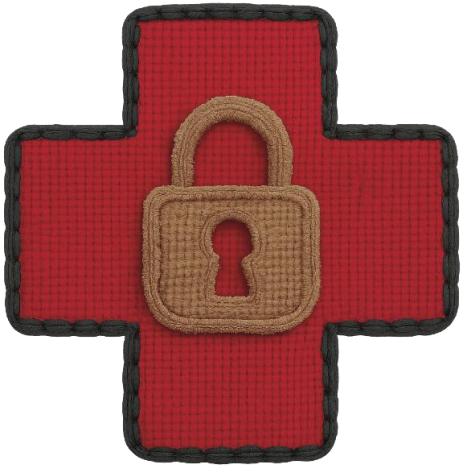
Northeastern University



Medical Device Cybersecurity – Week 2

01/13/2025 - Introduction and Course Overview

Axel Wirth | Chief Security Strategist | Medcrypt
axel@medcrypt.com

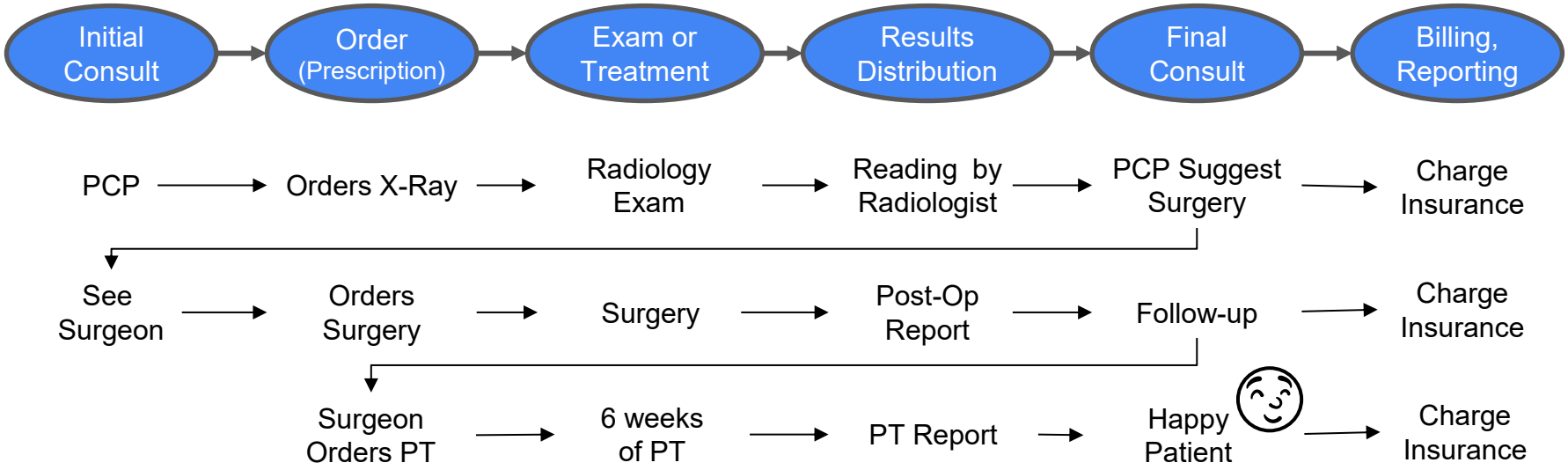
Today's Introductory Lecture

- Short Overview of the Medical Technology World
- Medical Device Cybersecurity – Framing the Topic
- Summary and Course Overview

Note – I may pull images off the WWW to give examples and support my explanation.
None of this should be considered endorsement of a specific product or vendor.

PATCH

Healthcare - How it Works (in most general terms, details ~~may~~ will vary)



- Complex interaction of clinical and administrative processes and data flows.
- Similar e.g., when ordering prescription, lab tests, etc.
- Interrupts may occur at any time and lead to tangents.
- Not all clinical processes are predictable and linear , e.g., Emergency Room visit

