



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

Copyright © 2018 by GE Healthcare
Permission granted to INCOSE to publish and use.

How Systems Engineering Can Reduce Cost & Improve Quality

1-2 May, 2019 Twin Cities, Minnesota

#hwgsec

25th anniversary
Annual INCOSE
International symposium
Seattle, WA
July 13 - 18, 2013

INCOSE

New SE systems-security responsibility: how is this being accepted?

IS15 Panel, Seattle, WA
14~July 15:30-16:55

Panel:

- **Rick Dove, INCOSE Fellow, CEO/CTO PSI, Inc. and Stevens Inst. of Tech.**
- **Steve Abrahamson, Dir. of Product Security Engineering, GE Healthcare.**
- **Kristen Baldwin. Principal Deputy to the Deputy Assistant Secretary of Defense for Systems Engineering, Office of the US Under Secretary of Defense for Acquisition.**
- **Dawn Beyer, PMP, CISSP, CSSLP, CISM. Lockheed Martin Fellow.**
- **Don Gelosh, Dir. SE Programs, Worcester Polytechnic Institute.**

Steve Abrahamson, BSME, MBA, CEM



GE Healthcare



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



GE

F3 25

4 58

1 18

CE



Career Path

HARM



Preventing Harm



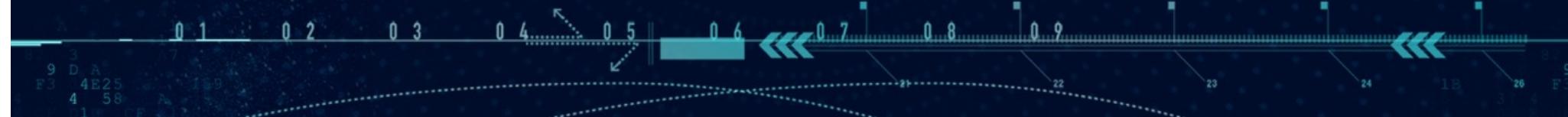
GE Healthcare



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

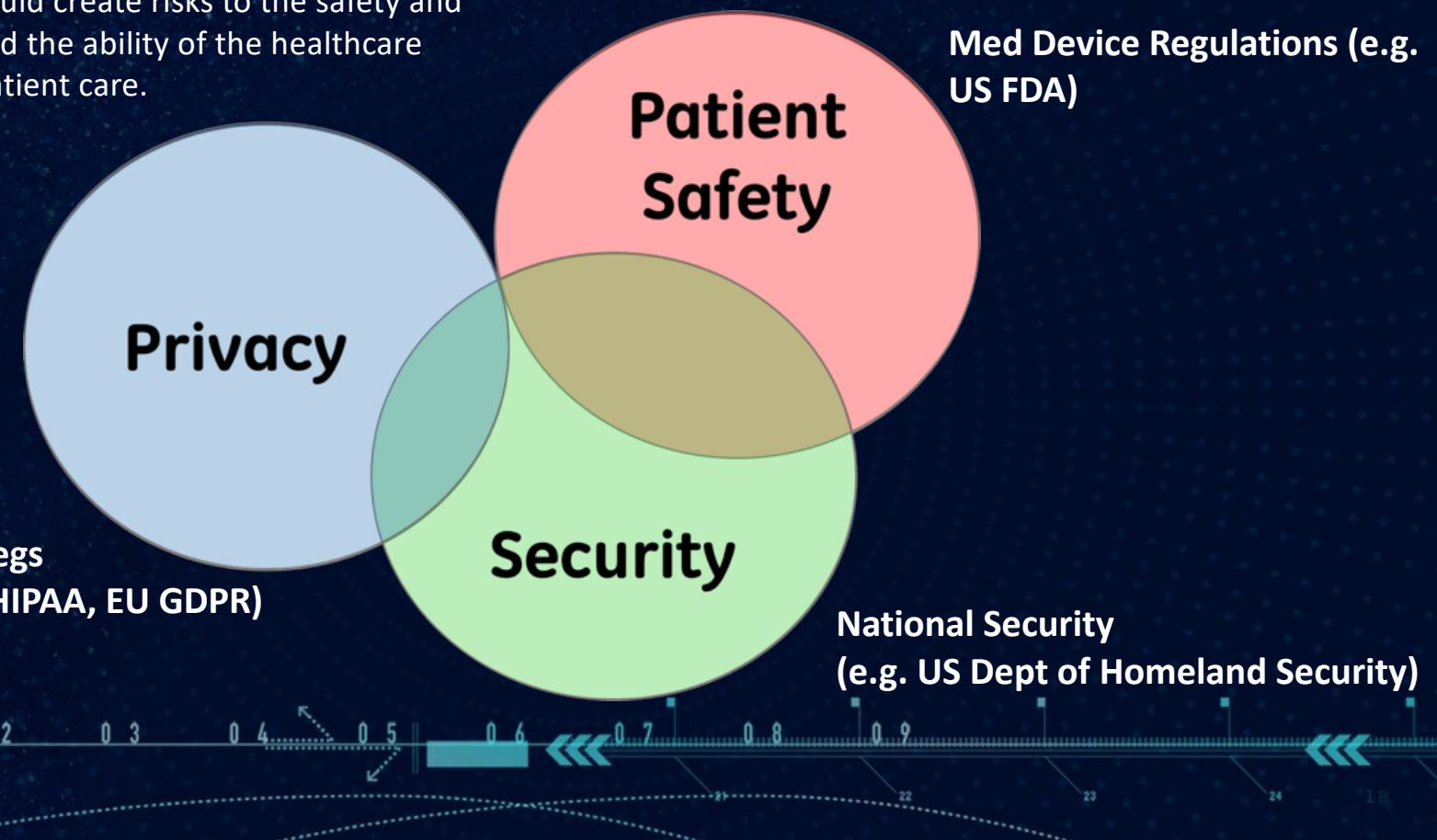
“Cyberspace. A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts... A graphic representation of data abstracted from banks of every computer in the human system. Unthinkable complexity. Lines of light ranged 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.



