William Hagestad II

THE FUTURE OF CYBER WARFARE IN HEALTHCARE

A MedTech Europe event

The MedTech Forum

bringing HealthTech stakeholders together

THE FUTURE OF CYBER WARFARE IN HEALTHCARE

Cybersecurity Engineering

Smiths Medical has an established cyber security engineering team proactively applying both Pre- and post Market Guidance for the cybersecurity of medical devices as encouraged by the Cyber Division of the FDA

Current & Future State:

- Recruit and hired internationally recognized white hat hacker
- Built nationally recognized cyber security engineering program with:
  - No budget, critical thinking, experience and will to succeed;
  - FDA Cyber Directorate requested Smiths Medical leadership:
    - Coordinated Disclosure TTX's in Minneapolis & McClean, VA
  - Disclosed Responsibly 10 CVEs :
    - Advisory (ICSMA-16-306-01)
    - Smiths Medical CADD-Solis Medication Safety Software Vulnerabilities
    - Advisory (ICSMA-17-250-02) Smiths Medical Medfusion 4000 Wireless Syringe Infusion Pump Vulnerabilities (SEP 2017)

- Actively assess medical devices for both clinical and technological cybersecurity cyber threats

Medical Device Cyber Security Maturity

21 MARCH 2016 → **13 JANUARY 2018**

Reactive ⟷ **Proactive**

Blocking & Tackling

- Lack of Executive support
- Underfunded
- Understaffed
- Lack of metrics for reporting
- Set up for failure

Compliance Driven

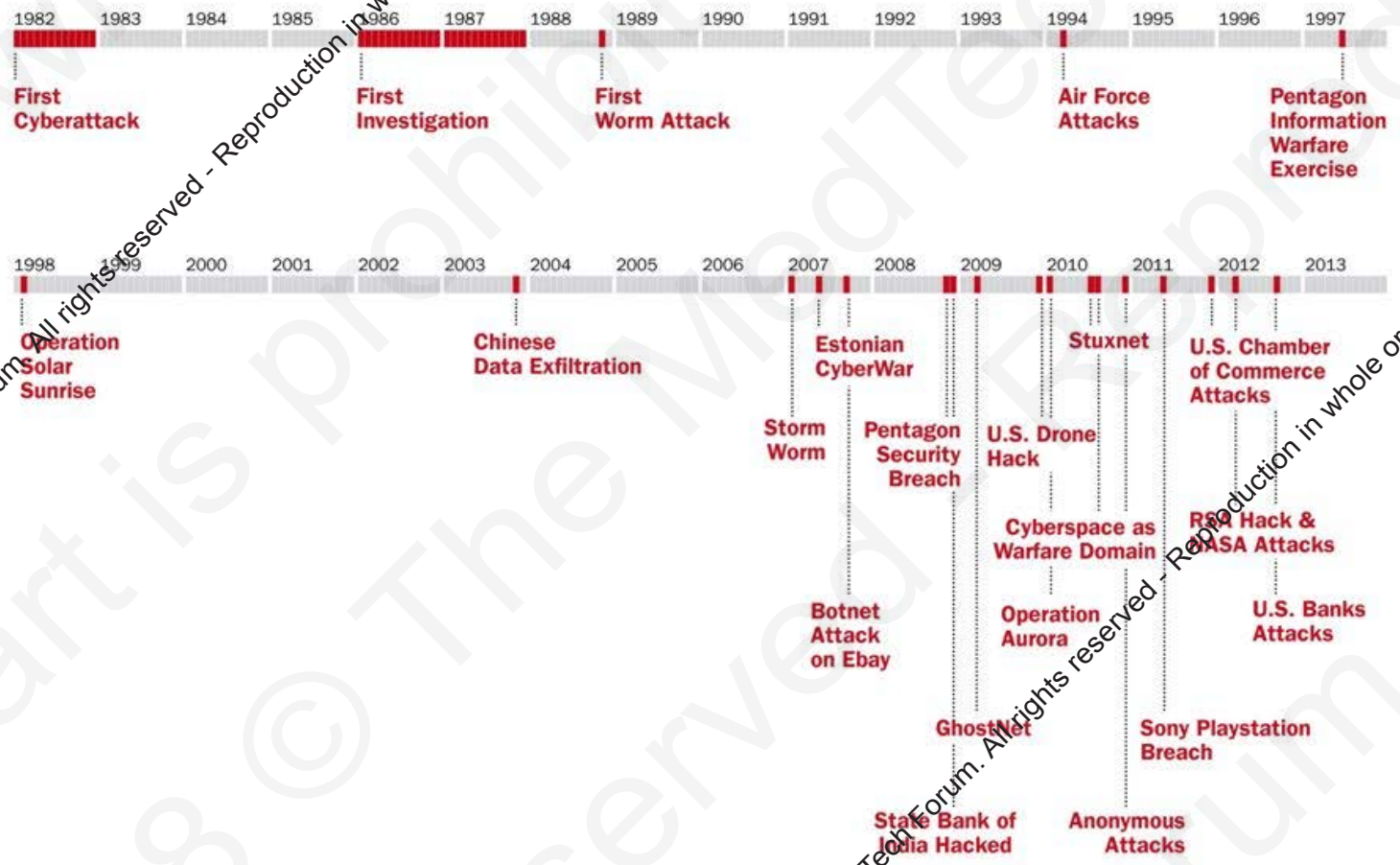
- Control-based security approach
- Align to mandatory regulations
  - EU/PII Data protection
  - FFIEC
  - HIPAA
  - ISO 2700x
  - PCI
  - NCUA

Risk-Based Approach

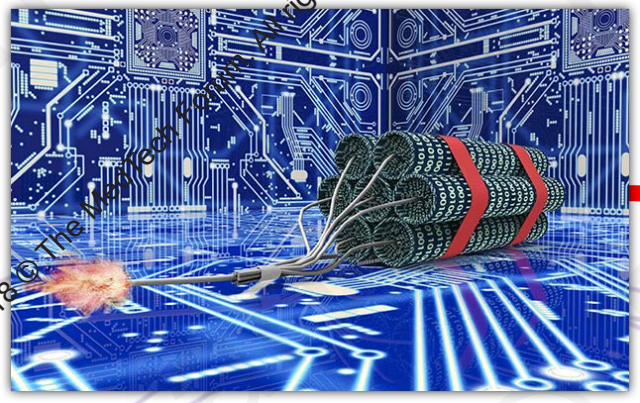
- Multi-layered security and risk-based approach
- Using behavior analytics and evaluating new technologies frequently
- Linking events across multiple disciplines

https://krebsonsecurity.com/2015/04/whats-your-security-maturity-level/

History of Cyber Warfare



https://media.licdn.com/mpr/mpr/AAEAAQAAAAAAAAoPAAAAJDE1MGNjZThhLTgwM2MtNGE5NS1iMDkyLTA3YTc3OGUyZTg4OQ.jpg



Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

September 10, 2015

Alert Number
I-091015-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office.**

Local Field Office Locations:
www.fbi.gov/contact-us/field

INTERNET OF THINGS POSES OPPORTUNITIES FOR CYBER CRIME

The Internet of Things (IoT) refers to any object or device which connects to the Internet to automatically send and/or receive data.

As more businesses and homeowners use web-connected devices to enhance company efficiency or lifestyle conveniences, their connection to the Internet also increases the target space for malicious cyber actors. Similar to other computing devices, like computers or Smartphones, IoT devices also pose security risks to consumers. The FBI is warning companies and the general public to be aware of IoT vulnerabilities cybercriminals could exploit, and offers some tips on mitigating those cyber threats.

What are some IoT devices?

- Automated devices which remotely or automatically adjust lighting or HVAC
- Security systems, such as security alarms or Wi-Fi cameras, including video monitors used in nursery and daycare settings
- Medical devices, such as wireless heart monitors or insulin dispensers
- Thermostats
- Wearables, such as fitness devices
- Lighting modules which activate or deactivate lights
- Smart appliances, such as smart refrigerators and TVs
- Office equipment, such as printers
- Entertainment devices to control music or television from a mobile device
- Fuel monitoring systems

How do IoT devices connect?

IoT devices connect through computer networks to exchange data with the operator, businesses, manufacturers, and other connected devices, mainly without requiring human interaction.

What are the IoT Risks?