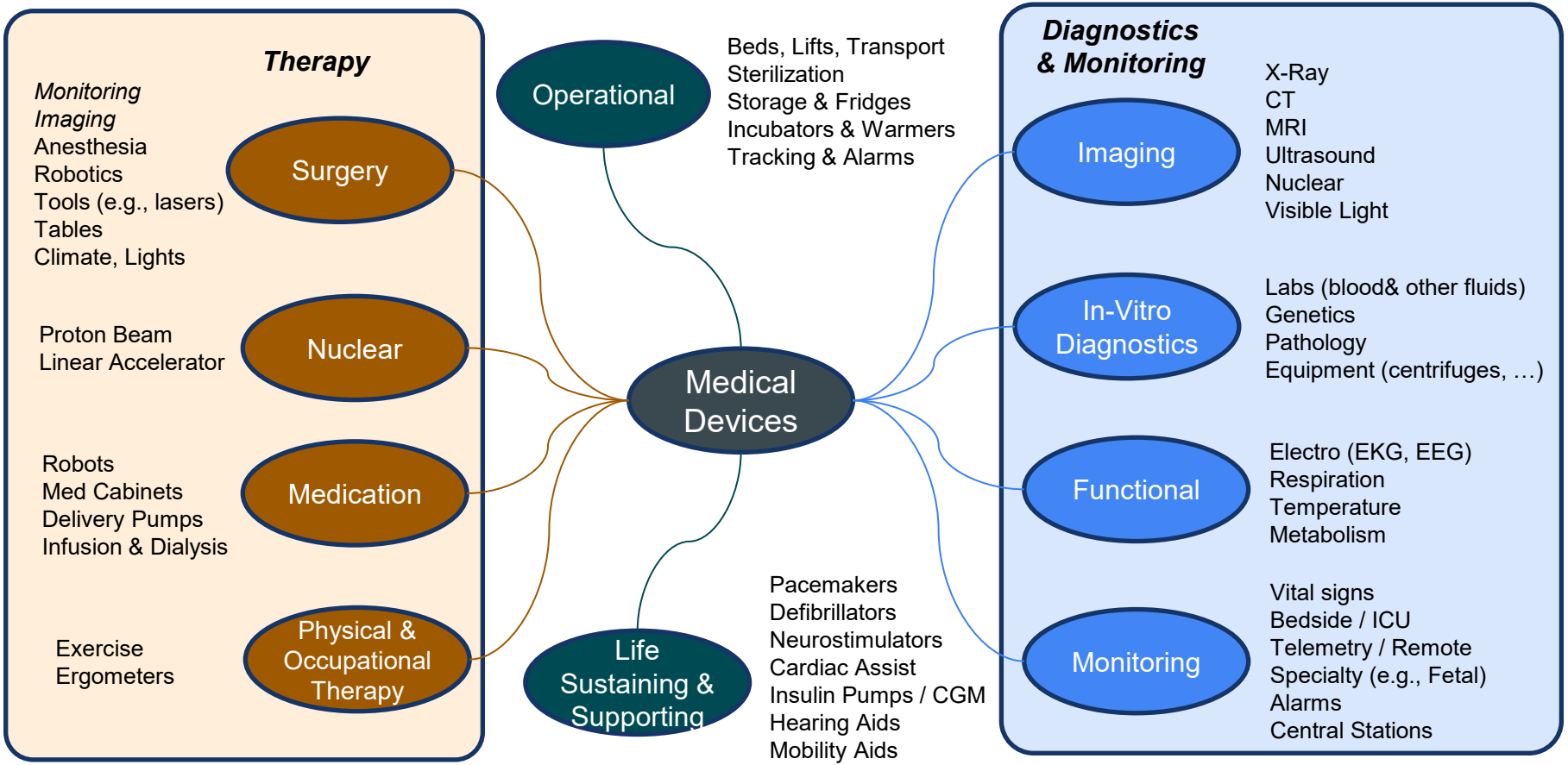
Healthcare Cybersecurity Challenges

We will discuss in more detail, but in summary:

- High degree of technical and organizational complexity
- Multi-vendor environment
- Prevalence of legacy equipment
- Split security responsibilities
- Clinical needs often beat security needs
- Perceived as an attractive target

The Big Wide World of Medical Devices

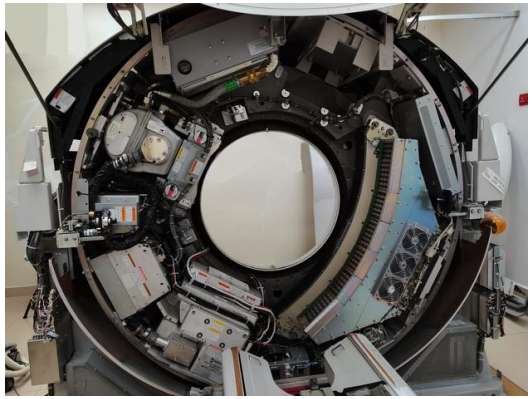
... and still incomplete. Most (but not all) are “regulated” medical devices



The Big Wide World of Medical Devices

- Previous slide is organized by shared characteristics and properties. In practice, we think and organize systems by clinical department …. Radiology, Cardiology, Emergency, …
- Imaging techniques are typically referred to as “Modality” … x-ray, ultrasound, CT, …
- Some departments don’t “own” patients, they perform services for other departments. These are typically referred to as “Ancellaries” … Radiology, Pathology, Pharmacy, Lab, …..
- All of the above have corresponding IT system integration to support clinical workflows and information sharing.

X-Ray – projection images
via electromagnetic radiation

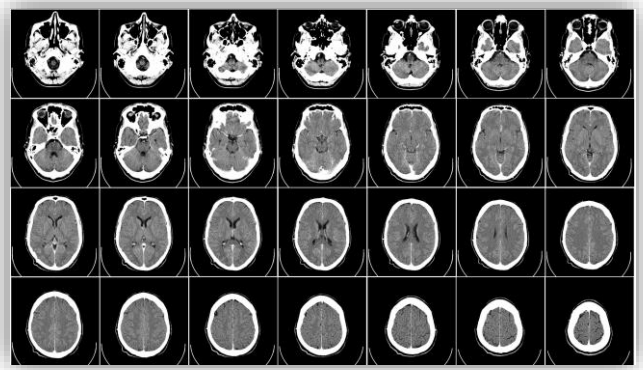


Computed Tomography (CT) – cross-sectional
reconstruction of rotating x-ray beam

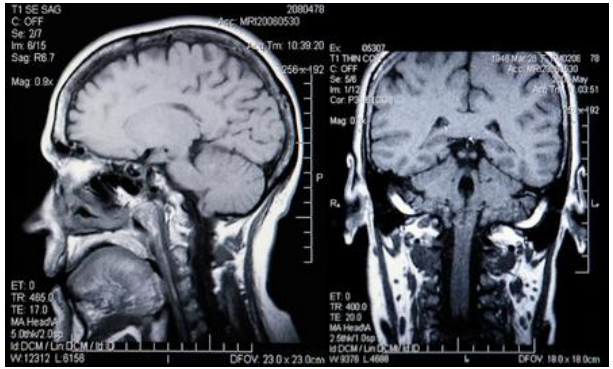
Magnetic Resonance Imaging (MRI) –
reconstruction of soft-tissue radio-pulse echoes

Ultrasound – reconstruction of
sound pulse echoes

X-Ray – projection images
via electromagnetic radiation



Computed Tomography (CT) – cross-sectional
reconstruction of rotating x-ray beam

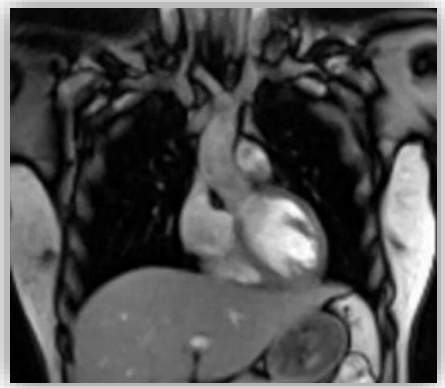


Magnetic Resonance Imaging (MRI) –
reconstruction of soft-tissue radio-pulse echoes

Ultrasound – reconstruction of
sound pulse echoes

Modern Medical imaging

- Essentially, we are using (m)any known physical process to generate medical images (electromagnetic radiation, nuclear radiation, sound waves, quantum resonance, …).
- Imaging may be provided by specialized departments (Radiology) or be integrated into clinical processes. E.g., ultrasound in Obstetrics, Surgery (and other invasive procedures), Cardiology, Urology, Internal Medicine, …).
- Imaging may be combined with e.g., biopsies, contrast media, EKG, …
- Modern Imaging uses a lot of advanced reconstruction techniques (e.g., objects in motion, combination imaging, 3D reconstruction, advanced image processing, …).



https://en.wikipedia.org/wiki/File:Real-time_MRI_-_Thorax.ogv

https://www.dailymail.co.uk/lifestyle/article-3070976/Blind-mother-gets-chance-unborn-son-time-doctors-surprise-3D-printout-ultrasound.html

