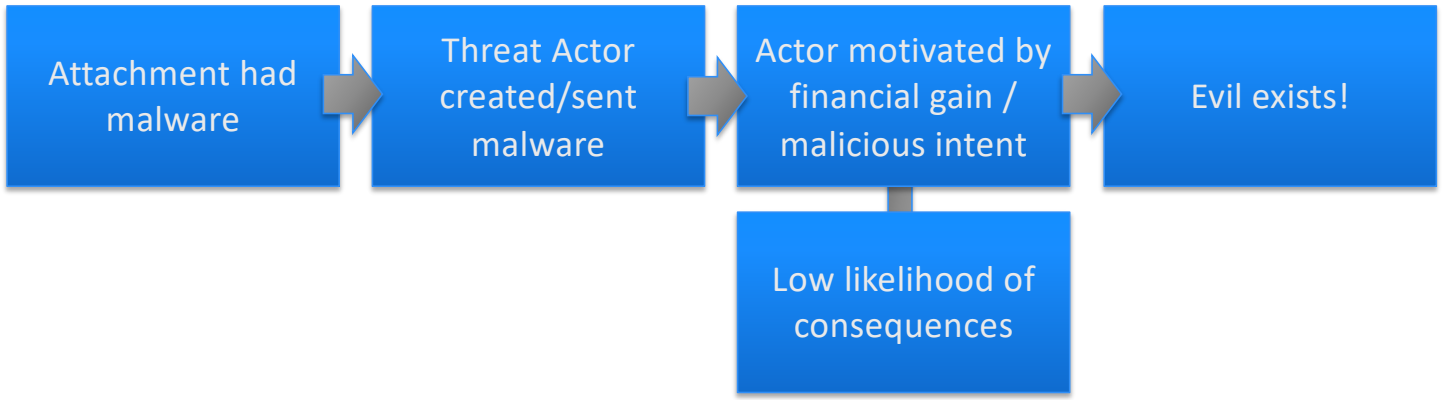
1 Vulnerability in Devices



2 Attachment had Malware



Adverse Event... Caused by… Caused by…



Potential Preventive Action ?

05 April 2018

…a majority of security professionals in the healthcare and pharmaceutical industries admit that they have had a data breach because of an unpatched vulnerability for which a patch was available.

This was one startling finding of a survey of nearly 3,000 security professionals across industries and countries by the Ponemon Institute on behalf of ServiceNow.

A full 77 percent of respondents said that their organizations do not have enough staff to patch vulnerabilities in a timely manner, while 60 percent said they would hire more staff to help with patching in the next 12 months.

However, adding cybersecurity staff may not always be possible…According to nonprofit IT advocacy group ISACA, the global shortage of cybersecurity professionals will reach 2 million by 2019.


Finding Solutions
GE Healthcare

A Quality Approach for Med Device Cyber Security

1. Consider user needs that include cyber security
2. Broaden risk management to cyber mis-use

Implement a structured process within Design engineering for Privacy and Security

3. Design devices to support security throughout the useful life of the device
4. Anticipate the need for routine security updates to deployed devices

Consider life cycle support during design, and implement strong patching processes

5. Consider multiple stakeholders and regulators with different requirements
6. Develop a “systems” view of patient care impact

Transparency and Collaboration to Implement Solutions

Quality and Medical Device Cyber Security

Traditional:
Conformance to specifications
Meeting the needs of the customer

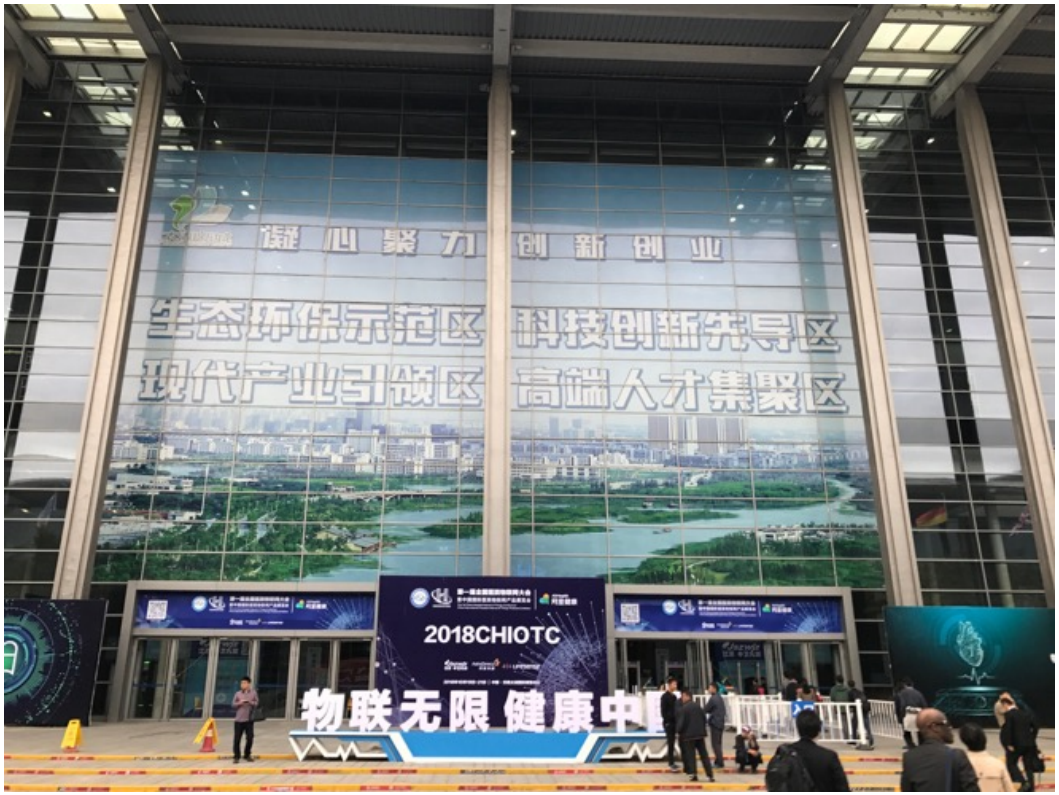
Regulatory:
Managing risks to patient care and safety