Deficient security capabilities and difficulties for patching vulnerabilities in these devices, as well as a lack of consumer security awareness, provide cyber actors with opportunities to exploit these devices. Criminals can use these opportunities to remotely facilitate attacks on other systems, send malicious and spam e-mails, steal personal information, or interfere with physical safety.

https://www.ic3.gov/media/2015/150910.aspx

Adversaries in Cyber Space – A Taxonomy

Introduction

Cyber Adversary Situational Awareness: Nefarious cyber adversaries who are likely to target Smiths-Medical products and services consist of various groups. The Adsversary Taxonomy below details the various threat actor groups, motives, most probable & possible targetrs of opportunity, their cyber attack methodologies and associated compromise capabilities.

Nation State Cyber Capabilities & Motives:

1) Islamic Republic of Iran: Hackers are state sponsored, very nationalistic, and overall very dangerous and destructive in their targeting and capabilities.

2) People's Republic of China (PRC): Hackers are both state sponsored and criminal. Generally Chinese hackers are always very nationalistic. Their capabilities are stealthy, effective and enduring. Chinese hackers will most likely target intellectual property, operational procedures, prodcut design files. Cyber espionage is their forte and they are extremely effective. A burgeoning cyber criminal capability exists and is also a clear and present danger to multi-national enterprises.

3) Russian Federation: Hackers are primarily criminal, although the State will use these hacking capabilities for the projection of force in conjunction with internal Russian law enforcement efforts and countering external threats to the State using military cyber capabilities.

Cyber Threat Actor	Motive	Targets of Opportunity	Methodologies	Capabilities
Nation States ~ Peace Time	Economic, Military, National Secrets, Political	Commercial Enterprises, Intelligence, National Defense, Governments, National	Military & Intel specific cyber doctrine, hacktivists	Asymmetric use of the cyber domain short of kinetic
Nation States ~ War Time	Economic, Military, Political	Commercial Enterprises, Intelligence, National Defense, Governments, National Infrastructure	Military & Intel specific cyber doctrine, hacktivists	Asymmetric use of the cyber domain including kinetic
Cyber Terrorists & Insurgents	Political	Infrastructure, Extortion and Political Processes	Combination of advanced persistent threat (APT)	A developing amd emergeing threat since 2012
Cyber Criminals – Grey & Black Markets	Financial	Intellectual Property Theft, Fraud, Theft, Scams, Hijacked Network & Computer Resources, Cyber Crime for Hire	Exploits, Malware Botnets, Worms & Trojans	Cell-based structure as an APT
Criminal Organizations – RBN	Financial		Use of above with distinct planning	Highly professional, dangerous
Rogue Organizations – Anonymous, LulzSec	Financial Military, National Secrets, Political Noteriety	Intellectual Property Theft, Direct & Indirect pressure from OGA Resources	Organic hacking capabilities unsurpassed	Organized yet de-centralized

Worst Case Scenario…

环球网 军事
mil.huanqiu.com
环球网 > 军事 > 航空航天 > 正文

波音飛機被黑客入侵

美黑客称曾入侵系统操控客机 波音质疑称不真实

2015-05-19 08:57:00 环球网 分享 参与

【环球航空报道】如果飞机的控制系统被黑客入侵，乘飞机还安全吗？据CNN18日报道，一名网络安全顾问向美国联邦调查局承认，他曾多次侵入航空公司的电脑系统，并在飞行途中控制了飞机引擎。

报道称，网络安全人员克里斯·罗伯茨4月发布推特，讨论入侵他乘坐的飞往雪城的航班。美国联合航空公司的安全人员看到这一言论后向FBI举报，罗伯茨随后遭到拘捕。在FBI的传唤调查中，罗伯茨坦言2011至2014年期间曾侵入飞机的娱乐系统15至20次。他还宣称，一旦进入电脑系统，可以对系统进行重新编码，使其能够向飞机发出上升指令。调查报告称，罗伯茨曾经"发出一个爬升指令，使得飞机做出了侧向飞行动作"。另外媒报道称，罗伯茨还在推特上吹嘘称能够控制飞机放下氧气罩。

罗伯茨表示，他掌握三种波音飞机和一种空客飞机的弱点，而他侵入的娱乐系统为泰雷兹公司和松下公司。他认为如此"广而告之"是为了"提高飞行的安全系数"。调查文件显示，FBI的特工与技术专家认为，"罗伯茨有能力和意愿利用携带的设备侵入飞行途中的客机娱乐系统，或许也能够控制任何安装娱乐程序的客机控制系统，这危及了公共安全。"

波音公司质疑这些控制飞机的言论，表示它们的娱乐系统"与飞机的航行系统是不相关的"。该公司还表示，波音飞机不止一个飞行系统。没有飞行员的确认与许可，飞机的飞行系统不会受到任何改变。空客公司目前仍没有做出回应。然而，航空公司已经积极行动起来。英国《每日电讯报》称，美联航上周发起一个活动，向"白客"们，即能够发现公司电脑系统漏洞的友善的黑客，提供一百万英里的免费旅程。▲

用手机继续阅读

Boeing airplane hacked by DHS…

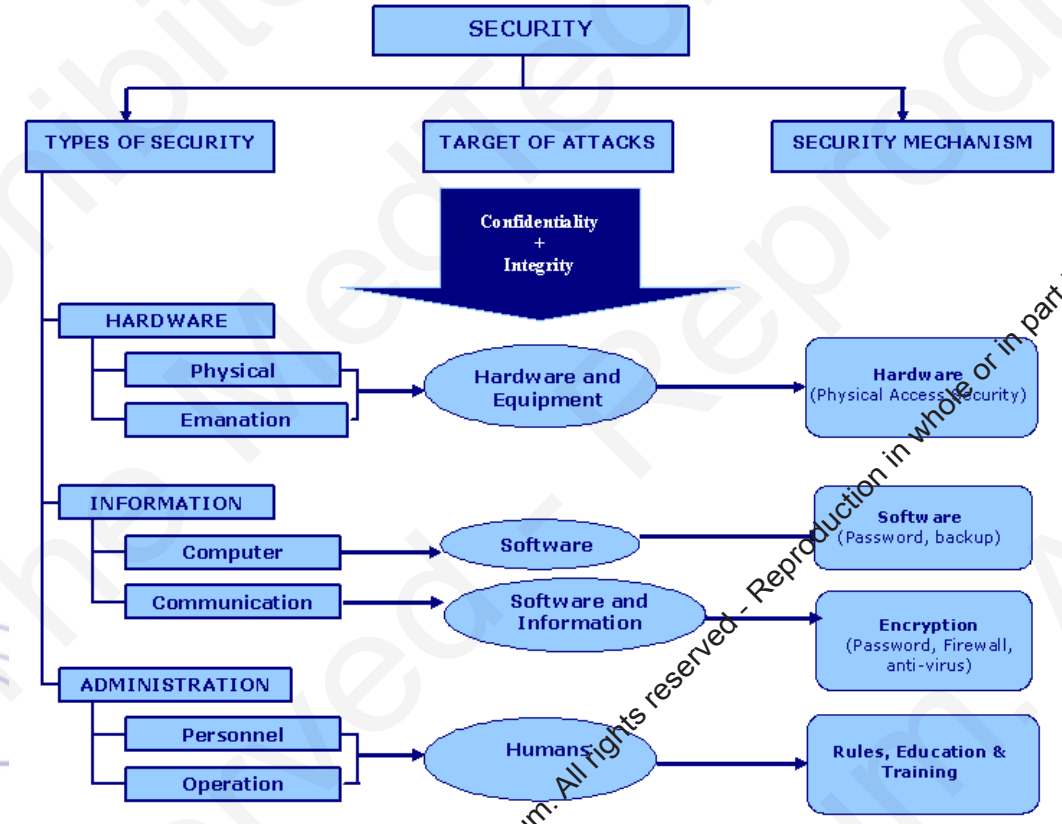
What if…

- HVP onboard aircraft connected to vulnerable medical device…
- Nation State Hacker targets HVP…
- Jumps from hacked medical device…
- To Linux-based inflight entertainment system…
- Jumps from easily compromised inflight entertainment system…
- To aircraft flight controls…
- Controls descent of aircraft…
- Augers aircraft into metropolitan CBD…
- Hacked device becomes part of a WMD

What is Security?