Medical Device Connectivity

Medical Devices are connected and integrated for a variety of purposes:

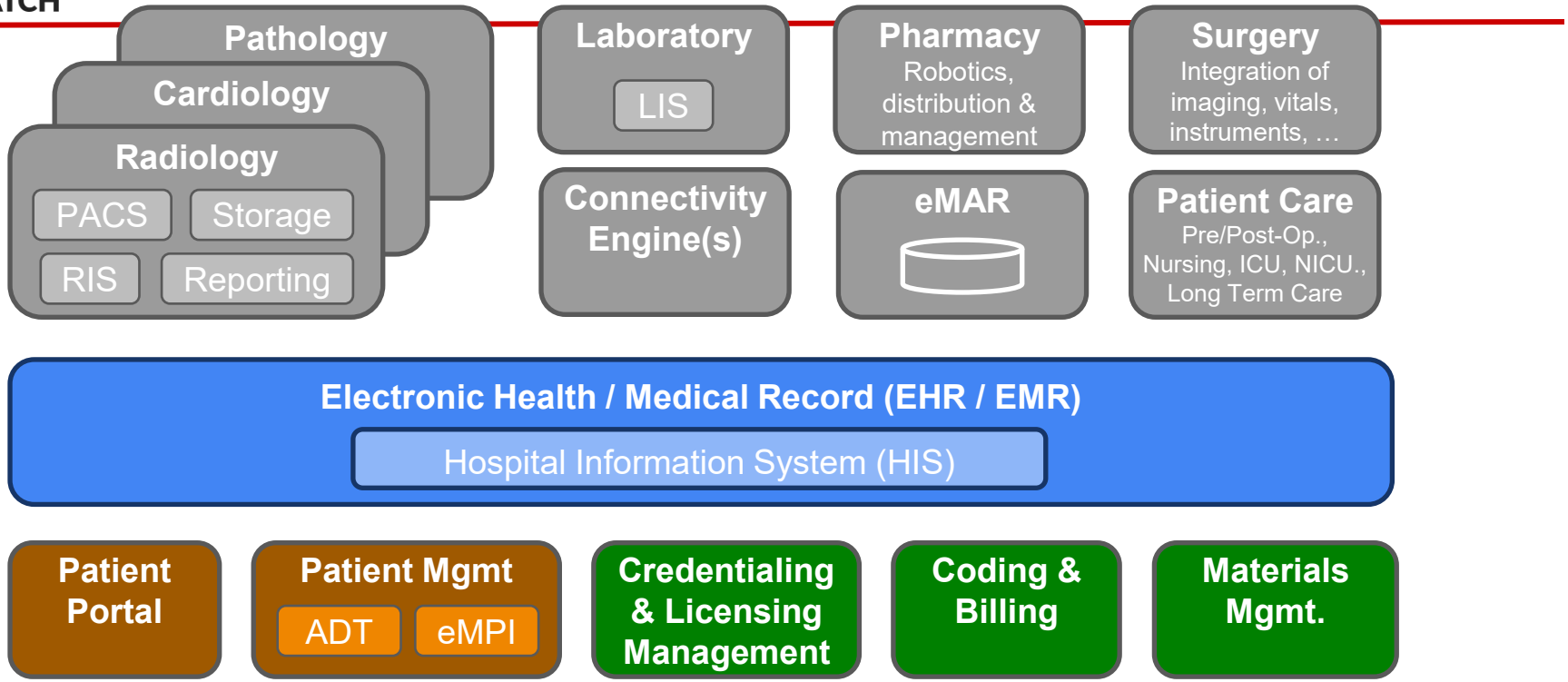
- Exchange of clinical information (lab results, images, diagnostic reports, …)
- Monitoring and alarms
- Logistics (orders, procedure status, discharge, prescriptions, …)
- Billing and coding
- Remote support and maintenance

Associated communication protocols vary based on purpose … and age:

- DICOM for images (and waveforms) and interpretive results
- HL7 for labs, orders, reports, medication management – newer version HL7 FHIR
- ASTM for lab equipment
- Proprietary, e.g., magnetic short range
- Typically exchanging via Ethernet, Wi-Fi, Bluetooth, …. RS232

Adoption of secure versions of the respective standards varies widely.

Common Health IT Systems (regardless of implementation (hosted, on site))



Common Health IT Systems - Summary

- Historically, clinical IT solutions develop din “clinical islands” with limited interconnectivity for patient management, billing, and results exchange
- Health IT systems are typically organized by clinical functions combined with some overarching components.
- Although some functional areas seem similar, differences in clinical needs drive differences in technical implementation: e.g., Radiology.
- From a cybersecurity perspective, health IT systems are more similar to traditional IT environments but complexities and multi-vendorism create unique challenges.

- None of this was “designed”, it followed an evolutionary path aligned with clinical needs.
- Outside hospital … nursing, primary care, clinics and service centers, retail & pharmacy, …
- Details and specific may vary
- ADT = Admission, Discharge, Transfer (HL7); EMPI = Enterprise Master Patient Index;
  eMAR = electronic Medication Administration Record; PACS = Picture Archiving and Communications System;
  H/R/C/LIS = Hospital / Radiology / Cardiology / Laboratory (etc.) Information System

Today's Introductory Lecture

- Short Overview of the Technology Medical World
- Medical Device Cybersecurity – Framing the Topic
- Summary and Course Overview

Note – I may pull images off the WWW to give examples and support my explanation.
None of this should be considered endorsement of a specific product or vendor.

Reality is More Complex and Subtle than Headlines

The Register

Hackers can steal your BRAIN WAVES

Depressingly familiar and stupid mistakes in EEG kit, health org's storage of recorded brains

Darren Pauli — Tue 13 Oct 2015 // 04:58 UTC

BruCon: Behold the future: attackers can already get between brain-waves and hospital kit, and it's just going to get worse according to IOActive senior consultant Alejandro Hernández.