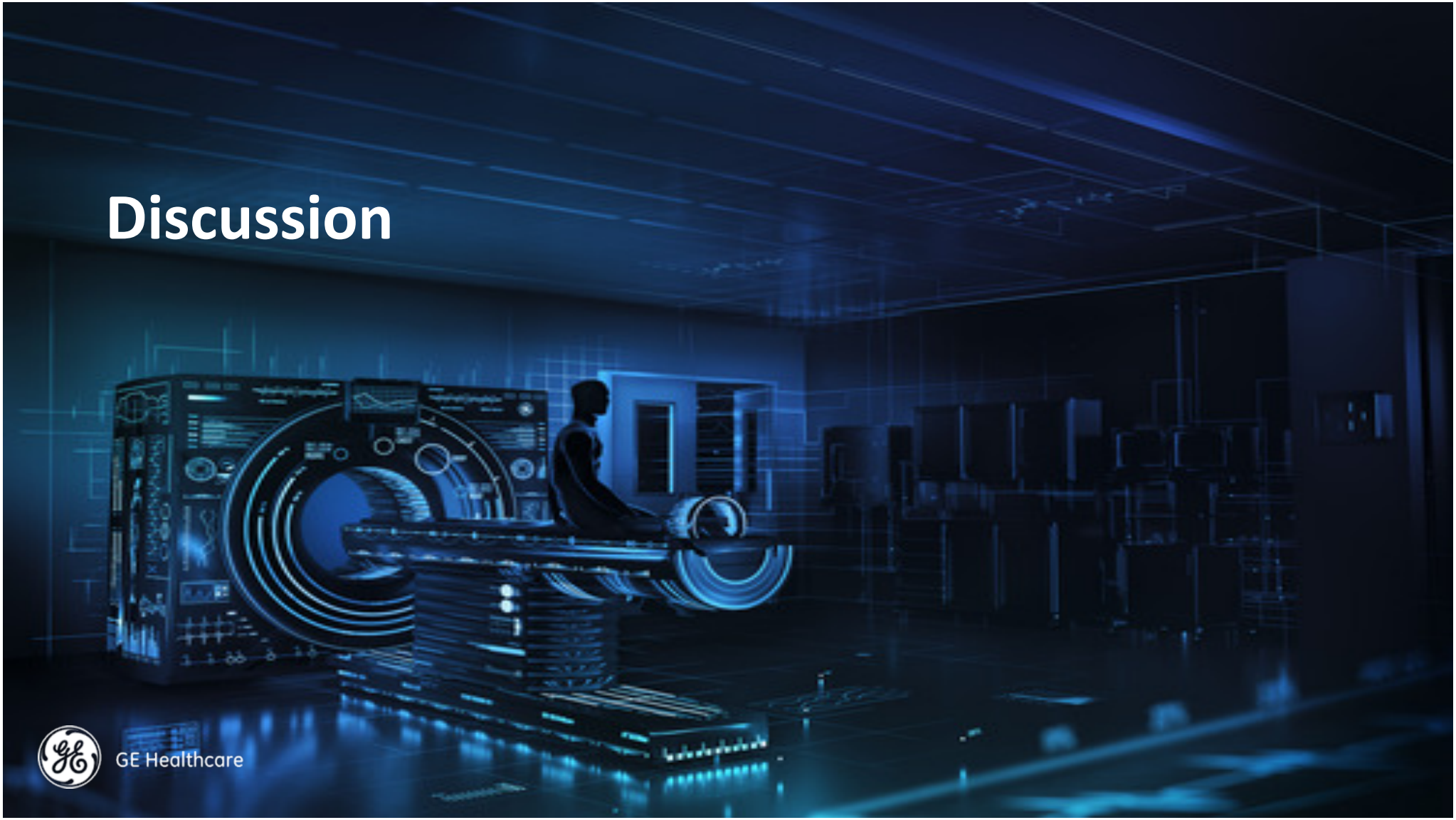
As designed

As used

China Healthcare IoT Conference – Interest in Security!

(Steve in Shanghai / Wuxi - 20 October 2018)




Discussion
GE Healthcare