How should it apply to Medical Device Manufacturers (MDM)?

How does it apply to Healthcare delivery Organisations (HDO)?



https://medicaldialogues.in/indian-origin-doctor-warned-against-uk-health-service-cyber-hack/
http://www.intelligentedu.com/computer_security_for_everyone/18-threats-attacks-hackers-crackers.html

2018 © The MedTech Forum. All rights reserved - Reproduction in whole or in part is prohibited.
2018 © The MedTech Forum. All rights reserved - Reproduction in whole or in part is prohibited.

WannaCry

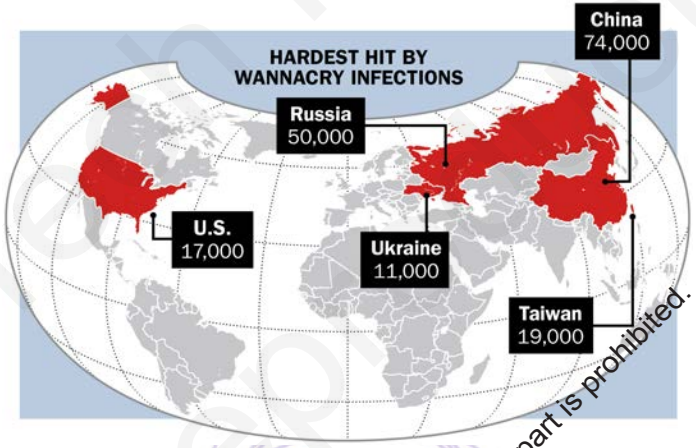
Ransomware Attack

2018 © The MedTech Forum. All rights reserved - Reproduction in whole or in part is prohibited.

2018 © The MedTech Forum. All rights reserved - Reproduction in whole or in part is prohibited.

Ransomware

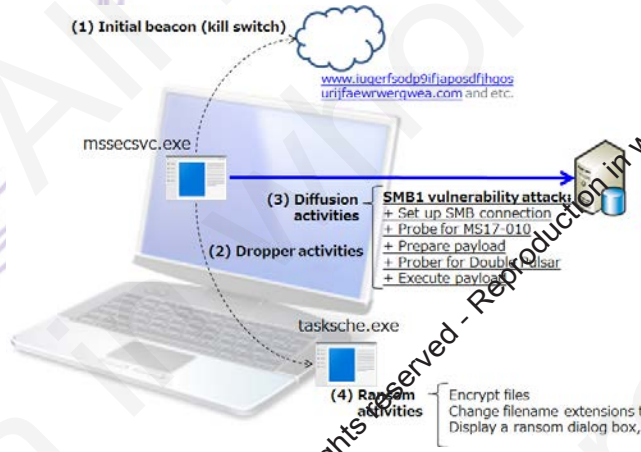
- WannaCry
- Petya/NotPetya

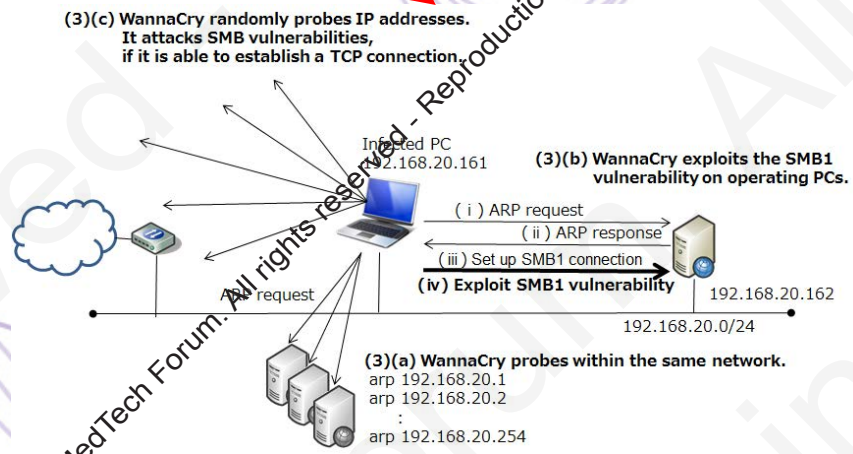


  - Apply common cyber security engineering best practices;
  - Assume any connected device is vulnerable;
  - Become a hard target against skilled adversaries…
  - Fundamental situational awareness….

http://time.com/4783910/why-a-global-cyber-crisis-stalled-this-time/

2018 © The MedTech Forum. All rights reserved - Reproduction in whole or in part is prohibited.
2018 © The MedTech Forum. All rights reserved - Reproduction in whole or in part is prohibited.



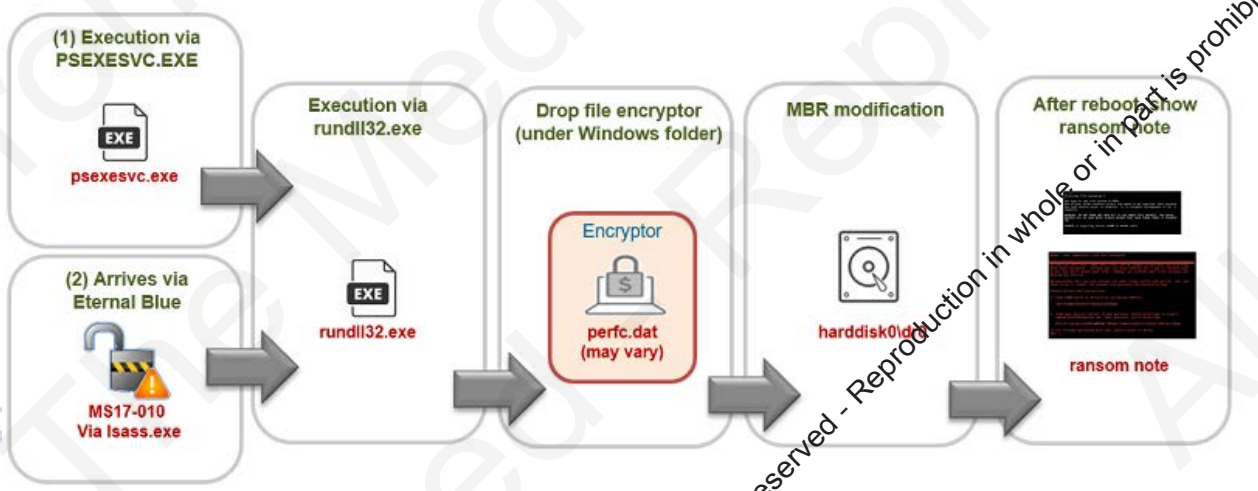


http://www.hitachi.com/hirt/publications/hirt-pub17008/index.html

2018 © The MedTech Forum. All rights reserved - Reproduction in whole or in part is prohibited.

2018 © The MedTech Forum. All rights reserved - Reproduction in whole or in part is prohibited.
2018 © The MedTech Forum. All rights reserved - Reproduction in whole or in part is prohibited.

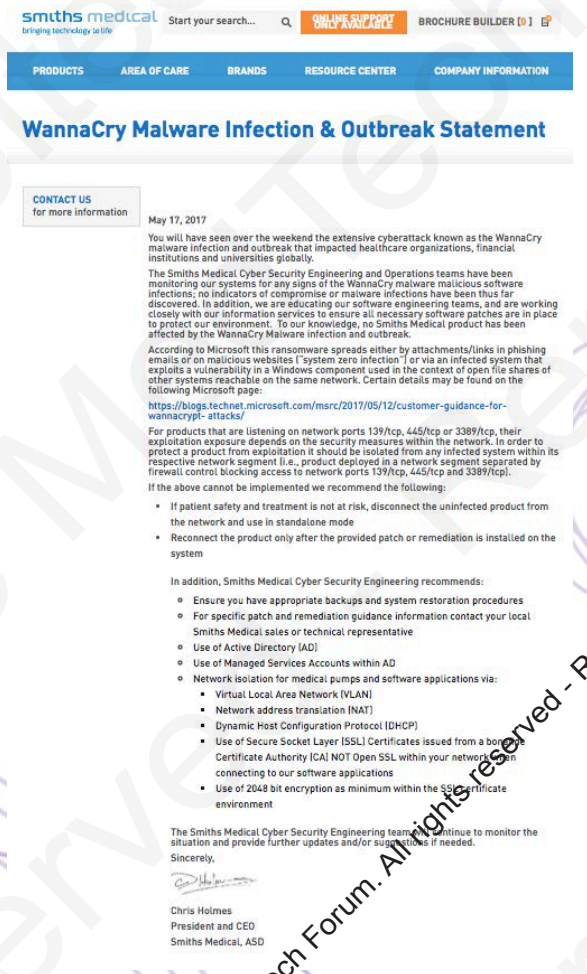
Petya/NotPetya



http://blog.trendmicro.be/wp-content/uploads/2017/06/petya4.png

Active cyber security participation from leadership…

From statement creation to publishing on external website 2 hours –
Incredible even with both CEO traveling, no corporate communications staff and yours truly enroute to an FDA event



smiths medical
bringing technology to life

Start your search...