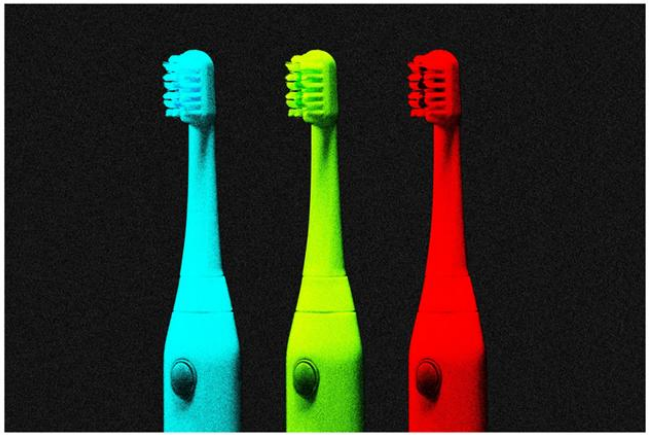
Hernández says the ability to steal, manipulate, and replay brain waves used in electroencephalography (EEG) is already emerging, with consumer-grade kit already able to be hacked and the health care industry taking few precautions to properly protect recorded brain waves.

WIRED

BACKCHANNEL BUSINESS CULTURE GEAR IDEAS POLITICS SCIENCE SECURITY MERCH

ANDY GREENBERG DHRUV MEHROTRA SECURITY FEB 10, 2024 9:00 AM

Security News This Week: How 3 Million 'Hacked' Toothbrushes Became a Cyber Urban Legend



https://www.theregister.com/2015/10/13/brain_waves_security/

https://www.wired.com/story/3-million-hacked-toothbrushes-urban-legend/

Cyber Threats: From Fines to Fiasco

Innovate Healthcare

RADIOLOGY BUSINESS

FOR IMAGING LEADERS IMPROVING ECONOMICS, OPERATIONS & OUTCOMES

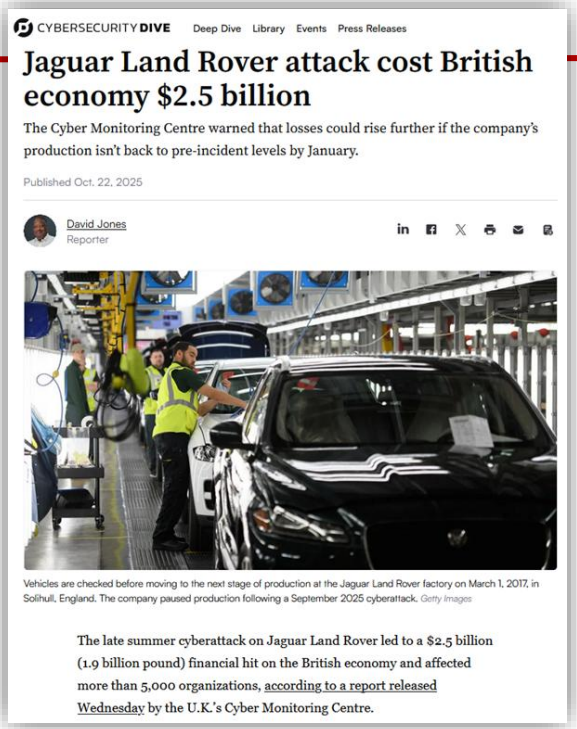
Private radiology practice will pay $3.25M to settle class-action lawsuit over cyberattack

Marty Stempniak | October 09, 2025 | Radiology Business | Legal News

A North Carolina private radiology practice will pay $3.25 million to settle a class-action lawsuit stemming from a recent cyberattack.

Greenville-based Eastern Radiologists first reported news of the data breach in March 2024 after an investigation found hackers had accessed its network. The incident impacted records for upward of 886,000 individuals, with exposed details including Social Security numbers, insurance information and imaging results.

https://radiologybusiness.com/topics/healthcare-management/legal-news/private-radiology-practice-will-pay-325m-settle-class-action-lawsuit-over-cyberattack



CYBERSECURITY DIVE Deep Dive Library Events Press Releases

Jaguar Land Rover attack cost British economy $2.5 billion

The Cyber Monitoring Centre warned that losses could rise further if the company's production isn't back to pre-incident levels by January.