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  8+ | August 15, 2013



GE Healthcare



Privacy Risk

Medscape 15 October 2018

The screenshot shows the Medscape homepage with a news article. The article title is "Healthcare Providers Are Common Source of Data Breaches" by Tinker Ready, published on September 28, 2018. Below the article, there is a red callout box containing a statement about data breaches. A red arrow points from the word "Note: US Data" to the beginning of the statement. The statement reads: "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." The Medscape navigation bar includes links for NEWS & PERSPECTIVE, DRUGS & DISEASES, CME & EDUCATION, ACADEMY, and VIDEOS.

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.



GE Healthcare

F3 25
4 58
1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 189

1 18

Availability Risk (+ safety risk + privacy risk)

The Guardian – 12 May 2017

The screenshot shows a news article from The Guardian. The header includes links for 'sign in', 'become a supporter', 'subscribe', 'search', 'jobs', and 'US edition'. The main title is 'the guardian'. The navigation bar below the header includes links for 'home', 'US', 'politics', 'world', 'opinion', 'sports', 'soccer', 'tech', 'arts', 'lifestyle', 'fashion', 'business', 'travel', 'environment', and a 'browse all sections' button. The article is categorized under 'Cybercrime'. The main headline is 'Massive ransomware cyber-attack hits nearly 100 countries around the world'. Below the headline, a sub-headline reads: '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'. There are two bullet points: '● Global cyber-attack - live updates' and '● 'Accidental hero' finds kill switch to stop spread'. To the left of the main content, there is a sidebar with social sharing icons (Facebook, Twitter, Email, etc.), a note that the article is 2 months old, a comment count of 7,179, and author information: 'Julia Carrie Wong and Olivia Solon in San Francisco'. The date is Friday 12 May 2017 15.57 EDT. Below the sidebar are several small icons. The main content area features a screenshot of a computer screen displaying a 'Statement on reported NHS cyber attack' from the NHS Digital website. The text in the screenshot discusses the ransomware attack and the investigation. To the right of the main content, there is an advertisement for 'Advertisement' featuring a map of the United States with green and yellow dots representing hacked states, with the text 'Do you live in one of the most hacked states?'. The bottom of the page features a horizontal navigation bar with various icons and a footer with the GE Healthcare logo and some numerical data.

Understanding Security Risk Management

$$\text{Risk} = f(\text{asset} \times \text{threats} \times \text{vulnerabilities}) - \text{controls}$$