ONLINE SUPPORT ONLY AVAILABLE

BROCHURE BUILDER (0)

PRODUCTS | AREA OF CARE | BRANDS | RESOURCE CENTER | COMPANY INFORMATION

WannaCry Malware Infection & Outbreak Statement

CONTACT US
for more information

May 17, 2017

You will have seen over the weekend the extensive cyberattack known as the WannaCry malware infection and outbreak that impacted healthcare organizations, financial institutions and universities globally.

The Smiths Medical Cyber Security Engineering and Operations teams have been monitoring our systems for any signs of the WannaCry malware malicious software infections; no indicators of compromise or malware infections have been thus far discovered. In addition, we are educating our software engineering teams, and are working closely with our information services to ensure all necessary software patches are in place to protect our environment. To our knowledge, no Smiths Medical product has been affected by the WannaCry Malware infection and outbreak.

According to Microsoft this ransomware spreads either by attachments/links in phishing emails or on malicious websites ("system zero infection") or via an infected system that exploits a vulnerability in a Windows component used in the context of open file shares of other systems reachable on the same network. Certain details may be found on the following Microsoft page:

https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt- attacks/

For products that are listening on network ports 139/tcp, 445/tcp or 3389/tcp, their exploitation exposure depends on the security measures within the network. In order to protect a product from exploitation it should be isolated from any infected system within its respective network segment (i.e., product deployed in a network segment separated by firewall control blocking access to network ports 139/tcp, 445/tcp and 3389/tcp).

If the above cannot be implemented we recommend the following:

- If patient safety and treatment is not at risk, disconnect the uninfected product from the network and use in standalone mode
- Reconnect the product only after the provided patch or remediation is installed on the system

In addition, Smiths Medical Cyber Security Engineering recommends:

- Ensure you have appropriate backups and system restoration procedures
- For specific patch and remediation guidance information contact your local Smiths Medical sales or technical representative
- Use of Active Directory (AD)
- Use of Managed Services Accounts within AD
- Network isolation for medical pumps and software applications via:
  - Virtual Local Area Network (VLAN)
  - Network address translation (NAT)
  - Dynamic Host Configuration Protocol (DHCP)
  - Use of Secure Socket Layer (SSL) Certificates issued from a bonafide Certificate Authority (CA) NOT Open SSL within your network when connecting to our software applications
  - Use of 2048 bit encryption as minimum within the SSL certificate environment

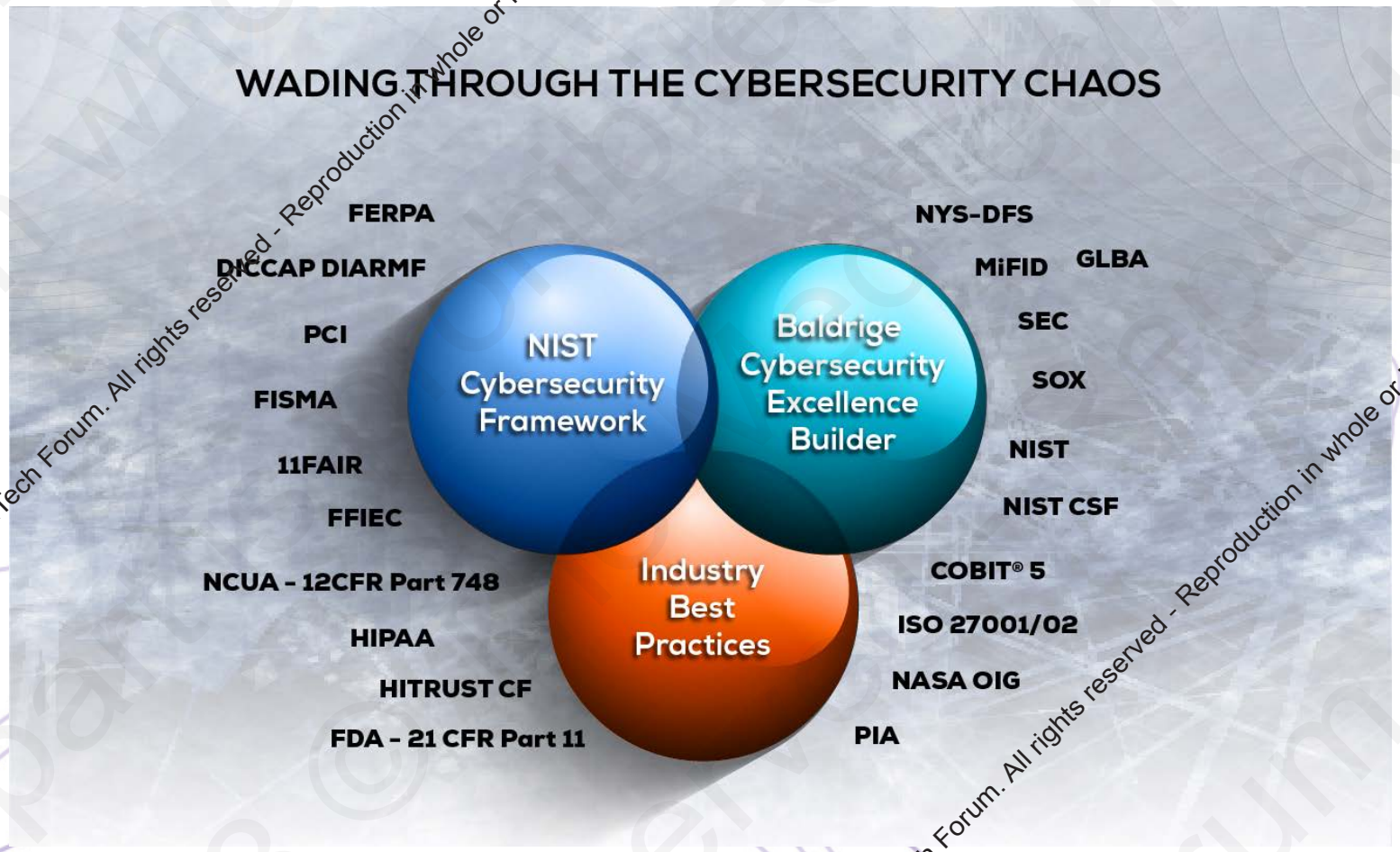
The Smiths Medical Cyber Security Engineering team will continue to monitor the situation and provide further updates and/or suggestions if needed.

Sincerely,

Chris Holmes
President and CEO
Smiths Medical, ASD

2018 © The MedTech Forum. All rights reserved - Reproduction in whole or in part is prohibited.