Published Oct. 22, 2025

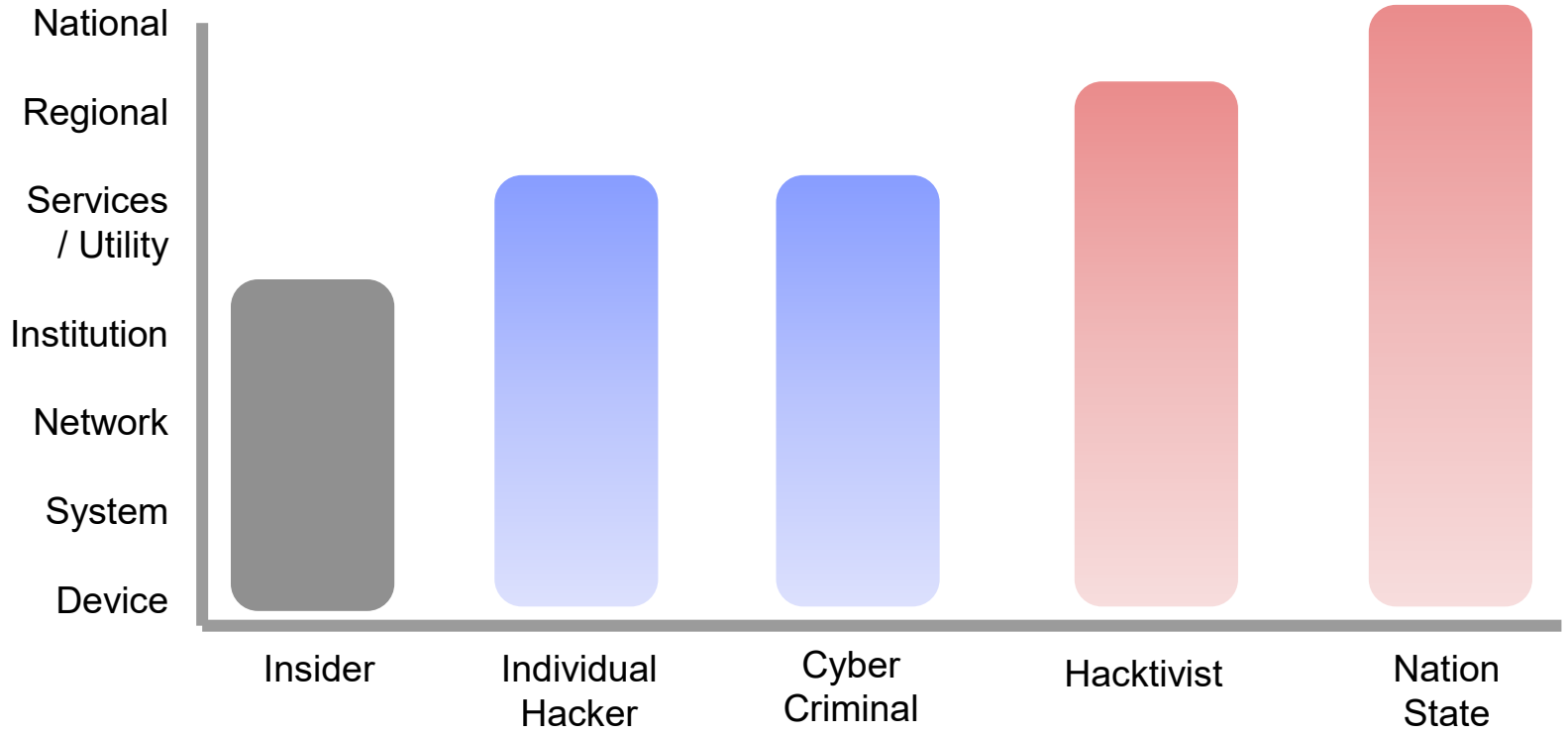
David Jones
Reporter

Vehicles are checked before moving to the next stage of production at the Jaguar Land Rover factory on March 1, 2017, in Solihull, England. The company paused production following a September 2025 cyberattack. Getty Images

The late summer cyberattack on Jaguar Land Rover led to a $2.5 billion (1.9 billion pound) financial hit on the British economy and affected more than 5,000 organizations, according to a report released Wednesday by the U.K.'s Cyber Monitoring Centre.

https://www.cybersecuritydive.com/news/jaguar-land-rover-attack-british-economy-25-billion/803491/

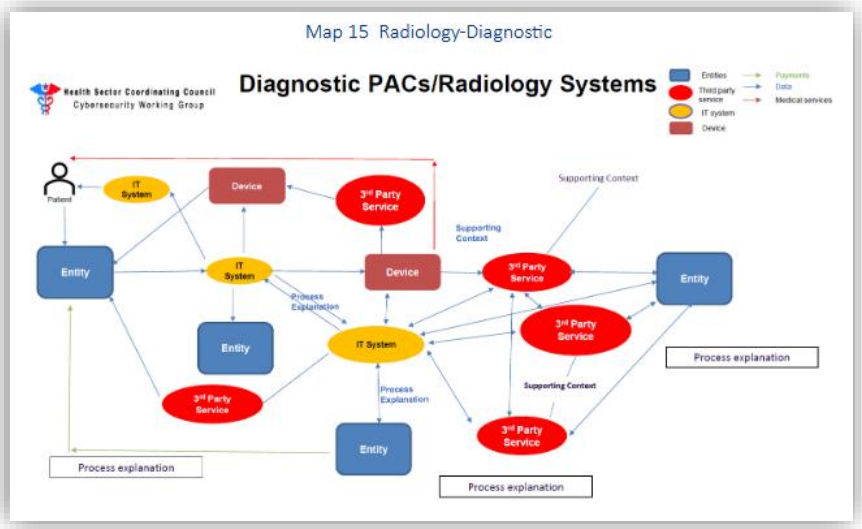
Threat Landscape – Origin and Impact Scope (Conceptually)



It’s Not a Device Problem, it is a System Problem

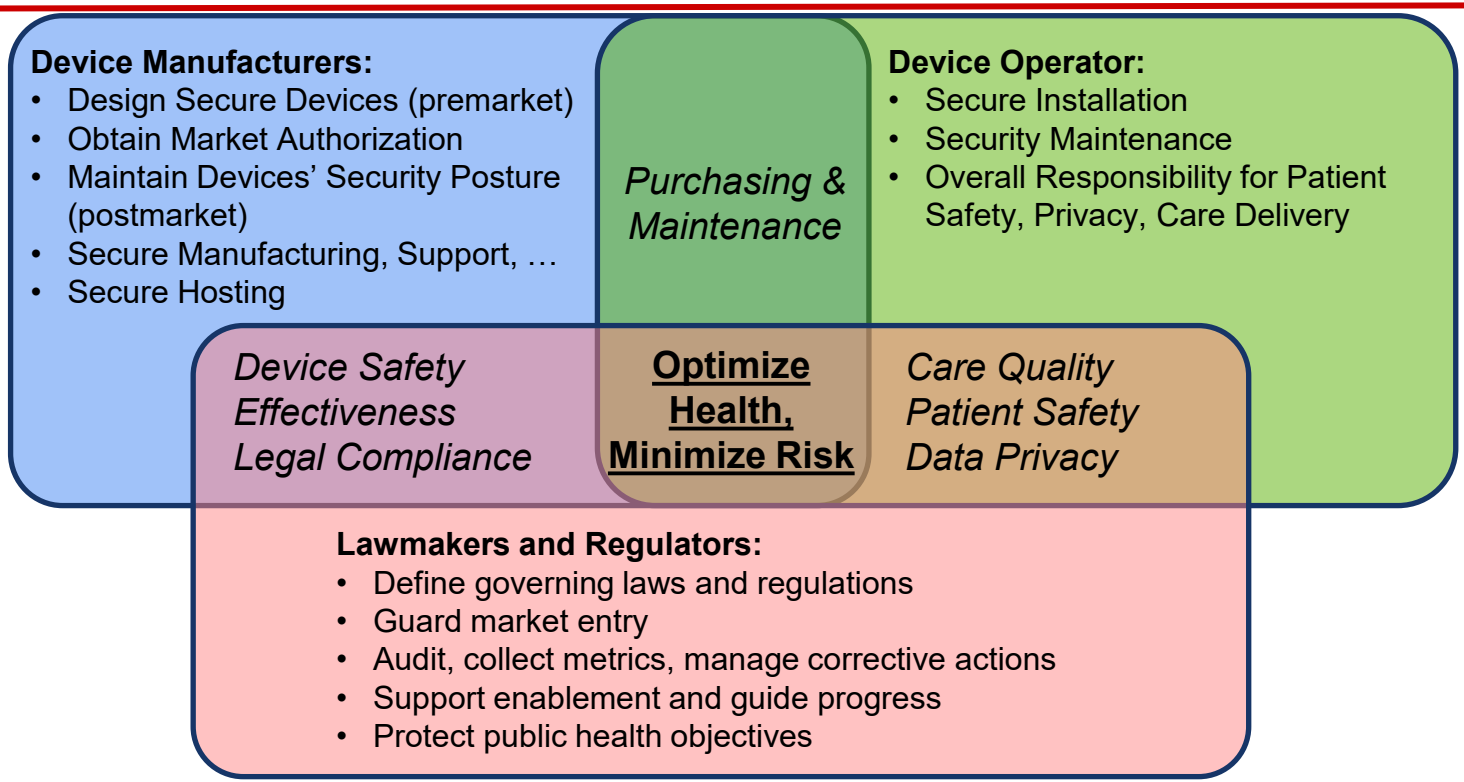
Health Sector Coordinating Council (HSCC) - “Health Industry Cybersecurity Sector Mapping and Risk Toolkit” (SMART):