Asset = data, device

Threats = malicious actions, malware

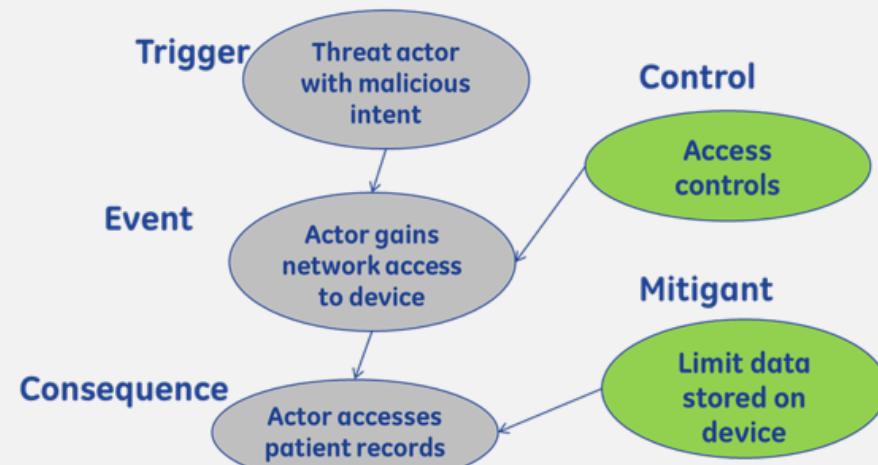
Vulnerabilities = exploitable weaknesses in design

Controls = security safeguards to block exploits

Security Controls

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

A simple network model for risk assessment:



GE Healthcare

F3 25 1 189

4 58

1 18



A New Perspective on Risk

Safety Risk Management:
Protecting people from malfunctioning devices

Security Risk Management:
Protecting devices from malfunctioning people



GE Healthcare



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.



GE Healthcare



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.



GE Healthcare

F3 25
4 58
1 189



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.



GE Healthcare



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"