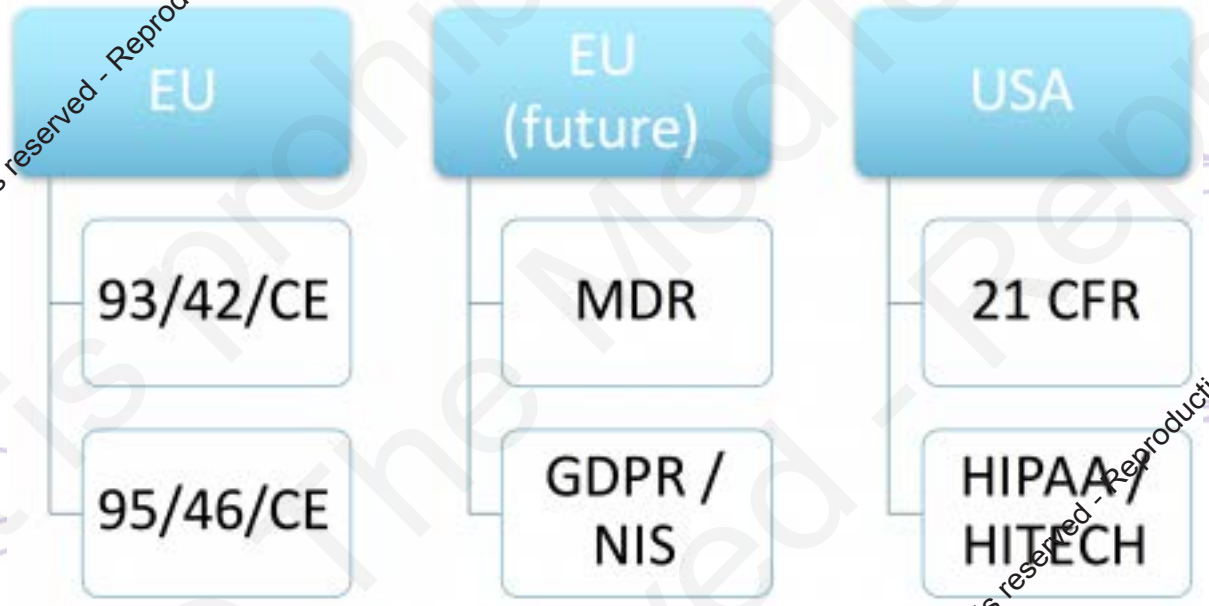
Overwhelming Guidance's & Standards…



https://www.assured.enterprises/nist-baldrige-cybersecurity-guidelines/

2018 © The MedTech Forum. All rights reserved - Reproduction in whole or in part is prohibited.
2018 © The MedTech Forum. All rights reserved - Reproduction in whole or in part is prohibited.

Comparing Medical Device Cybersecurity Requirements:

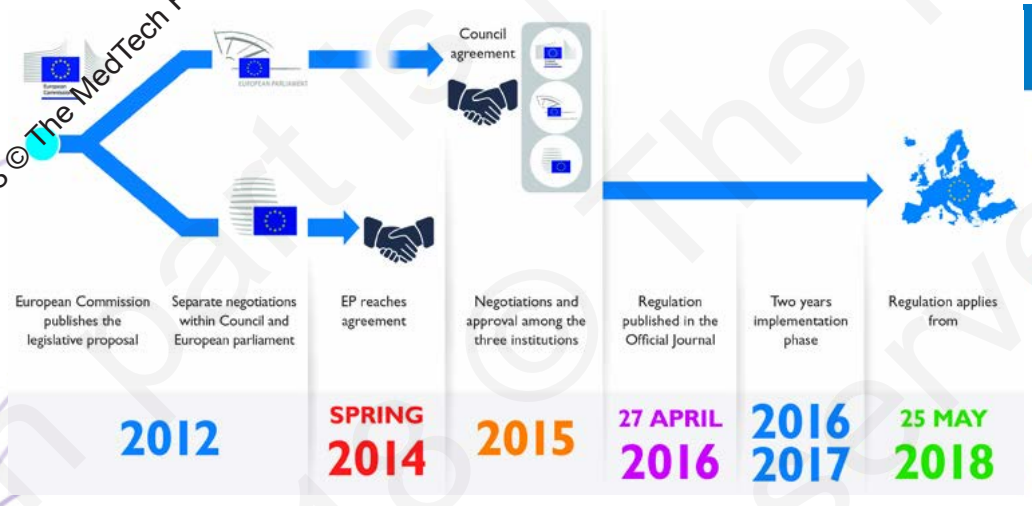


http://blog.cm-dm.com/post/2016/10/24/Cybersecurity-in-medical-devices-Part-1-Regulations

European Union…Protection of Personal Data

- Directive 95/46/EC of the European Parliament and of the Council of **24 October 1995** on the protection of individuals with regard to the processing of personal data and on the free movement of such data…
- **General Data Protection Regulation (GDPR)….**

After four years of preparation and debate the GDPR was **finally approved** by the EU Parliament on **14 April 2016**. It will enter in force 20 days after its publication in the EU Official Journal and will be directly application in all members states two years after this date. Enforcement date: **25 May 2018** - at which time those organizations in non-compliance will face heavy fines.



https://www.eugdpr.org/

https://www.lepide.com/infographics/gdpr-compliance-checklist.html

European Union … Medical Devices Specific

- Applicable Directives – for European Medical Industry
  - Council Directive 93/42/EEC of 14 June 1993 concerning **medical devices** OJ L 169 of 12 July 1993

	Title
2.1 Scope, field of application, definition	MEDDEV 2.1/1 (14 kB) Definitions of "medical devices", "accessory" and "manufacturer" **April 1994**
	MEDDEV 2.1/2 rev.2 (14 kB) Field of application of directive "active implantable medical devices" **April 1994**
	MEDDEV 2.1/2.1 (12 kB) Treatment of Computers Used to Program Implantable Pulse Generators **February 1998**
	MEDDEV 2.1/3 rev.3 (183 kB) Borderline products, drug-delivery products and medical devices incorporating,as integral part, an ancillary medicinal substance or an ancillary human blood derivative **December 2009**
	MEDDEV 2.1/4 (21 kB) Interface with other directives – Medical devices/directive89/336/EEC relating to electromagnetic compatibility and directive 89/686/EEC relating to personal protective equipment **March 1994** For the relation between the MDD and directive 89/686/EEC concerning personal protective equipment, please see the Commission services interpretative document of 21 August 2009 (28 kB)
	MEDDEV 2.1/5 (10 kB) Medical devices with a measuring function **June 1998**
	MEDDEV 2.1/6 (514 kB) Qualification and Classification of stand alone software **July 2016**

While there are Euro Commission directives…

Also, ISO's…

July 2012 EN ISO 14971:2012, Medical devices — Application of risk management to medical devices

American Standards…

May 2016 TIR57 "Principles for medical device security – Risk management"

https://ec.europa.eu/growth/sectors/medical-devices/guidance

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:1993L0042:20071011:en:PDF

2018 © The MedTech Forum. All rights reserved - Reproduction in whole or in part is prohibited.
2018 © The MedTech Forum. All rights reserved - Reproduction in whole or in part is prohibited.

US Food & Drug Administration – Cyber Division

a) Guidance for Industry, FDA Reviewers and Compliance on Off-The-Shelf Software Use in Medical Devices, U.S. Department of Health and Human Services, Food and Drug Administration, Center for Devices and Radiological Health, Office of Compliance, Office of Device Evaluation issued September 9, 1999

b) Guidance for Industry Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software issued January 14, 2005

c) Medical Device Development Tools, Draft Guidance, Food and Drug Administration Staff issued 14 November 2013

d) Content of Premarket Submissions for Management of Cybersecurity in Medical Devices, Guidance for Industry and Food and Drug Administration Staff issued October 2, 2014

e) Infusion Pumps Total Product Life Cycle Guidance for Industry and FDA Staff issued December 2, 2014

f) Postmarket Management of Cybersecurity in Medical Devices, Draft Guidance for Industry and Food and Drug Administration Staff issued on January 22, 2016

g) Updated recommendations on submitting a new 510(k) for device modifications August 5, 2016

h) Deciding When to Submit a 510 K for a software change to an existing device issued August 8, 2016