- Device → System → Institution → Public Health
- Initiated following the ChangeHealth breach.
- Identify critical functions across the healthcare sector.
- Methodology to identify, visualize, and manage systemic cyber risks related to third-party services.
- Methodology and templates
  - inventorying processes
  - documenting workflows
  - identifying vendors
  - assessing risks
  - developing mitigations
- Provides generalized mapping of 17 critical workflows.



https://healthsectorcouncil.org/wp-content/uploads/2025/10/HIC-SMART-1.pdf

Understanding Stakeholder Perspectives and Relationships

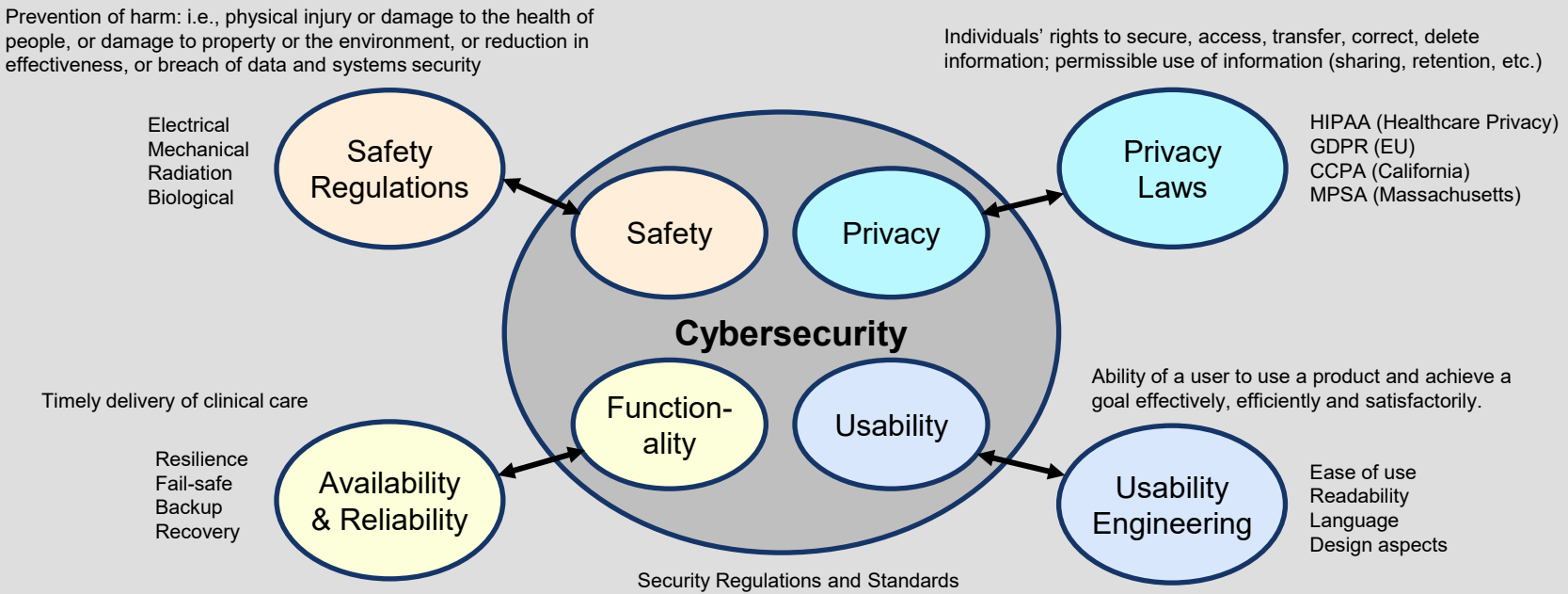


Few Additional Notes

- Roles are increasingly blurring – e.g., hospital may contract device maintenance back to the manufacturer (or other 3rd party).
- Can't reduce responsibilities to a single party, in the end it requires all stakeholders to work together.
- Security does not stand on its own, it is always in the context of and in combination with other requirements.
- Conflicts and constraints are real – do the best under the current circumstances while continuing to improve.
- The law of unintended consequences - security is important and needs to improve while avoiding harm.
- Understand – it's a spectrum of capabilities (human and technical).

Complex Relationship of Risks

Cybersecurity by itself has no purpose



Business Risk Tolerance: Downtime, Revenue; Laws & Regs; Reputation; Risk Tolerance; Nature of Business; etc.

Complex Relationship of Risks

Cybersecurity by itself has no purpose

- Is Cybersecurity a Science, Craft, or an Art? …. Answer: it depends
- Most generally, Cybersecurity Requirements are Secondary and derived from a set of Primary Objectives: Laws, Regulations, Standards, and Practices:
  - Privacy
  - Safety
  - Reliability
  - Usability
  - Business Objectives
- Implementing these cybersecurity requirements then enables the fulfillment of above primary objectives. (this is mostly true, with exceptions)
- BUT 1: There are dependencies and tradeoffs between them, e.g., security vs safety
- BUT 2: This has also led to blind spots, e.g., gaps in laws leading to gaps in security.
- Lastly, implementation and practical execution widely depends on context:
  e.g., IT vs OT vs IoT vs Medical Devices vs Cloud.

Today's Introductory Lecture

- Short Overview of the Technology Medical World
- Medical Device Cybersecurity – Framing the Topic
- Summary and Course Overview

Note – I may pull images off the WWW to give examples and support my explanation.
None of this should be considered endorsement of a specific product or vendor.