GE Healthcare

F3 25
4 58
1 189

CP

1 2

2 3

4 5

6 7

8 9

10 11

12 13

14 15

16 17

18 19

20 21

22 23

24 25

26 27

28 29

30 31

32 33

34 35

36 37

38 39

40 41

42 43

44 45

46 47

48 49

50 51

52 53

54 55

56 57

58 59

60 61

62 63

64 65

66 67

68 69

70 71

72 73

74 75

76 77

78 79

80 81

82 83

84 85

86 87

88 89

90 91

92 93

94 95

96 97

98 99

100 101

102 103

104 105

106 107

108 109

110 111

112 113

114 115

116 117

118 119

120 121

122 123

124 125

126 127

128 129

130 131

132 133

134 135

136 137

138 139

140 141

142 143

144 145

146 147

148 149

150 151

152 153

154 155

156 157

158 159

160 161

162 163

164 165

166 167

168 169

170 171

172 173

174 175

176 177

178 179

180 181

182 183

184 185

186 187

188 189

190 191

192 193

194 195

196 197

198 199

200 201

202 203

204 205

206 207

208 209

210 211

212 213

214 215

216 217

218 219

220 221

222 223

224 225

226 227

228 229

230 231

232 233

234 235

236 237

238 239

240 241

242 243

244 245

246 247

248 249

250 251

252 253

254 255

256 257

258 259

260 261

262 263

264 265

266 267

268 269

270 271

272 273

274 275

276 277

278 279

280 281

282 283

284 285

286 287

288 289

290 291

292 293

294 295

296 297

298 299

300 301

302 303

304 305

306 307

308 309

310 311

312 313

314 315

316 317

318 319

320 321

322 323

324 325

326 327

328 329

330 331

332 333

334 335

336 337

338 339

340 341

342 343

344 345

346 347

348 349

350 351

352 353

354 355

356 357

358 359

360 361

362 363

364 365

366 367

368 369

370 371

372 373

374 375

376 377

378 379

380 381

382 383

384 385

386 387

388 389

390 391

392 393

394 395

396 397

398 399

400 401

402 403

404 405

406 407

408 409

410 411

412 413

414 415

416 417

418 419

420 421

422 423

424 425

426 427

428 429

430 431

432 433

434 435

436 437

438 439

440 441

442 443

444 445

446 447

448 449

450 451

452 453

454 455

456 457

458 459

460 461

462 463

464 465

466 467

468 469

470 471

472 473

474 475

476 477

478 479

480 481

482 483

484 485

486 487

488 489

490 491

492 493

494 495

496 497

498 499

500 501

502 503

504 505

506 507

508 509

510 511

512 513

514 515

516 517

518 519

520 521

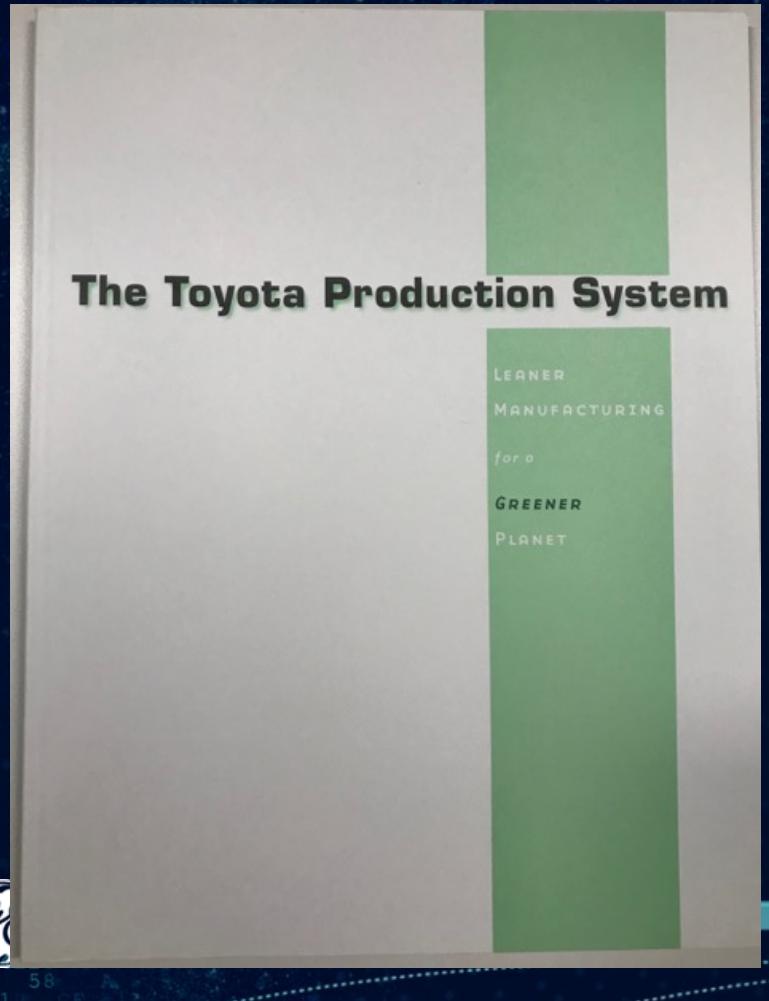
522 523

524 525

526 527

528 529

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

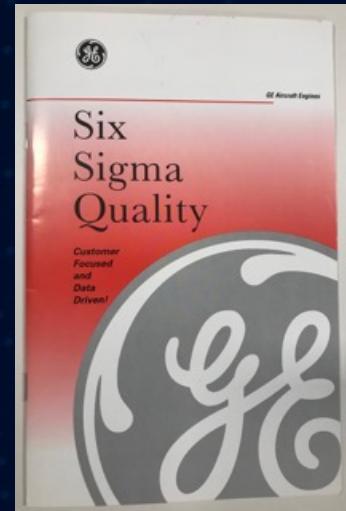
Steve Abrahamson, BSME, MBA, CEM, CSSBB, CSSMBB

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.

"Six 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



GE Healthcare

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



GE Healthcare

0 1 0 2 0 3 0 4 0 5 0 6 0 7 0 8 0 9 21 22 23 24 18 26 F3 25 189 4 58 1 188

Key Cyber Interfaces with the Med Device QMS

Pre-Market:

- Design Inputs
- Risk Management
- V&V

} Implications of Agile?

Post Market:

- Surveillance

} Enough?

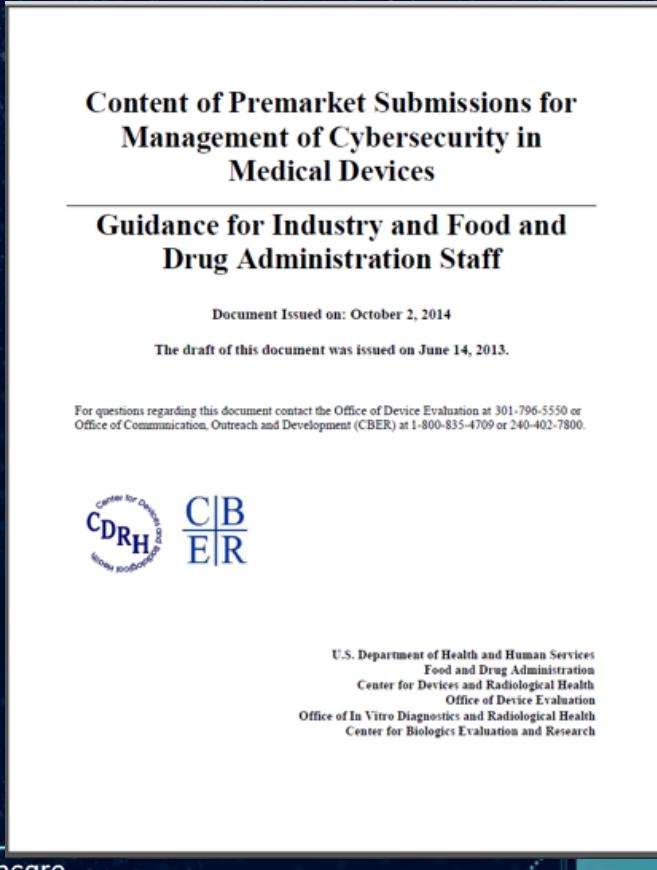


GE Healthcare



FDA Cybersecurity Guidance – Premarket

(02 October 2014)



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.