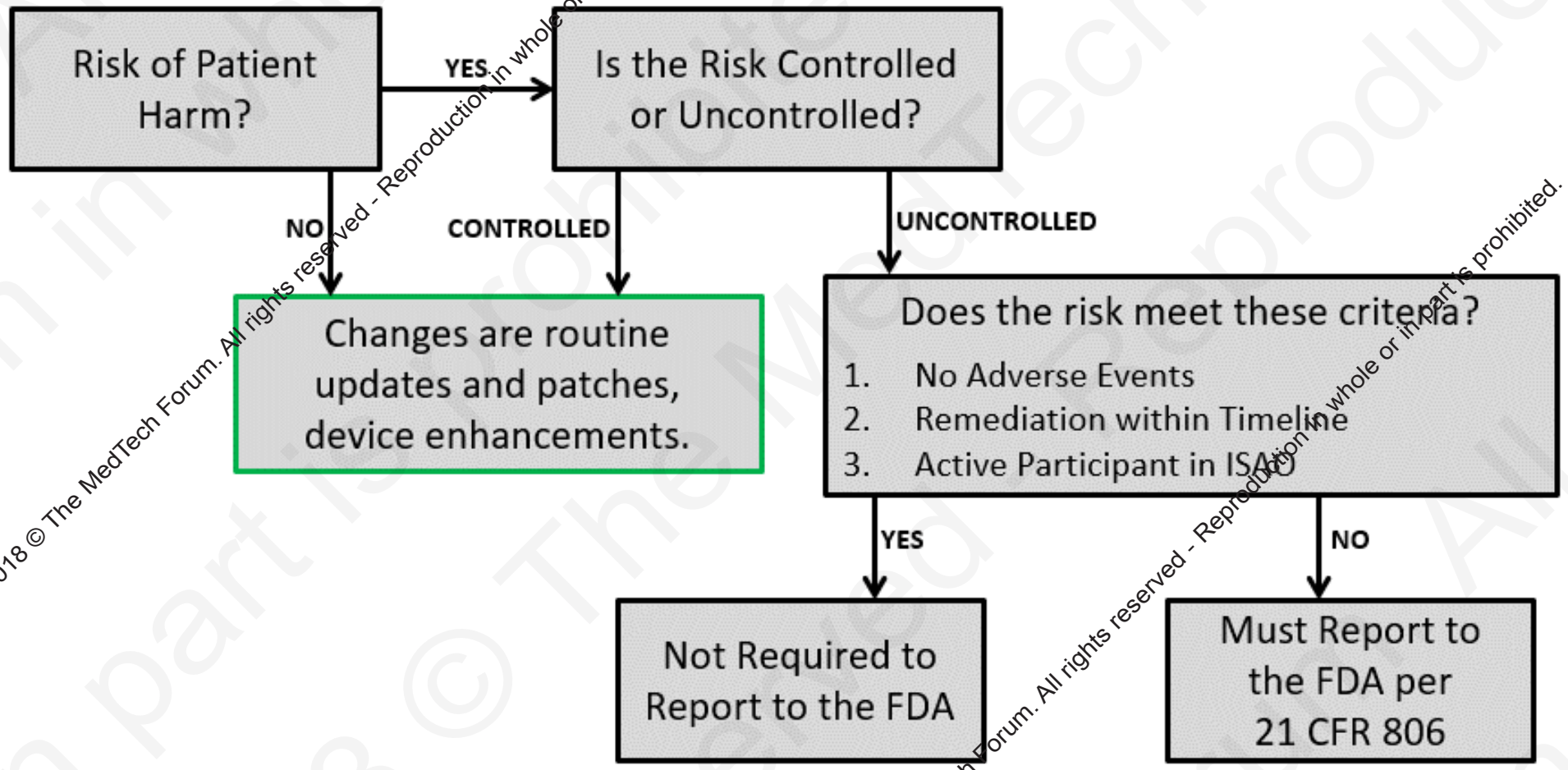
i) Postmarket Management of Cybersecurity in Medical Devices Guidance for Industry and Food and Drug Administration Staff Document issued on December 28, 2016.

j) Deciding When to Submit a 510(k) for a Change to an Existing Device, Guidance for Industry and Food and Drug Administration Staff Document issued on October 25, 2017

k) Deciding When to Submit a 510(k) for a Software Change to an Existing Device, Guidance for Industry and Food and Drug Administration Staff Document issued on October 25, 2017

2018 © The MedTech Forum. All rights reserved. Reproduction in whole or in part is prohibited.
2018 © The MedTech Forum. All rights reserved. Reproduction in whole or in part is prohibited.

US Food & Drug Administration – Cyber Division



THE FUTURE OF CYBER WARFARE IN HEALTHCARE

- Global environment is very asymmetric & challenging…
- Medical devices considered part of IoT…why is this important?
- IoT considered part of Critical Infrastructure Protection…by EU & many nations
- Vulnerable medical devices = IoT…Leading to national security threats …

2018 © The MedTech Forum. All rights reserved - Reproduction in whole or in part is prohibited.
2018 © The MedTech Forum. All rights reserved - Reproduction in whole or in part is prohibited.

Healthcare Delivery Cyber Security Leadership Actions

Wireless infusion pump ecosystems, if not secured properly, can possibly contribute to the following HDO cyber risks;

- access by malicious actors
- loss or corruption of enterprise information and patient data and health record
- a breach of protected health information
- loss or disruption of healthcare services via ransomware
  - (e.g.; WannaCry & Petya) or other known common vulnerabilities & exploits (CVE)
- damage to an organization's reputation, productivity, and bottom-line revenue

Sky is not falling….or has it already fallen….?

Medical Device Threat Vectors

Data	Device	Network
No Data Backup	Insecure Configurations	Insecure Network Configurations
No Data Integrity	Hardcoded Passwords	Insufficient Firewall Rules
No Data Validation	No Tamper Detection	Unencrypted Network Communication
Weak Authentication	Insufficient Patching	Lack of Segmentation
Weak Authorization	Legacy Operating Systems	Lack of Segregation
	No Anti-Virus Protection	
	Weak/Insufficient Access Control	
	Indefensible BIOS	
	Minimal to Zero Logging	

HEALTHCARE ALREADY INVOLVED IN FUTURE CYBER WARFARE

- Strategic & Tactical Challenges…

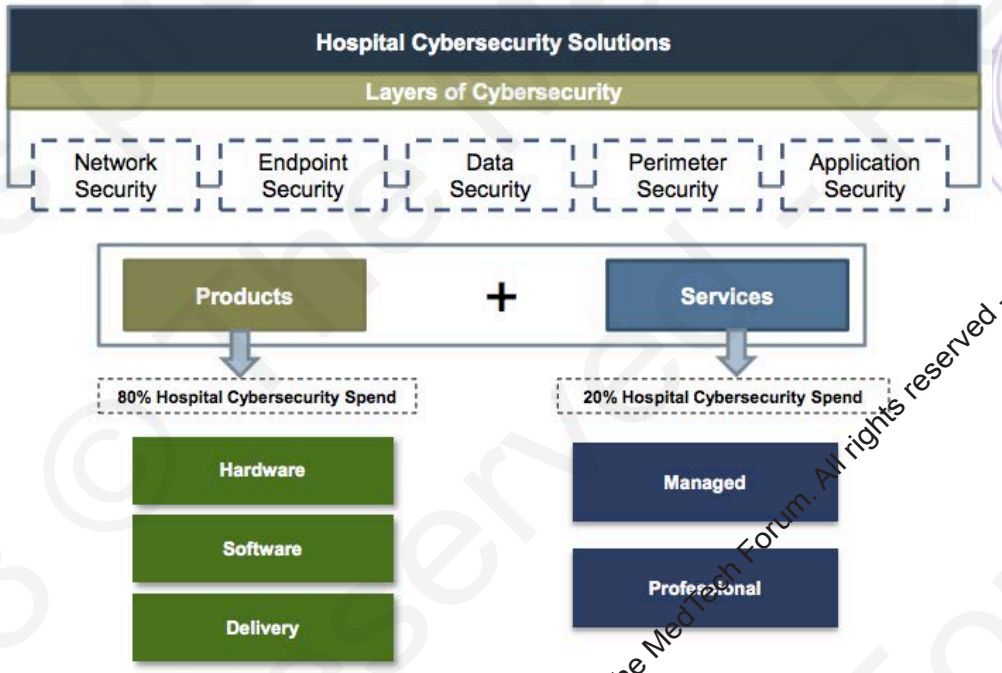
  - Medical Devices are considered vulnerable IoT devices
  - Delayed threat intel sharing -
  - Medical Device Manufacturers slow to implement cyber security engineering – 2 years NEW in most cases
  - HealthCare data breaches costly cybercrime – Current annual sunk cost $ 7.3BN Euros
  - HealthCare records very valuable to cyber criminals, more so than personal financial data
  - Ransomware clear and present danger –
    - WannaCry, NotPetya
  - Nation States – Democratic People's Republic of Korea motivated to infect IoT via ransomware

HEALTHCARE CYBER WARFARE vs MEDICAL DEVICE MANUFACTURERS

PATIENT CARE AND PATIENT SAFETY MUST BE A SHARED PRIORITY OF EFFORT!