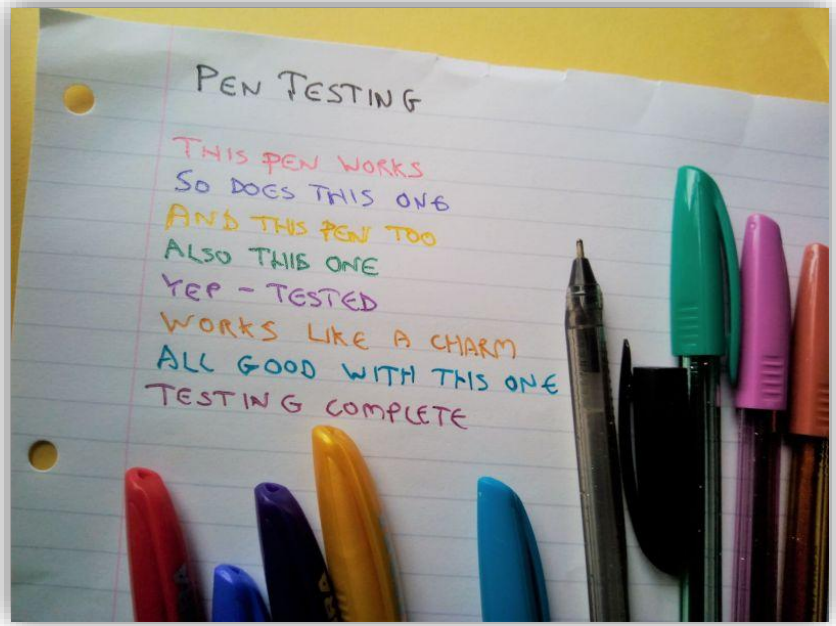
Course Overview

Weeks 1-4	Cybersecurity Fundamentals Cybersecurity in Healthcare
Weeks 5-7	Medical Device Cybersecurity Regulations & Standards
Weeks 8-13	Hospital Perspective Device Manufacturer Practices Guest Lectures on Select topics
Weeks 14-15	Other Stakeholders Cybersecurity Future Outlook Course Recap and Summary

Course Overview

Guest Lectures:

- Medical Device Pen Testing (confirmed)
- Big Picture – Beyond the Hospital (confirmed)
- ARPA-H UPGRADE Project (confirmed)
- Mock Regulatory Exercise (pending)
- Device Manufacturer Tour (pending)



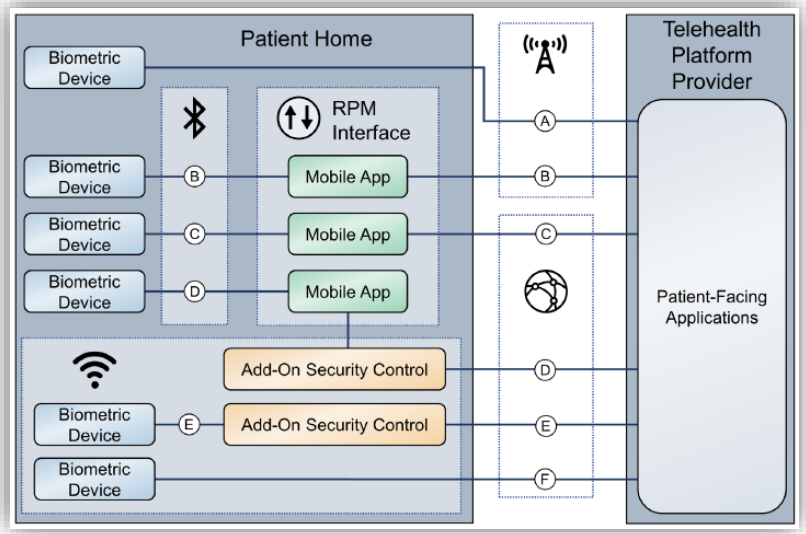
Healthcare Cybersecurity – The Good, the Bad, and the Ugly

- Clinical needs prioritized over technical needs
- IT processes:
  - Difficult to automate during continual care delivery
  - Especially for medical devices. limited tooling availability
- Long technology live cycles:
  - Delayed patch deployment
  - Prevalence of legacy devices
- Complexity of devices and complex integrations
  - Broad attack surface
  - Difficult to manage and maintain
  - Distributed / departmental ownership
- Vendor dependency / lack of internal knowledge
- Cyber-adversaries perceive healthcare organizations as an easy target
- High pressure to “keep the lights on”

These are VERY Different Security Problems

Implantable
Pacemaker

Surgical
Robot



Remote
Monitoring

Baselining the Problem

Shared security properties and challenges across IoT, OT, Medical Devices faced by an increasingly hostile and sophisticated threat landscape.

Device Security Drivers	Management Challenges	Evolving Threats	Regulatory Advancements
• Resource constrained • Historically, security not a design objective • Time-to-market driven • Lack of security features • Regulatory impediments	• Inventory visibility • Long patch cycles • Long life / legacy • Security tool incompatibility • Shared responsibility	• Sophisticated • Targeted • Opportunistic • Fast-evolving • Now: AI-powered • IT ➔ OT target shift	• Med. Devices: FDA; EU MDR, AU TGA • IoT: EU CRA & NIS2, US States (CA, OR, CT, …) • Govt. Procurement: US, KR, UK, JP, …
Manufacturers	***Operators***	***Adversaries***	***Government***

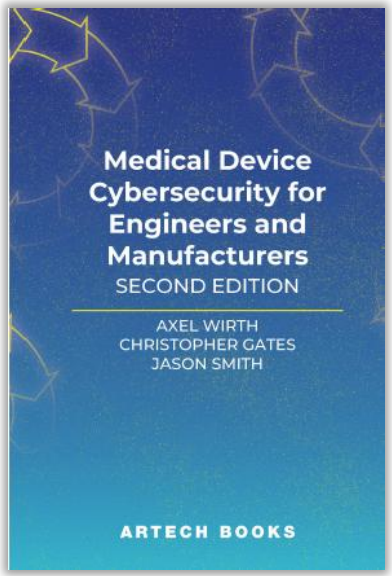
Compliance is not Security – **HIPAA Kills!**

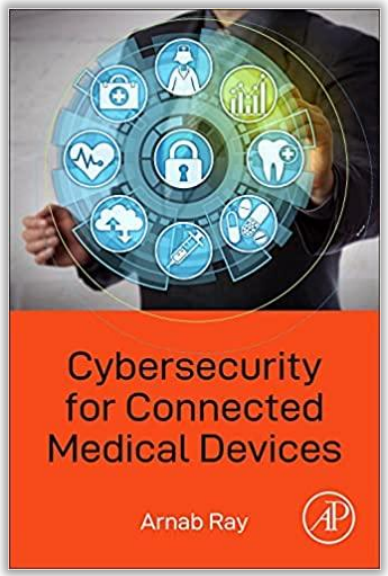
“Compliance only works if your enemy is the compliance auditor”