GE Healthcare

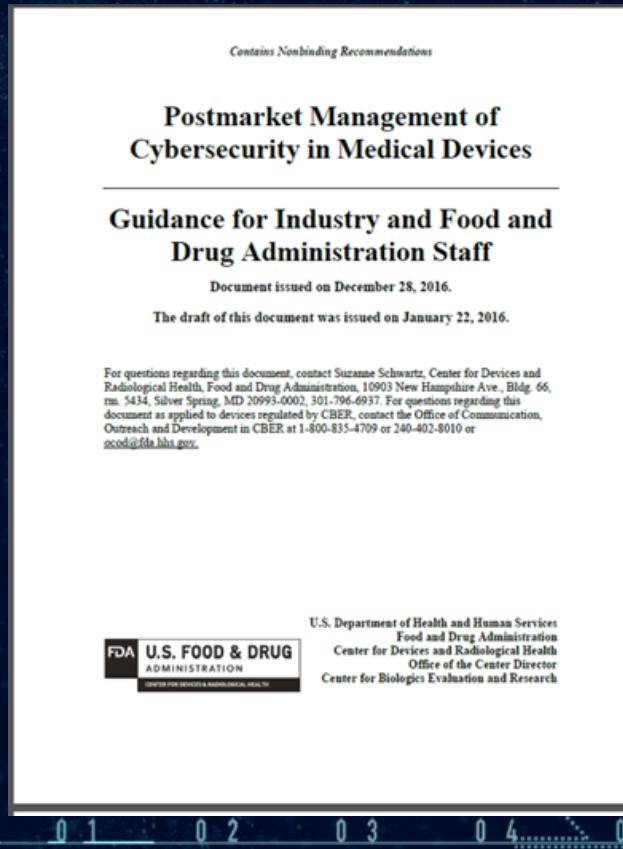
F3 25
4 58
1 189

1 CP

6 7 8 9 21 22 23 24 18 26 F3

FDA Cybersecurity Guidance – Postmarket

(28 December 2016)



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



GE Healthcare



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



GE Healthcare



From FDA DRAFT Guidance: Content of Premarket Submissions for Management of Cybersecurity in Medical Devices

317 **V. Designing a Trustworthy Device: Application of NIST 318 Cybersecurity Framework**

319 As mentioned in Section IV, for software devices, documentation related to design controls,
320 and specifically design validation and software validation and risk analysis in 21 CFR
321 820.30(g), is often necessary to provide a reasonable assurance of safety and effectiveness in a
322 premarket submission. For devices with cybersecurity risks, we recommend that
323 manufacturers design devices that are trustworthy because trustworthy devices may be more
324 likely to meet their applicable statutory standard for premarket review and because trustworthy
325 devices are more likely to remain safe and effective throughout their life-cycle. Trustworthy
326 devices: (1) are reasonably secure from cybersecurity intrusion and misuse; (2) provide a
327 reasonable level of availability, reliability, and correct operation; (3) are reasonably suited to
328 performing their intended functions; and (4) adhere to generally accepted security procedures.
329 In addition, documentation demonstrating the trustworthiness of a device will help FDA more
330 quickly and efficiently assess the device's safety and effectiveness with respect to
331 cybersecurity.
332

