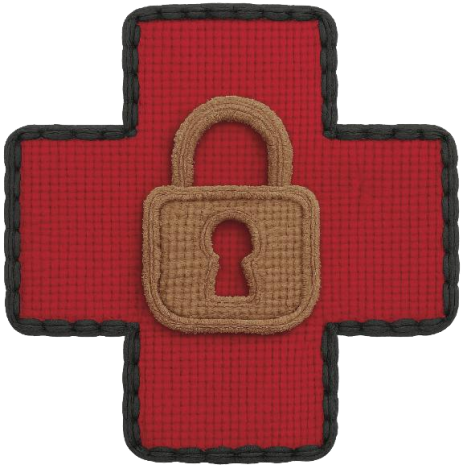
Northeastern University



Medical Device Cybersecurity – Week 5

02/03/2026 – Medical Device Introduction

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

Medical Device Cybersecurity
Introduction

- Manufacturer vs Hospital Perspective
- Medical Device Incident Examples
- Trends and Analyses

What do these two gentlemen have in common?

Dick Cheney, former U.S. VP

Jay Radcliffe, Security Researcher

Both made medical decisions based out of concern that their implanted medical device could be hacked!

Differing Perspectives and Objectives

Regulators:

- Enforce safety
- Improve cybersecurity
- Mandate privacy protections
- Ensure care continuity

Manufacturers:

- Design secure & resilient devices
- Provide security maintenance
- Enable their customers to comply
- Protect their infrastructure
- Protect their customers' data

Operators:

- Procure secure devices
- Integrate devices securely
- Maintain devices' security
- Protect sensitive data
- Secure decommissioning

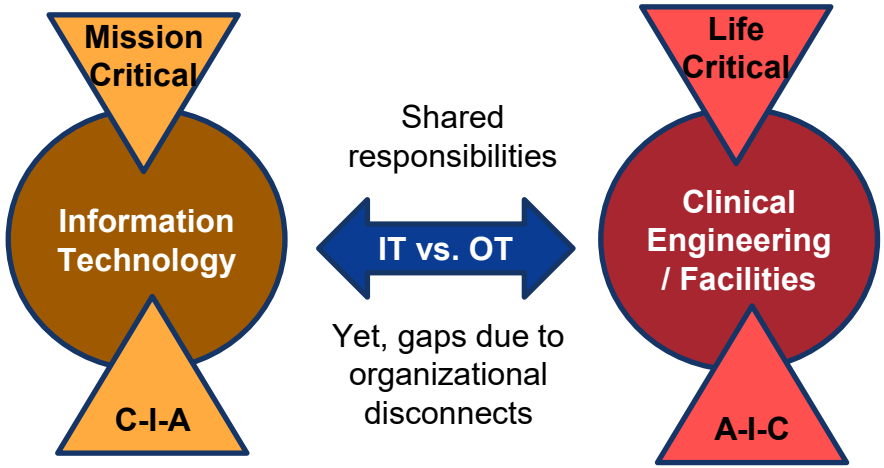
Patients:

- Avoid being harmed
- Have confidence in your devices
- Timely and reliable care
- Protect my data

Hospital Perspective

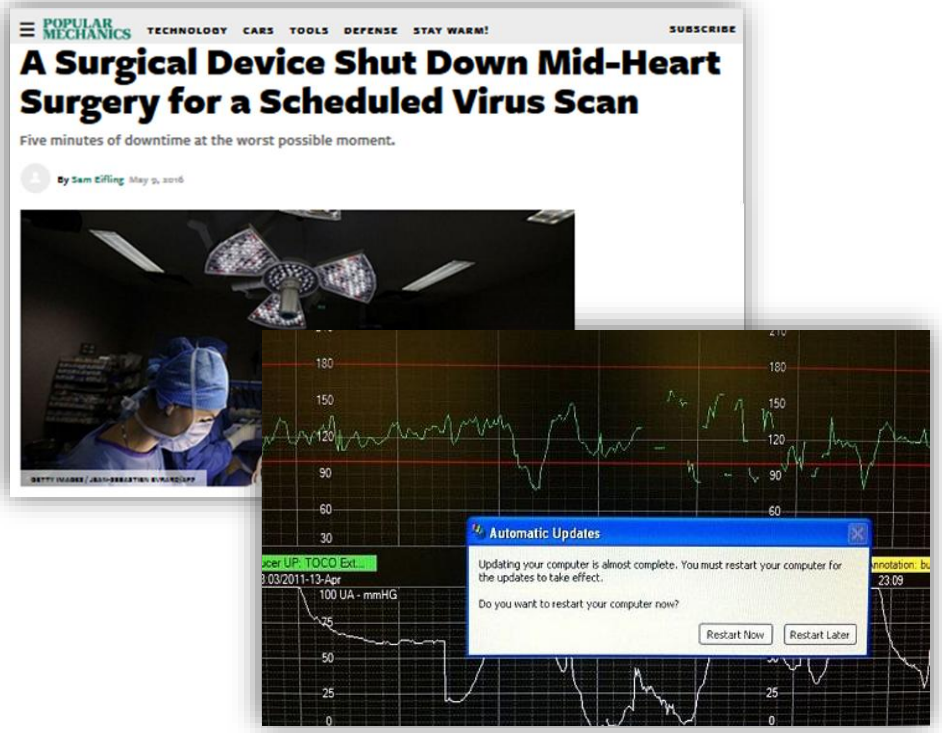
Hospital challenges: complexity, maturity, equipment age, disconnects.