Thank you!

axel@medcrypt.com

General Resources - For Medical Device Manufacturers

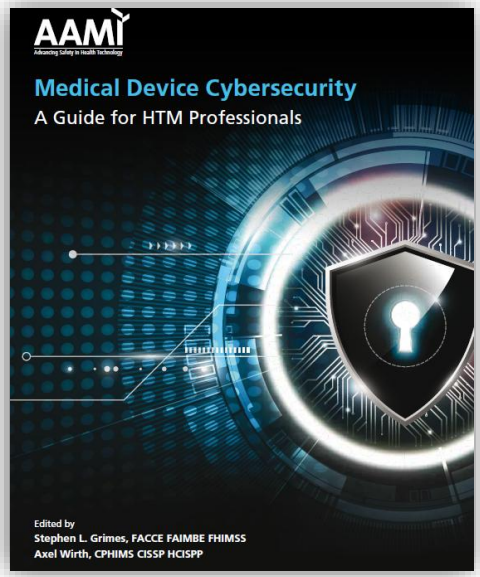




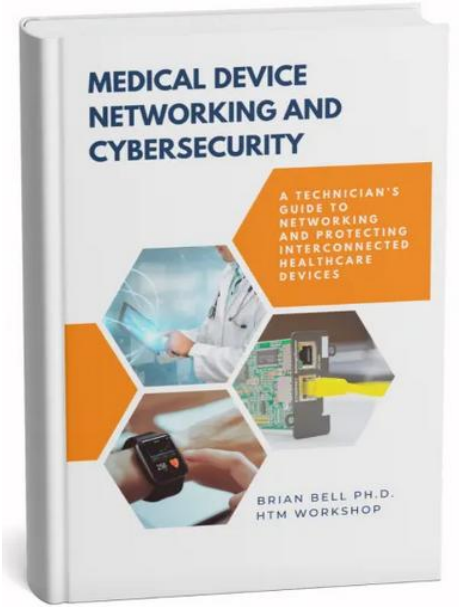
US: https://us.artechhouse.com/Medical-Device-Cybersecurity-for-Engineers-and-Manufacturers-Second-Edition-P2416.aspx
UK: https://uk.artechhouse.com/Medical-Device-Cybersecurity-for-Engineers-and-Manufacturers-Second-Edition-P2354.aspx

https://www.amazon.com/Cybersecurity-Connected-Medical-Devices-Arnab/dp/0128182628/ref=sr_1_4

General Resources - For Healthcare Delivery Organization



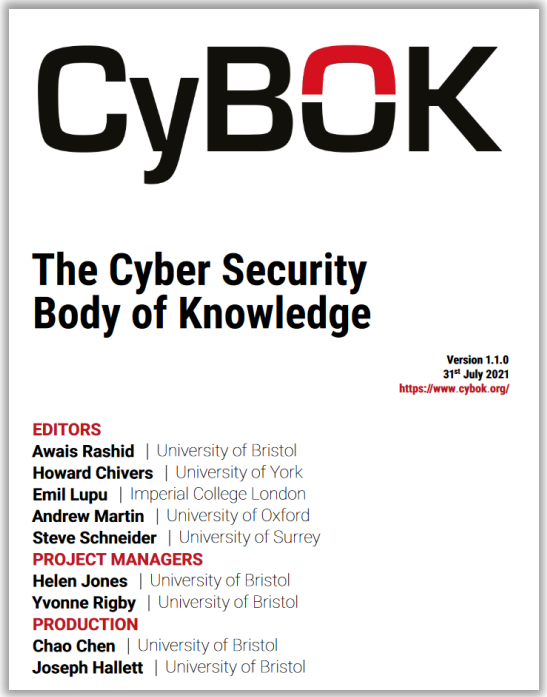
https://store.aami.org/s/store#/store/browse/detail/a152E000006j66qQAA



https://htm-workshop.com/shop/medical-device-networking-and-cybersecurity/

CY 7790 / CY 4973 - Medical Device Cybersecurity

General Resources - CyBOK


CyBOK

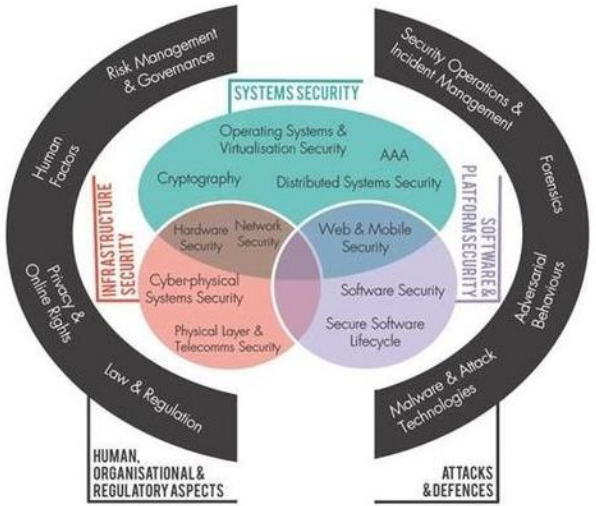
The Cyber Security Body of Knowledge

Version 1.1.0
31st July 2021
https://www.cybok.org/

EDITORS
Awais Rashid | University of Bristol
Howard Chivers | University of York
Emil Lupu | Imperial College London
Andrew Martin | University of Oxford
Steve Schneider | University of Surrey
PROJECT MANAGERS
Helen Jones | University of Bristol
Yvonne Rigby | University of Bristol
PRODUCTION
Chao Chen | University of Bristol
Joseph Hallett | University of Bristol

The Cyber Security Body of Knowledge v1.1,
https://www.cybok.org/media/downloads/CyBOK_v1.1.0.pdf

CyBOK Knowledge Base
https://www.cybok.org/knowledgebase1_1/



Staying Informed on the Day-to-Day

- Security briefs and threat alerts via Health Sector Cybersecurity Coordination Center (HC3) https://www.hhs.gov/about/agencies/asa/ocio/hc3/index.html
- US Department of Homeland Security's Industrial Control Systems—Cyber Emergency Response Team (ICS-CERT) medical device alerts (ICSMA) https://www.cisa.gov/news-events/cybersecurity-advisories?f%5B0%5D=advisory_type%3A96
- Healthcare and Public Sector Highlights - Cybersecurity (via HHS) https://www.cisa.gov/topics/cybersecurity-best-practices/healthcare
- CISA HPH Sector https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/healthcare-and-public-health-sector