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



GE Healthcare

F3 25
4 58
1 189

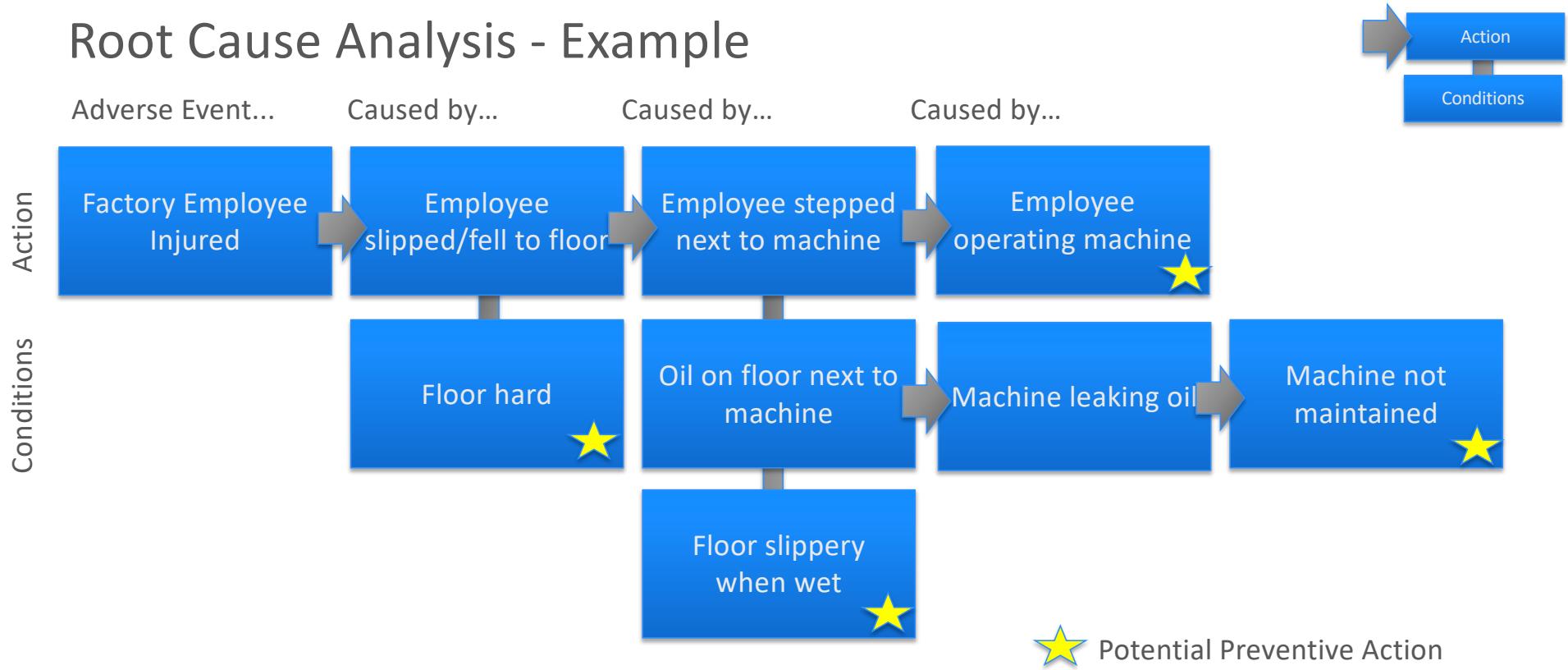


Root Cause Analysis



GE Healthcare

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



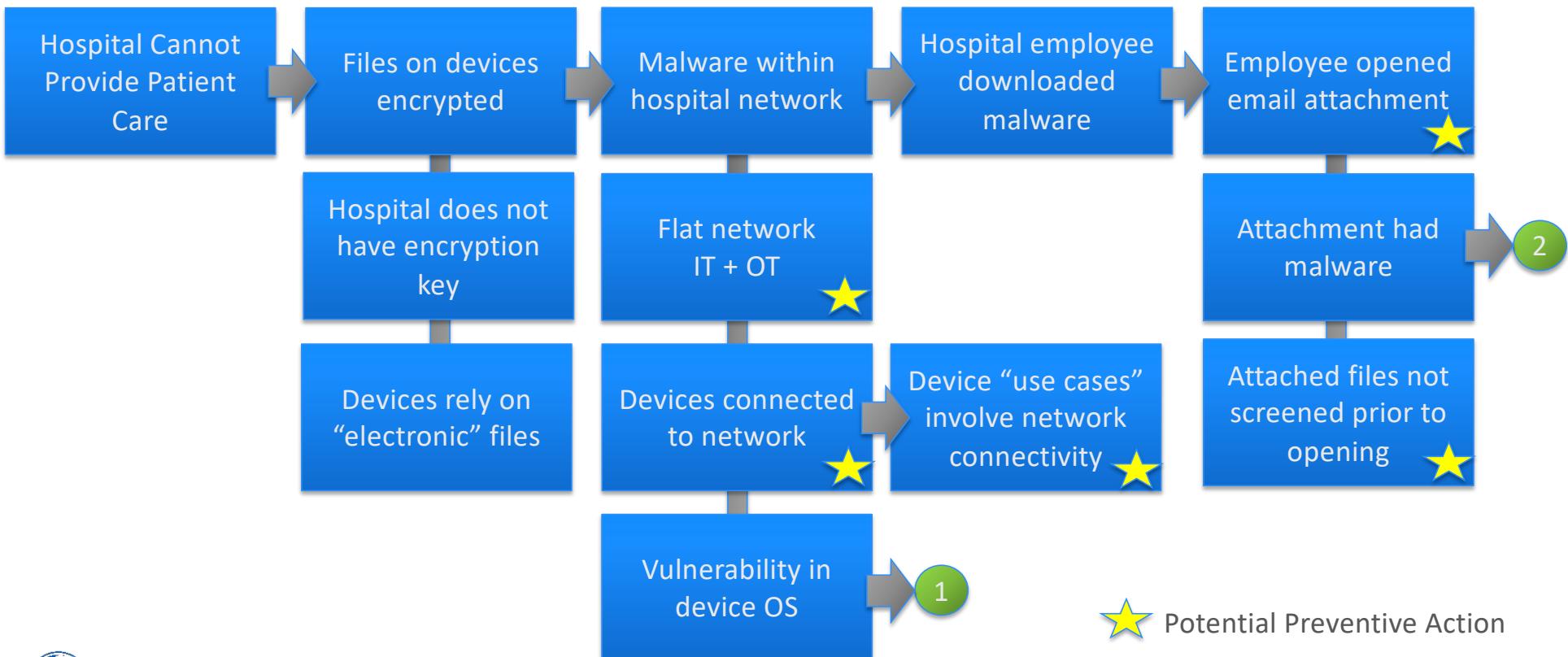
Root Cause Analysis – Actions and Conditions