- Different expectations force cyber security change…

Your Devices are perfect for Clinical use… Cyber use…. Well, we need to deliver care not cybersecurityY our devices could be used for intentional harm…



Our Devices are good enough… Clinical use not cyber use…. No one would use our devices for intentional harm…

http://www.frost.com/c/10024/home.do

Cybersecurity Engineering Tasks	Importance//Relevance
FDA Guidance - Postmarket Management of Cybersecurity in Medical Devices	Begin building continuity of cybersecurity engineering around Smiths-Medical infusion pumps in accordance with FDA Draft Guidance – NOT OPTIONAL
NIST Special Publication 800-30 Risk Management Guide for Information Technology Systems Revision 1 2012	Medical Infusion Pump Risk & Vulnerability Assessments - Comprehensive self assessment of our entire medical infusion pump architecture determining known cyber security vulnerabilities of medical infusion pump architecture … Through tactical cybersecurity actions identify & understand risks
NIST SP 800-53 Rev. 5 (DRAFT) Security and Privacy Controls for Information Systems and Organizations	Map NIST Security Controls to Device Design Controls, mitigate known vulnerabilities in order to proactively mitigate ALL cyber risk to patients
Apply NIST's Cybersecurity Framework (CSF) Version 1.1 (DRAFT) & NIST Cybersecurity Framework (CSF) Reference Tool	Utilise crosswalk functionality of NIST CSF Ref Tool mapping to cybersecurity engineering standards
Member of National Health – Information Sharing and Analysis Center (NH-ISAC)	Achieve collaborative situational awareness of cyber security threats directly impacting US healthcare community – actionable cyber intelligence participation
FDA recommended Vulnerability & Coordinated//Responsible Disclosure Policies	Create proactive public identification and handling capability to identify cyber risks & vulnerabilities to Smiths-Medical infusion pumps
Participate in NIST National Cyber Center of Excellence (NCCoE) medical infusion pump evaluation program – NIST SPECIAL PUBLICATION 1800-8 Securing Wireless Infusion Pumps In Healthcare Delivery Organizations	Drive & participate in cyber security standards in wireless environments for medical infusion pumps

http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf
https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/draft
https://www.nist.gov/cyberframework/csf-reference-tool
https://nccoe.nist.gov/sites/default/files/library/sp1800/hit-infusion-pump-nist-sp1800-8-draft.pdf

2018 © The MedTech Forum. All rights reserved - Reproduction in whole or in part is prohibited.

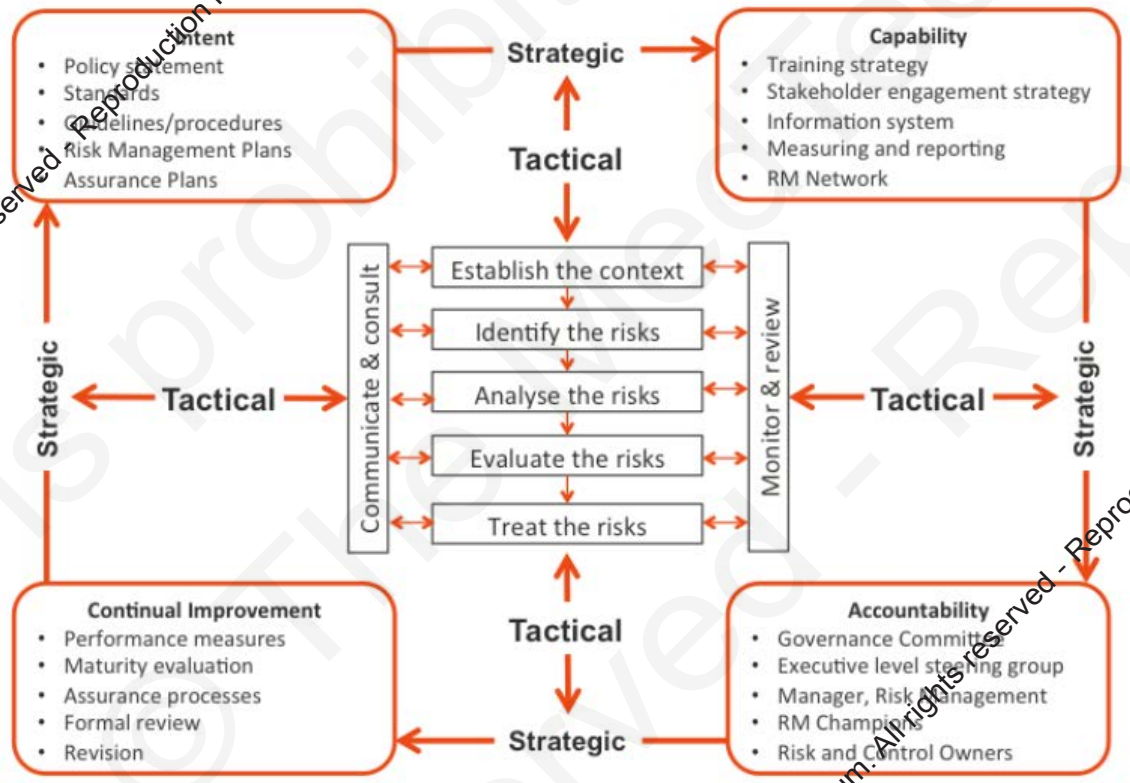
Review of Smith's Medical risk assessments using NIST SP 800-57

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

2018 © The MedTech Forum. All rights reserved - Reproduction in whole or in part is prohibited.

Review of Smith's Medical risk assessments through NIST SP 800-30…

Strategic & tactical components of our risk management framework



http://broadleaf.com.au/wp-content/uploads/2014/05/2014-05-23-Managing-disruption-related-risk-600x414.png

How we conduct risk & vulnerability assessments of medical infusion pumps

a. Identify known Common Vulnerabilities and Exposures (CVE)

b. Categorize CVEs by technology component

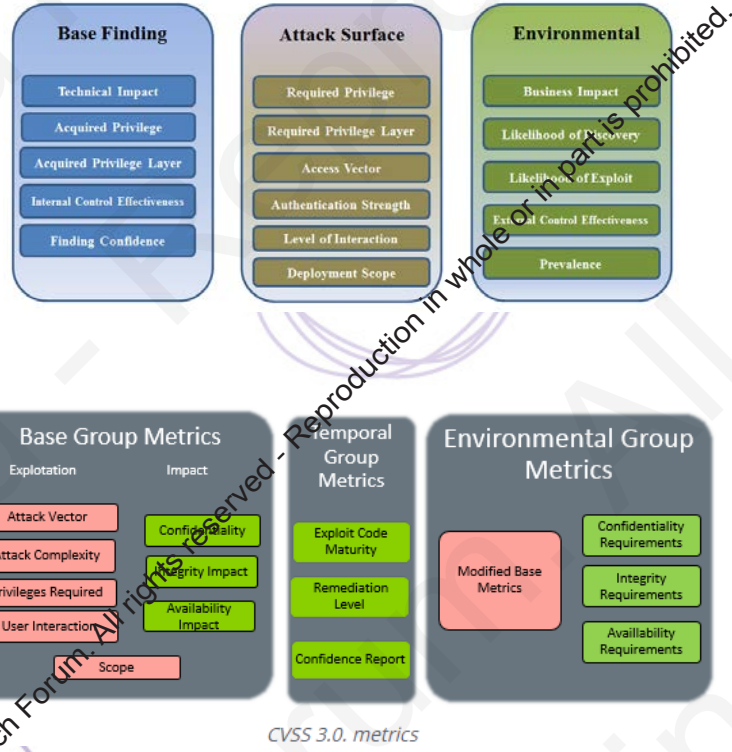
c. Identify primary & secondary compensating controls

d. Assign risk evaluation parameters…traditionally the 5 x 5 matrix
   i. Severity (s)
   ii. Probability (p)
   iii. Detection (d)

e. Calculate Risk Probability Number (RPN) for;
   i. Primary compensating controls – existing designed security
   ii. Secondary compensating controls – future design security

f. Calculate Common Vulnerability Score based upon CVSS version 3.0 (2015)

https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator
https://www.certsi.es/en/blog/cvss-3-en



CVSS 3.0. metrics

NIST SP 800-30 Rev 1.0 2012

Adversary Capability Assessment Reference Tables

(a) CYBER ADVERSARY CAPABILITIES & CHARACTERISTICS
(b) CYBER ADVERSARY INTENT CHARACTERISTICS
(c) CYBER ADVERSARY TARGETING CHARACTERISTICS
(d) RANGE OF EFFECTS FOR NON-ADVERSARIAL THREAT SOURCES

Adversary Threat Events Reference Tables

a) Threat Events (Characterized by Tactics, Techniques/Technology & Procedures/Protocols - TTPs)
b) Description of Adversarial Threat Event

Introduction

Cyber Adversary Situational Awareness: Nefarious cyber adversaries who are likely to target Smiths-Medical products and services consist of various groups. The Adsversary Taxonomy below details the various threat actor groups, motives, most probable & possible targetrs of opportunity, their cyber attack methodologies and associated compromise capabilities.