Financial, legal, reputational, and operational impact (including care delay)



In addition, risk of direct harm (death or serious injury)

Medical Device Security - Examples



Poor IT Management Practices

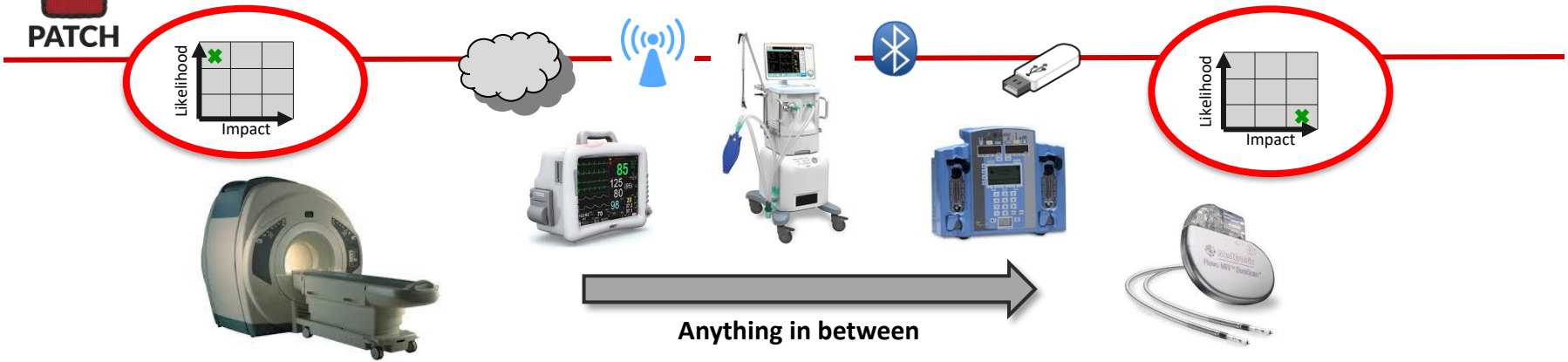
- Medical Device not recognized for its unique needs and unique dependencies
- Examples:
  - OS upgrade during procedure
    - Patient care risk
    - Device may not even have keyboard / mouse to manage system messages
  - Device (or supporting server, workstation, firewall, etc.) forced to “IT Standard”
    - Forced OS upgrade
    - Configuration change (e.g. Anti-Virus)
    - Potential functional impact, regulatory and compliance violation

Hospital Security Challenges

Challenge	Root Cause	Security Impact
Long product life	• High replacement costs • Continued clinical utility • Dependencies (integration to training)	• Outdated security posture • HW EOL >> SW EOL • Prevalence of legacy equipment
Shared responsibilities	• Need for focus and specialization • Traditionally, departmental budgeting and purchasing decisions	• Communication & execution gaps • Varying security maturity
Care continuity	• 24x7 operations • Difficult to align maintenance activities with clinical operations	• Delayed patch deployment • System interdependency
Vendor dependency	• Regulations (e.g., FDA) • Technology constraints • Long development cycles	• Requiring vendor patch release • Vendor may dictate technology • Behind in technology platforms • Can not install security agents

Complexity of the Medical Device Ecosystem

PATCH



General platform, wired/wireless network

High risk of operational impact due to broad vulnerabilities, e.g. malware related shutdown. But – low(er) patient safety risk!

"Collateral Damage"

Targeted attack on highly vulnerable hospital ecosystem

The big "IF"

Implantable, proprietary, short-range communication

Requires targeted attack, technical skill, and affects only one patient. But – patient's can be harmed

Security Research

Deliberate attack to harm patient or hospital or manufacturer reputation

General Cyber Risk Classification of Medical Devices

	Implantable	Patient Care	Capital Equipment	Non-Medical
Example	Pacemaker, Insulin Pumps	Infusion Pump, Monitoring	MRI, CT, Proton Beam Accelerator	HVAC, elevators, security, fridges
Product Life	5-15 Years	5-10 years	10++ Years	5-10 years
Operating System	None / proprietary	Customized, RTOS, some commercial	Commercial (Windows, Linux)	Commercial (RTOS ... Windows, Linux)
Other COTS	No	Some, but limited (e.g., network stack)	Many (readers, media players, databases, …)	Some, but limited (e.g., network stack)
Integration	Proprietary; local (but can connect from there)	Wired/ wireless network	Wired/ wireless network	Wired/ wireless network
Targeted Attack potential	Yes (security research)	Yes (security research and actual incidents)	Yes (security research and actual incidents)	Yes (security research and actual incidents)
Collateral Damage potential	No	Maybe	Yes (incident based on opportunity)	Yes (incident based on opportunity)
Impact	Patient safety	Patient safety, care delivery	Patient safety, care delivery	Care delivery, (patient safety)
Harm Potential	High	Medium to high	Medium	Medium to low
Documented Incidents	Research only	Yes (hack by patient)	Yes (device as beachhead)	Yes, in many industries (Stuxnet, Volt Typhoon)

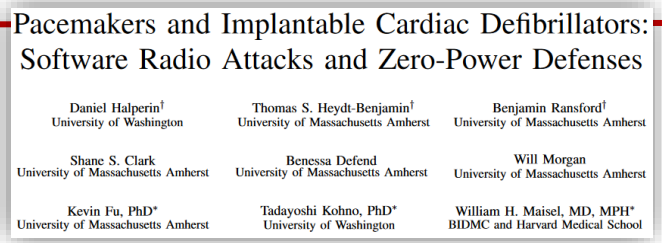
Acronyms

COTS = Commercial off-the-shelf Software
I/F = Interface
I/O = Input / Output
OS = Operating System
PHI = Protected Health Information (HIPAA)
RTOS = Real-time Operating System
SW = Software
U/I = User Interface