Adverse Event...

Caused by...

Caused by...

Caused by...



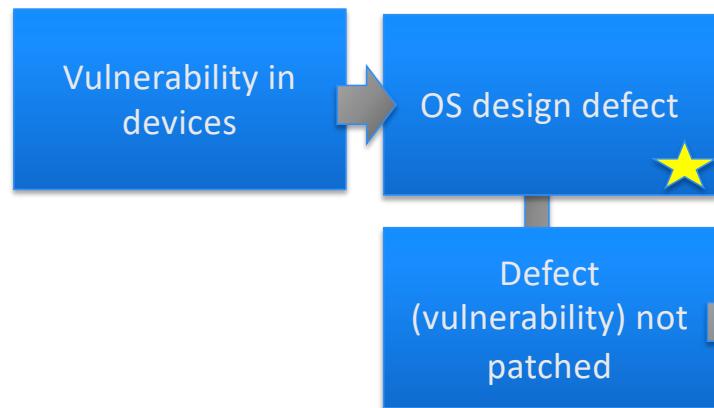
1

Vulnerability in Devices

Adverse Event...

Caused by...

Caused by...



Patch not available
(some devices)

or

Patch not
approved by
manufacturer

Available and
approved patches
not applied

or

Vulnerabilities and
patches not
monitored

OS not supported
(EOL)

Device useful life >
s/w support life

Ineffective patch
support from
manufacturer

Ineffective patch
management by
HDO



Potential Preventive Action

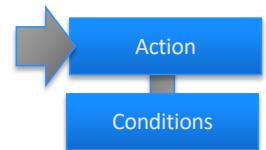
Ineffective:

- Process
- Documentation
- Communication
- Asset Management
- Resource Allocation
- Etc.



2

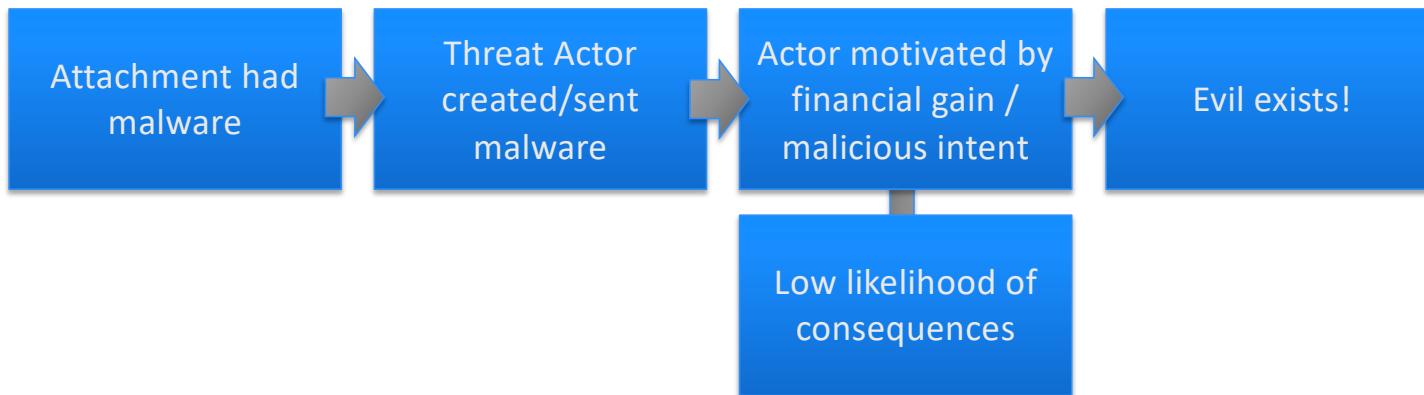
Attachment had Malware



Adverse Event...