Nation State Cyber Capabilities & Motives:
1) Islamic Republic of Iran: Hackers are state sponsored, very nationalistic, and overall very dangerous and destructive in their targeting and capabilities.
2) People's Republic of China (PRC): Hackers are both state sponsored and criminal. Generally Chinese hackers are always very nationalistic. Their capabilities are stealthy, effective and enduring. Chinese hackers will most likely target intellectual property, operational procedures, prodcut design files. Cyber espionage is their forte and they are extremely effective. A burgeoning cyber criminal capability exists and is also a clear and present danger to multi-national enterprises.
3) Russian Federation: Hackers are primarily criminal, although the State will use these hacking capabilities for the projection of force in conjunction with internal Russian law enforcement efforts and countering external threats to the State using military cyber capabilities.

Cyber Threat Actor	Motive	Targets of Opportunity	Methodologies	Capabilities
Nation States ~ Peace Time	Economic, Military, National Secrets, Political	Commercial Enterprises, Intelligence, National Defense, Governments, National	Military & Intel specific cyber doctrine, hacktivists	Asymmetric use of the cyber domain short of kinetic
Nation States ~ War Time	Economic, Military, Political	Commercial Enterprises, Intelligence, National Defense, Governments, National Infrastructure	Military & Intel specific cyber doctrine, hacktivists	Asymmetric use of the cyber domain including kinetic
Cyber Terrorists & Insurgents	Political	Infrastructure, Election and Political Processes	Combination of advanced persistent threats (APT)	A developing amd emergeing threat since 2012
Cyber Criminals – Grey & Black Markets	Financial	Intellectual Property Theft, Fraud Theft, Scams, Hijacked Network & Computer Resources, Cyber Crime for Hire	Exploits, Malware Botnets, Worms & Trojans	Cell-based structure as an APT
Criminal Organizations – RBN	Financial		Use of above with distinct planning	Highly professional, dangerous
Rogue Organizations – Anonymous, LulzSec	Financial Military, National Secrets, Political Notoriety	Intellectual Property Theft, Direct & Indirect pressure on OGA Resources	Organic hacking capabilities unsurpassed	Organized yet de-centralized

US Government Reference Publication for these threat assessment tables is provided by NIST Special Publication 800-30 Guide for Conducting Risk Assessments.
Available @: http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf

Categories of Risk Control

	Risk Control Categories	
1	Identify	Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs. Examples of outcome Categories within this Function include: Asset Management; Business Environment; Governance; Risk Assessment; and Risk Management StrategyDevelop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs. Examples of outcome Categories within this Function include: Asset Management; Business Environment; Governance; Risk Assessment; and Risk Management Strategy
2	Protect	Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services. The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event. Examples of outcome Categories within this Function include: Access Control; Awareness and Training; Data Security; Information Protection Processes and Procedures; Maintenance; and Protective Technology
3	Detect	Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event. The Detect Function enables timely discovery of cybersecurity events. Examples of outcome Categories within this Function include: Anomalies and Events; Security Continuous Monitoring; and Detection Processes.
4	Respond	Develop and implement the appropriate activities to take action regarding a detected cybersecurity event. The Respond Function supports the ability to contain the impact of a potential cybersecurity event. Examples of outcome Categories within this Function include: Response Planning; Communications; Analysis; Mitigation; and Improvements.
5	Recover	Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event. The Recover Function supports timely recovery to normal operations to reduce the impact from a cybersecurity event. Examples of outcome Categories within this Function include: Recovery Planning; Improvements; and Communications.

https://blog.greenlight.guru/iso-14971-medical-device-risk-management

RISK - combination of probability of occurrence of harm & severity of harm

HAZARD - potential source of harm

HAZARDOUS SITUATION - circumstance in which people, property, or environment are exposed to one or more hazard(s)

HARM - physical injury or damage to the health of people, or damage to property or environment

SEVERITY - measure of possible consequences of a hazard

RISK ANALYSIS - systematic use of available information to identify hazards & estimate the risk

RISK ESTIMATION - process used to assign values to the probability of occurrence of harm & severity of that harm

RISK EVALUATION - process of comparing estimated risk vs. given risk criteria to determine acceptability of risk

RISK ASSESSMENT - overall process comprising a risk analysis and a risk evaluation

RISK CONTROL - process in which decisions are made and measures implemented by which risks are reduced to, or maintained within, specified levels

RESIDUAL RISK - risk remaining after risk control measures have been taken

2018 © The MedTech Forum. All rights reserved - Reproduction in whole or in part is prohibited.
2018 © The MedTech Forum. All rights reserved - Reproduction in whole or in part is prohibited.

Common Vulnerability Resources

Based upon named examples of commonly known vulnerabilities, which includes;

i. Vulnerabilities with exploits
ii. Cross Site Request Forgery
iii. Sql injection
iv. Memory corruption
v. Gain Informatic
vi. Code Execution
vii. File Inclusion
viii. Cross Site Script
ix. HTTP Response
x. DOS Attack
xi. Buffer Overflow
xii. Gain Privilege
xiii. Directory Trave
xiv. Bypass 'someth

https://www.cvedetails.com/index.php
https://www.tenable.com/sc-dashboards/cvss-temporal-risk-heat-map

2018 © The MedTech Forum. All rights reserved - Reproduction in whole or in part is prohibited.
2018 © The MedTech Forum. All rights reserved - Reproduction in whole or in part is prohibited.

Common Vulnerability Resources – US GOV

https://ics-cert.us-cert.gov/content/overview-cyber-vulnerabilities
https://www.us-cert.gov/related-resources

2018 © The MedTech Forum. All rights reserved - Reproduction in whole or in part is prohibited.

Common Vulnerability Resources

https://www.owasp.org/images/3/3c/OWASP_Top_10_-_2017_Release_Candidate1_English.pdf

OWASP Top 10 – 2013 (Previous)	OWASP Top 10 – 2017 (New)
A1 – Injection	A1 – Injection
A2 – Broken Authentication and Session Management	A2 – Broken Authentication and Session Management
A3 – Cross-Site Scripting (XSS)	A3 – Cross-Site Scripting (XSS)
A4 – Insecure Direct Object References - Merged with A7	A4 – Broken Access Control (Original category in 2003/2004)
A5 – Security Misconfiguration	A5 – Security Misconfiguration
A6 – Sensitive Data Exposure	A6 – Sensitive Data Exposure
A7 – Missing Function Level Access Control - Merged with A4	A7 – Insufficient Attack Protection (NEW)
A8 – Cross-Site Request Forgery (CSRF)	A8 – Cross-Site Request Forgery (CSRF)
A9 – Using Components with Known Vulnerabilities	A9 – Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards - Dropped	A10 – Underprotected APIs (NEW)

2018 © The MedTech Forum. All rights reserved - Reproduction in whole or in part is prohibited.

ENDGAME….

- Preventing Harm Patients – Most Important!
- Deterring, Preventing more Ransomware incidents such WannaCry or Petya/NotPetya
- Designing cyber security into medical devices, not as an afterthought…

Desired Future State…

- Teach, mentor & Encourage smaller manufacturers;
- More active participation by all of Smiths Medical;
- Desire for an FDA Cyber assist visit…

http://www.hitachi.com/hirt/publications/hirt-pub17008/index.html

2018 © The MedTech Forum. All rights reserved - Reproduction in whole or in part is prohibited.

smiths medical

bringing technology to life

Questions / Feedback?

Thank you!

Bill Hagestad,

Senior Principal Cyber Security Engineering

2018 © The MedTech Forum. All rights reserved - Reproduction in whole or in part is prohibited.