Medical Device Cybersecurity
Introduction

- Manufacturer vs Hospital Perspective
- Medical Device Incident Examples
- Trends and Analyses

Medical Device Security – Research Examples



Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses

Daniel Halperin† University of Washington
Thomas S. Heydt-Benjamin† University of Massachusetts Amherst
Benjamin Ransford† University of Massachusetts Amherst
Shane S. Clark University of Massachusetts Amherst
Benessa Defend University of Massachusetts Amherst
Will Morgan University of Massachusetts Amherst
Kevin Fu, PhD* University of Massachusetts Amherst
Tadayoshi Kohno, PhD* University of Washington
William H. Maisel, MD, MPH* BIDMC and Harvard Medical School

Proceedings of the 2008 IEEE Symposium on Security and Privacy

August 5, 2011 10:14 AM

Black hat hacker can remotely attack insulin pumps and kill people

By Chenda Ngak

(Credit: iStockphoto)

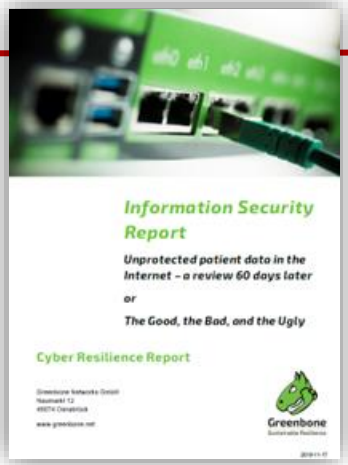
(CBS/AP) - As if we didn't already have enough to be neurotic about, a man at the Black Hat Technical Security Conference gave a presentation detailing how he could take control of insulin pumps from miles away and kill his victims.

Take a minute to panic. Now keep reading.

Jerome Radcliffe is a diabetic. The nefarious hack he presented at the conference Thursday was a response to his condition. "I have two devices attached to me at all times; an insulin pump and a continuous glucose monitor," said Radcliffe. He said that the devices turned him into a supervisory control and data acquisition (SCADA) system.

- Early Days Security Research:
  - ICD (IEEE, 2008, Kevin Fu) – widely noted but resulted in little change
  - Insulin Pump (BlackHat Conference, 2011, Jay Radcliffe, Barnaby Jack) - and triggered events (GAO report, FDA pre- and postmarket guidance)
- Exploiting proprietary protocols to change device settings
- Reported vulnerability to manufacturer, encountered resistance
- To date, no documented case that these (or similar) vulnerabilities have been exploited and resulted in patient harm
- Many researchers followed: Billy Rios, Mayo Clinic, Homeland Security (DHS), ….
- Security researcher: “The least secure device I ever laid hands on”
- Hacks that could kill – but research only, so far … and TV shows

Medical Device Cyber Incident Examples – Research



Greenbone Security Research (2019):

- 129 / 172 exposed PACS archives
- 1.19 billion images, 370 million directly accessible
- Representing about 800 institutions

https://www.greenbone.net/en/the-good_bad_ugly-amount_is_rising-2/

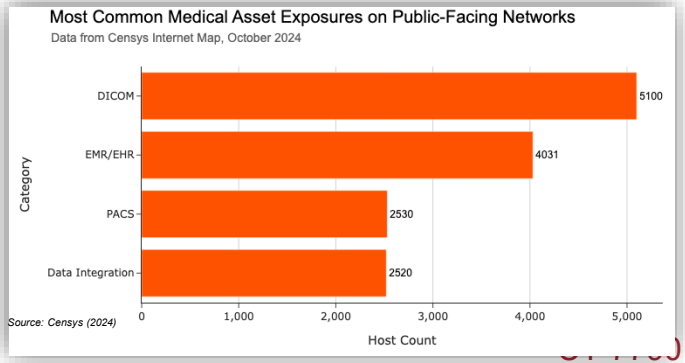
CybelAngel study (2020):

- Scanned 4.3B IP addresses across 67 countries
- Found 45M medical images accessible online

https://cybelangel.com/blog/medical-data-leaks/

Aplite (2023):

- 59M patients personal and medical records accessible online
- Presented at BlackHat Europe

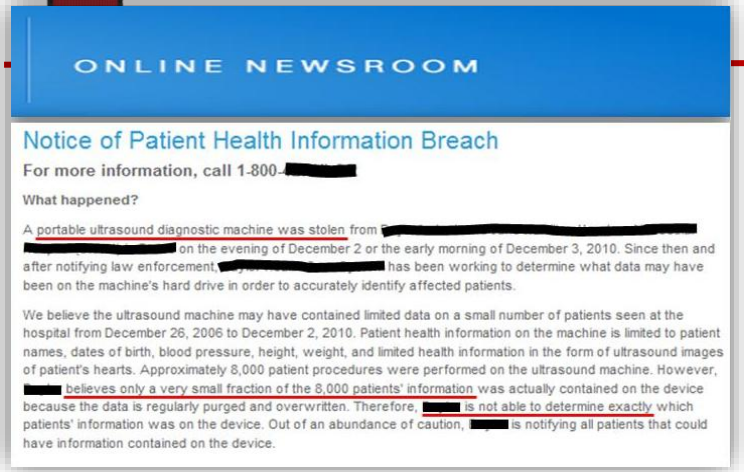


Censys (2024):

- Study: "The Global State of Internet of Healthcare Things (IoHT) Exposures on Public-Facing Networks:
- 5100 DICOM / 2530 PACS systems exposed
- Nearly 50% located in the US

https://censys.com/state-of-internet-of-healthcare-things/

Medical Device Cyber Incident Examples



ONLINE NEWSROOM

Notice of Patient Health Information Breach

For more information, call 1-800-[redacted]

What happened?