Caused by...

Caused by...



Potential Preventive Action ?



05 April 2018



The screenshot shows the HealthITSecurity website. At the top, there is a navigation bar with links to Home, News, Features, Interviews, White Papers & Webcasts, and Events. Below the navigation bar, there is a banner for 'Telehealth 2018' in San Diego, CA, on June 7-8, 2018. The banner includes a photo of Nathaniel Leckman, Esq., Partner, Chair of Telemedicine Industry Team at Foley & Lardner LLP, and a 'REGISTER' button. The main content area is titled 'CYBERSECURITY NEWS' and features an article with the headline 'Survey Finds Lax Patching Practices Feed Healthcare Data Breaches'. The article text states: 'Security professionals admit that they have had a healthcare data breach because of an unpatched vulnerability for which a patch was available.' Below the article is a small image of a digital interface. To the right of the article, there is a sidebar with a box for 'imprivata' featuring 'EPCS Success: Champlain Valley Physicians Hospital of Plattsburgh, NY shares implementation success' and a 'Click to View >' button. There is also a 'Newsletter Signup' button.

...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



GE Healthcare



Quality and Medical Device Cyber Security

Traditional:
Conformance to specifications
Meeting the needs of the customer

Regulatory:
Managing risks to patient care and safety

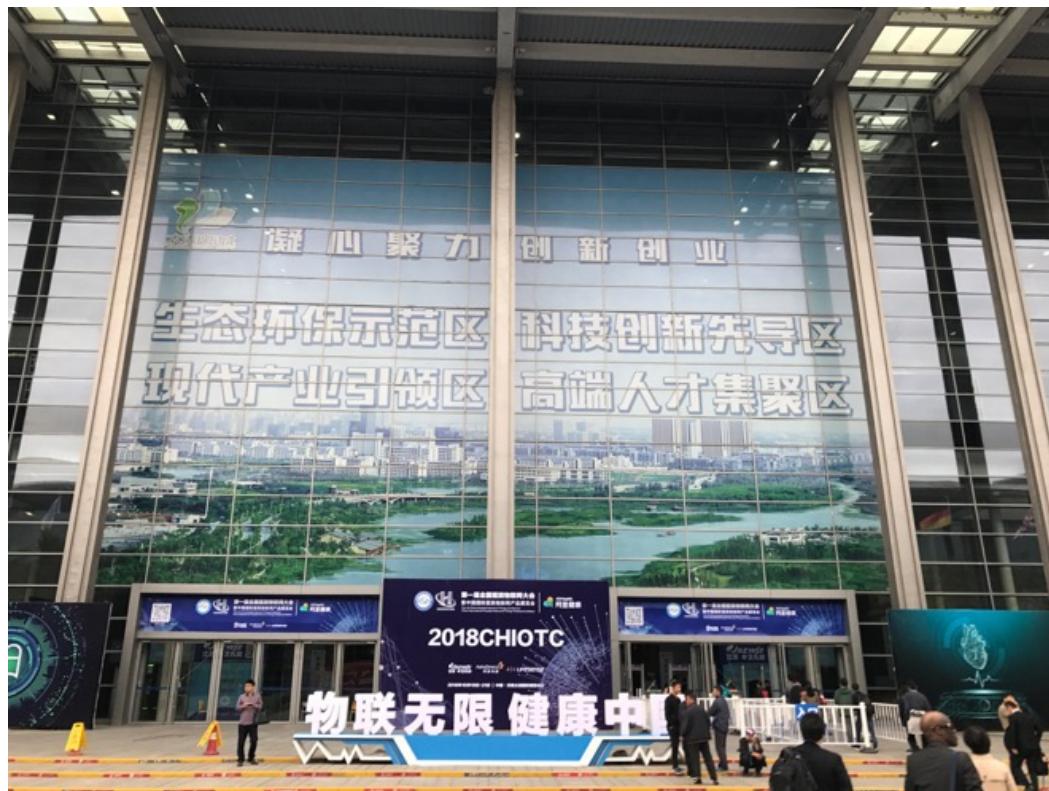
As designed
As used



GE Healthcare



China Healthcare IoT Conference – Interest in Security! (Steve in Shanghai / Wuxi - 20 October 2018)



Discussion



GE Healthcare