A portable ultrasound diagnostic machine was stolen from [redacted] on the evening of December 2 or the early morning of December 3, 2010. Since then and after notifying law enforcement, [redacted] has been working to determine what data may have been on the machine's hard drive in order to accurately identify affected patients.

We believe the ultrasound machine may have contained limited data on a small number of patients seen at the hospital from December 26, 2006 to December 2, 2010. Patient health information on the machine is limited to patient names, dates of birth, blood pressure, height, weight, and limited health information in the form of ultrasound images of patient's hearts. Approximately 8,000 patient procedures were performed on the ultrasound machine. However, [redacted] believes only a very small fraction of the 8,000 patients' information was actually contained on the device because the data is regularly purged and overwritten. Therefore, [redacted] is not able to determine exactly which patients' information was on the device. Out of an abundance of caution, [redacted] is notifying all patients that could have information contained on the device.

at

01. 12. 12. - 12:00

Patient hackers managed to dial a drug in hospital

By Rachael Williams

Patients at a Linz hospital became addicted to opiates after one of them managed to hack the computer that automatically delivered the drug, allowing them to dial up the drugs whenever they wanted.

01. 12. 12. - 12:00

more General News news

RSS Feed General News

The general hospital in Linz was spun into crisis at the end of 2011 when two people were admitted and attached to infusion pumps after being severely injured by gunshots and explosions.

Infusion pumps enable patients to provide themselves with medicine when they felt pain, but the supply of the medicine was only available in extremely limited doses.

It soon became clear that both patients had however become dependent on high dosages of painkillers. Their usage was so high that one of the patients even went into respiratory arrest.

Data Breach / Privacy Risks

- Lost or stolen device (multiple reported)
- Unencrypted transmission
- Poor decommissioning, lack of data sanitation (PHI, credentials)

Insider Threats

- Gun shot wound patients on PCA pump
- Drug dependent, dosage not sufficient
- Found pump service manual online
- Increased safety limit via Admin account

Medical Device Cyber Incident Examples

Device as Means for an Attack

- Beachhead and hiding point
- Demonstrated in 3 hospitals in 2015
- Found in 60+ hospitals since then (Bloomberg)
- Blood Gas, X-Ray, PACS, MRI, Defib, Fluro, …
- Current and legacy malware (incl. ransomware and botnet exploits)
- Traced back to Russian crime server
- Well-orchestrated APT attacks
- Medical devices a “near perfect target”
- Evolving attack strategy in recognition of medical device opportunity (2016)

Medical Device Security - Exam

Use of AI to Manipulate PACS Images

- PACS (at least the diagnostic software) is considered a medical device (SAMD = Software as a Medical Device)
- Security researchers used Machine Learning to introduce / remove evidence of cancer
- Three radiologists and an AI tool evaluated the images:
  - Radiologists were fooled 99% of the time for injection, and 94% of the time for removal
  - The AI system was fooled 100% of the time

Hackers can add, remove cancer and other illnesses from Computer Tomography scans

April 5, 2019 By Pierluigi Paganini

Researchers demonstrated that hackers can modify 3D Computer Tomography scans to add or remove evidence of a serious illness, including cancers.

A group of researchers from the Ben-Gurion University and the Soroka University Medical Center, Beer-Sheva, in Israel, have demonstrated that hackers can modify 3D medical scans to the result of a clinical examination.

Attackers can add or remove evidence of various illnesses, including aneurysms, heart disease, blood clots, infections, arthritis, cartilage problems, torn ligaments, and tumors in the brain, heart or spine.

The experts developed proof-of-concept (PoC) malware that uses a machine learning technique known as generative adversarial network (GAN) to alter 3D images generated during a Computer Tomography (CT) scan. Scans are sent to picture archiving and communication systems (PACS) that store them. The format used to transmit and store the images is DICOM. GE Healthcare, Fujifilm, Philips, and RamSoft are main vendors of PACS systems.

PACS and DICOM servers are often left exposed to the Internet, the experts found roughly 2,700 servers exposed online using the Shodan search engine.

The experts also discovered that medical imagery data are transmitted without encryption, an attacker can potentially run man-in-the-middle (MitM) attacks to manipulate them.

The experts conducted a penetration test in a radiology department of a hospital. In a test scenario, they connected a small MitM device between the CT scanner's workstation and the PACS network that allowed them to intercept traffic from the CT scanner. The researchers developed an attack framework dubbed CT-GAN to manipulate the images via the GAN technique.

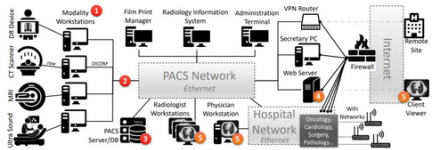


Figure 3: A network overview a PACS in a hospital. 1-3: points where an attacker can tamper with all scans. 4-5: points where an attacker can tamper with a subset of scans.

https://securityaffairs.co/wordpress/83412/hacking/computer-tomography-scans-hack.html

Medical Device Cyber Incident Examples

THE LANCET
Oncology

News

Increase in health-care cyberattacks affecting patients with cancer

A recent cyberattack against oncology services in the USA has left several hospitals reeling and patient care disrupted as sensitive patient information such as names, dates of birth, social security numbers, and diagnosis and treatment information were potentially exposed.

The attack—which occurred in April, 2021—targeted data stored in cloud-based systems supplied by the Swedish company Elekta (Stockholm, Sweden), affecting patients in several US states, including the Cancer Centers of Southwest Oklahoma (Lawton, OK, USA), the multihospital system Northwestern Memorial HealthCare (NMHC, Chicago, IL, USA), and Emory Saint Joseph's Hospital (Atlanta, GA, USA). The NMHC alone reported that the sensitive data of approximately 200 000 of their patients were compromised in the attack.

Yet, it was not just patient data that were affected; hackers targeted the software for linear accelerators used in radiotherapy, resulting in disruption to treatment sessions at 42 different health-care sites. This hack of clinical technology represents an emerging threat in global medical technology cybersecurity, in which attacks are no longer limited to the usual data breaches but increasingly target medical systems to disrupt patient care and devices that function as entry points into hospital networks. Devices infected by ransomware can be disabled so that they no longer perform their clinical function, experts warn, thus affecting the very functionality on which patient health care depends.

"Critical functions are shifting from on-premises software infrastructure to distributed and remote infrastructure, including newly essential cloud services depended upon during the diagnosis and treatment of disease", explained Kevin Fu, acting Director of Medical Device Cybersecurity at the US Food and Drug Administration's Center for Devices and Radiological Health (Silverspring, MD, USA). "Publicly noted cybersecurity incidents in 2021 include a fundamentally new problem where ransomware remediation disrupted the cloud services necessary for critical function of cancer radiotherapy rather than simply disrupting electronic health record systems and other, more traditional hospital IT infrastructures. Such increasingly common ransomware incidents highlight the ungraceful failure of perimeter-based firewalls and the safety consequences of not separating operational technology from IT by design."

In addition to cybercriminals using increasingly sophisticated approaches, experts believe that the incidence of attacks has risen exponentially during the COVID-19 pandemic as hackers have exploited the vulnerabilities exposed within medical care networks as a result of the crisis. In their annual Breach Barometer report on the subject, technology consulting firm Protenus (Baltimore, MD, USA) recorded 470 cases of cyberhacking in health-care organisations in 2020 versus only 330 in 2019—representing an increase of 42% from one year to the next. The largest breach reported in 2020 was the result of a hacking incident involving ransomware that affected 3 220 726 patient records in a single health system.

In the past few months alone, a spate of international cyberattacks on health-care systems have highlighted cybersecurity as an urgent global issue. In April, 2021, hackers used ransomware to infect the digital and technology systems of Uniting Care Queensland (Brisbane, QLD, Australia), rendering their email and operation booking systems inaccessible; the following month in San Diego (CA, USA), Scripps Health fell victim to an attack in which hackers stole the sensitive data of 147 267 of its patients before deploying ransomware on the network; and in Ireland, a large-scale cyberattack involving ransomware forced the Health Service Executive, Ireland's publicly funded health-care system, to shut down its entire information technology system, cutting off access to patient records and disrupting services that rely on digital processes, such as scans, referrals, and diagnostic services. As technology advances and health-care systems become increasingly digitally connected, the potential risk of such incidents will only increase, emphasising the need for health-care organisations worldwide to take steps to prioritise cybersecurity and reduce their vulnerability to cybercriminals.

"Increasing cyberattacks affecting hospitals and health care systems worldwide result in compromised care for patients in the screening, diagnosis and treatment of their cancer", commented Carl Nelson (Larner College of Medicine, University of Vermont Medical Center, Burlington, VT, USA). "Radiotherapy is particularly vulnerable to systems disruptions due to the reliance on complex radiation planning, delivery and verification systems that require uninterrupted, integrated network communication. Both cloud-based systems and local network server systems are vulnerable to cyberattacks and require contingency planning for prolonged system outages. Whether cyberattacks are intentional ransomware or inadvertent malware, the similar debilitating resulting lack of operability of systems vital for the care of patients with cancer will ultimately result in compromised oncology care and patient survival."

Elizabeth Gourd

Lancet Oncol 2021
Published Online
July 29, 2021
https://doi.org/10.1016/S1470-2045(21)00453-4

www.thelancet.com/oncology Published online July 29, 2021 https://doi.org/10.1016/S1470-2045(21)00453-4 1

Ransomware attack on cloud-based radiotherapy planning service (April 2021):

- Compromised sensitive data of approx. 200,000 patients
- Targeted software for linear accelerators, disrupting treatment at 42 sites

"Increasing cyberattacks affecting hospitals and health care systems worldwide result in compromised care for patients in the screening, diagnosis and treatment of their cancer … Radiotherapy is particularly vulnerable to systems disruptions due to the reliance on complex radiation planning, delivery and verification systems that require uninterrupted, integrated network communication … Whether cyberattacks are intentional ransomware or inadvertent malware, the similar debilitating resulting lack of operability of systems vital for the care of patients with cancer will ultimately result in compromised oncology care and patient survival."

https://www.sciencedirect.com/science/article/pii/S1470204521004514

Understand the Whole System

Friday, June 8, 2012

Click Here to Download Your AVEA Ventilator Software Update. Trust Me.

[Updates contributed from readers appear at the bottom of this blog post.]

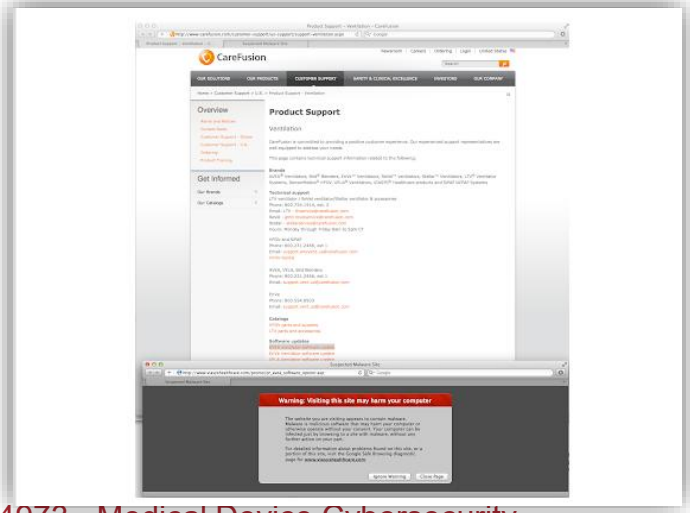
> Summary: The web server distributing the software updates for a ventilator (a medical device) itself needs some help with software updates. According to Google, the web server was infected with 48 viruses and 2 scripting exploits. 20 pages resulted in malicious software being downloaded and installed without user consent.
>
> The risks should be obvious. This is an update for a medical device, and yet one must download it in a manner as if software sepsis is no big deal. Health care professionals might as well stop their washing hands while they're at it.

Hospital IT staff: How much do you trust the Internet for updating medical device software? A number of researchers in software upgrades bemoan the general state of the art for secure software updates. Worse, the cryptographic technology at the core of commercial software update mechanisms is broken and being actively exploited by the Flame virus.

Well, if you work for a hospital, the Flame virus is probably the least of your worries. You just want to keep your HIT systems and software-controlled medical devices working. Vendors routinely install software updates for medical devices from the Internet or USB keys. I've seen medical sales engineers download pacemaker-related software from the Internet.

Today I tried to download a software update for CareFusion AVEA Ventilators. What I found may disturb hospital IT staff. Here's a screenshot. When I clicked on the highlighted link for "AVEA Ventilator software update," a second dialog box popped up, "Warning: Visiting this site may harm your computer."

- Infected download server for patches
- 48 viruses and 2 scripting exploits
- FDA stipulates to look at the whole system: clinical function, technical function, integration, …



SECURITYWEEK
CYBERSECURITY NEWS, INSIGHTS & ANALYSIS

Malware & Threats | Security Operations | Security Architecture | Risk Management | CISO Strategy | ICS/OT | Funding/M&A

VULNERABILITIES

St. Jude Medical Recalls 465,000 Pacemakers Over Security Vulnerabilities

Pacemaker Patients Must Visit Healthcare Provider for Firmware Update That Addresses Security Vulnerabilities

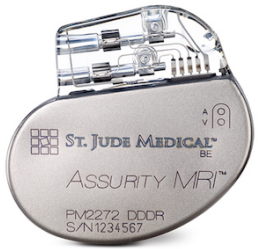
By Ionut Arghire
August 31, 2017

Pacemaker Patients Must Visit Healthcare Provider for Firmware Update That Addresses Security Vulnerabilities

A firmware update to address security vulnerabilities has been approved and is now available for radio frequency (RF)-enabled St. Jude Medical (now Abbott) implantable pacemakers, the U.S. Food and Drug Administration (FDA) announced this week.

Vulnerabilities in St. Jude Medical's devices were made public last year by [redacted] as investment strategy to short sell shares of St. Jude's stock. The report claimed that attackers could, among other things, crash implantable cardiac devices and drain their battery at a fast rate.

St. Jude rushed to refute the allegations and even sued the two companies, while University of Michigan researchers analyzed the [redacted] report and discovered that their proof-of-concept (PoC) exploit did not actually crash the implanted cardiac device.



[redacted] responded to the lawsuit in October, after contracting security consulting firm [redacted] provide an expert opinion on St. Jude implantable cardiac devices. They also

Example Cyber-Recall

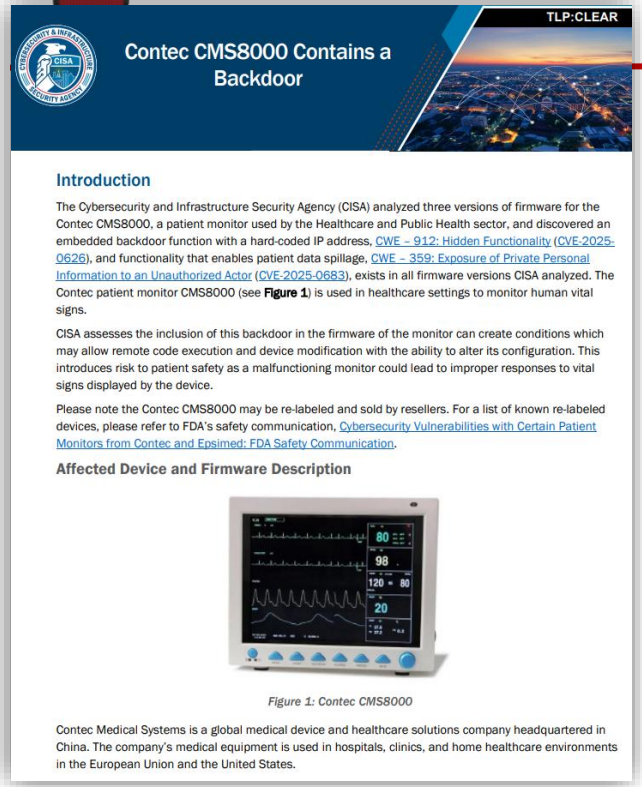
Lessons from a Recall:

- The Adversary is not always in Russia, North Korea, or China.
- Good CVD process could have helped, but both sides need to play.
- Patching is never easy.
- How to communicate with non-technical stakeholders?
- Patient communication is key - but not easy.

To install the update, patients must visit a healthcare provider, as the operation cannot be performed at home.

"The FDA recommends that patients and their health care providers discuss the risks and benefits of the cybersecurity vulnerabilities and the associated firmware update designed to address such vulnerabilities at their next regularly scheduled visit," the FDA announced.

FDA/CISA Warning: Contec CMS8000 Contains a Backdoor



TLP:CLEAR

Contec CMS8000 Contains a Backdoor

Introduction

The Cybersecurity and Infrastructure Security Agency (CISA) analyzed three versions of firmware for the Contec CMS8000, a patient monitor used by the Healthcare and Public Health sector, and discovered an embedded backdoor function with a hard-coded IP address, CWE – 912: Hidden Functionality (CVE-2025-0626), and functionality that enables patient data spillage, CWE – 359: Exposure of Private Personal Information to an Unauthorized Actor (CVE-2025-0683), exists in all firmware versions CISA analyzed. The Contec patient monitor CMS8000 (see **Figure 1**) is used in healthcare settings to monitor human vital signs.

CISA assesses the inclusion of this backdoor in the firmware of the monitor can create conditions which may allow remote code execution and device modification with the ability to alter its configuration. This introduces risk to patient safety as a malfunctioning monitor could lead to improper responses to vital signs displayed by the device.

Please note the Contec CMS8000 may be re-labeled and sold by resellers. For a list of known re-labeled devices, please refer to FDA's safety communication, Cybersecurity Vulnerabilities with Certain Patient Monitors from Contec and Epsimed: FDA Safety Communication.

Affected Device and Firmware Description

Figure 1: Contec CMS8000

Contec Medical Systems is a global medical device and healthcare solutions company headquartered in China. The company's medical equipment is used in hospitals, clinics, and home healthcare environments in the European Union and the United States.

https://www.cisa.gov/sites/default/files/2025-01/fact-sheet-contec-cms8000-contains-a-backdoor-508c.pdf

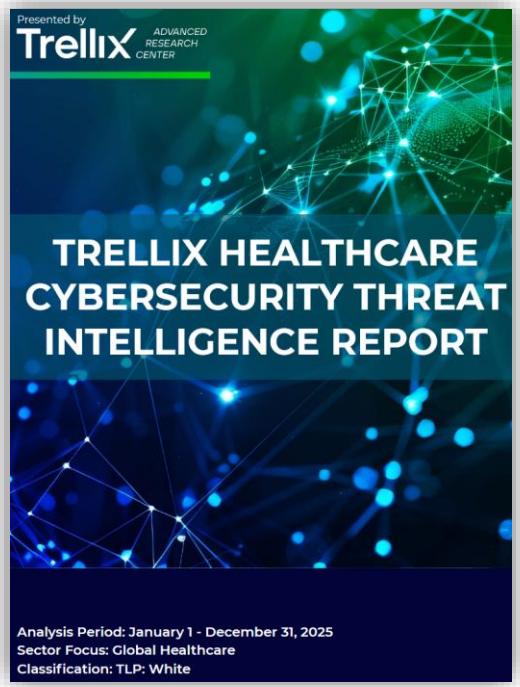
Contec Health CMS8000 Patient Monitor

- CSMA-25-030-01; January 30, 2025
- Classified as remotely exploitable / low attack complexity
- CVE-2024-12248 - Out-of-bounds Write, CWE-787
  CVSS v3.1 score 9.8; CVSS; v4 score 9.3
- CVE-2025-0626 - Hidden Functionality (Backdoor), CWE-912
  CVSS v3.1 score 7.5; CVSS v4 score 7.7
- CVE-2025-0683 - Exposure of Private Personal Information to an Unauthorized Actor (Privacy Leakage), CWE-359
  CVSS v3.1 score 5.9; CVSS v4 score 8.2
- Preconfigured / hard-coded IP address for product updates and HL7 communication pointing to a University in China.
- Subsequent research by Claroty and Cylera would indicate that this was not a malicious backdoor but a poor design decision.
- Also found in monitors from 2 other manufacturers (IP questions).
- Good security practices could have avoided this: threat modeling, code review, pen testing, and coordinated vulnerability disclosure (CVD).

Medical Device Cybersecurity
Introduction

- Manufacturer vs Hospital Perspective
- Medical Device Incident Examples
- Trends and Analyses

Survey Insights



Not all are trustworthy. Always ask:

- What is the publishing entity's motivation? That may limit how they frame their survey and the type of data they are collecting.

Do your homework:

- Does their methodology seem defensible?
- Is the source reputable?
- Did they collect sufficient number of results?
- Do the results pass the plausibility check?
- Does it align with known data and trends?

Survey Insights

PATCH

LANDMARK HEALTHCARE CYBERSECURITY INCIDENTS IN 2025

In 2025, the U.S. Department of Health and Human Services (HHS) disclosed about 516 breaches, impacting more than 35.5 million individuals. Each breach represents more than just data on a spreadsheet; it means patients facing uncertainty about their privacy and organizations scrambling to restore trust.

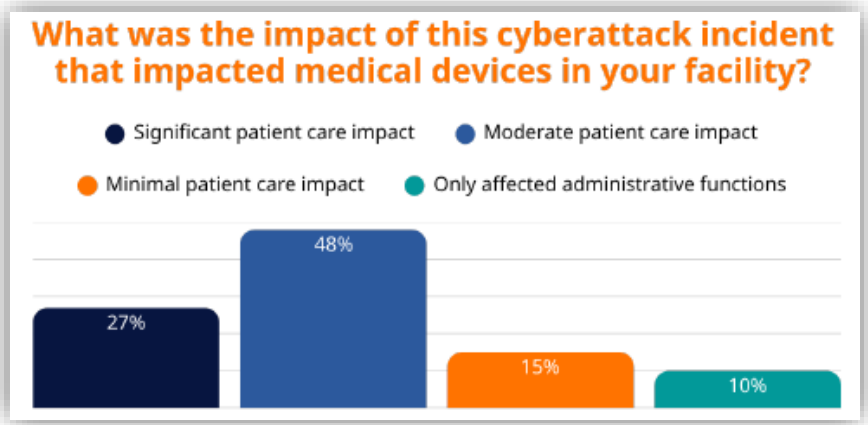
Previous years ~700/yr

Conclusion – this report does not seem trustworthy

Non-device vulnerabilities listed in the medical device section

- Contec Health CMS8000 (CVE-2025-0683): This critical vulnerability involves an embedded backdoor within the firmware of patient monitors. In its default configuration, the device transmits plain-text patient data to a hard-coded public IP address, allowing unauthorized remote actors to exfiltrate private health information or take control of the device to perform unintended actions.
- Oracle E-Business Suite (CVE-2025-61882): This multi-stage exploit chain combines authentication bypass and remote code execution to compromise Oracle Concurrent Processing without requiring user credentials. On October 6, 2025, the AHA issued an urgent alert urging immediate action for all hospitals using Oracle EBS. The FBI classified this as a "stop-what-you're-doing and patch immediately" vulnerability, noting its role in large-scale healthcare data theft. High-profile groups like Cl0p ransomware have targeted this flaw to shut down operational back-ends and exfiltrate sensitive employee and financial data from health systems. One of the UK's largest hospital trusts confirmed it was a victim of the Cl0p ransomware gang, which exploited this specific zero-day in August 2025 to steal financial and patient-related invoice data.
- Cisco Secure Email (CVE-2025-20393): This maximum-severity (CVSS 10.0) zero-day vulnerability affects AsyncOS software when the Spam Quarantine feature is enabled. On December 18, 2025, NHS England Digital issued a high-severity alert regarding an ongoing exploitation campaign targeting Cisco Secure Email appliances.
- SonicWall SMA 1000 (CVE-2025-40602): A critical local privilege escalation flaw found in the Appliance Management Console (AMC) due to insufficient authorization checks. Published in December 2025, the NHS England National CSOC assessed future exploitation of this vulnerability as "likely" for healthcare entities. The alert warns that when chained with CVE-2025-23006, this flaw allows for unauthenticated remote code execution (RCE) with root privileges.

Survey Insights



When experiencing a cyber attack, 75% reported the impact as significant to moderate.

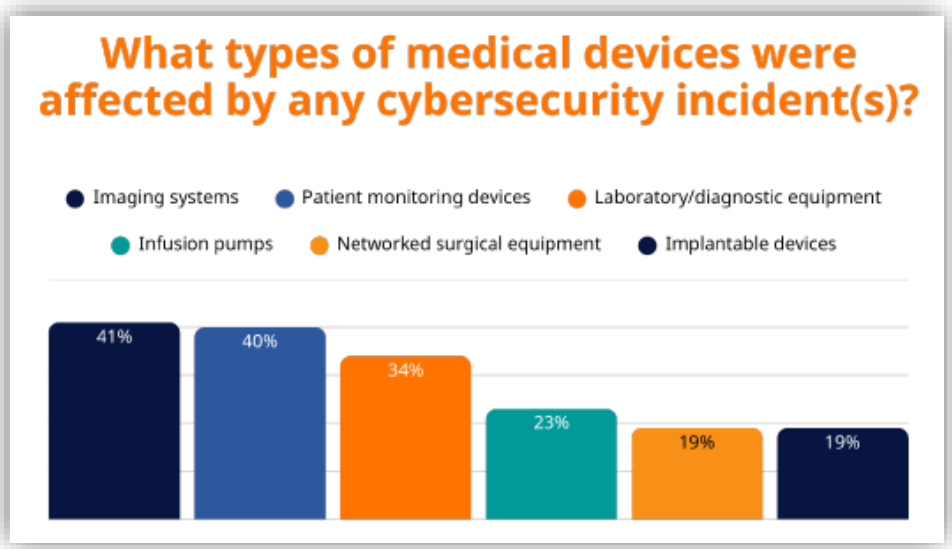
Survey Insights

What drives the Top 4? My guess:

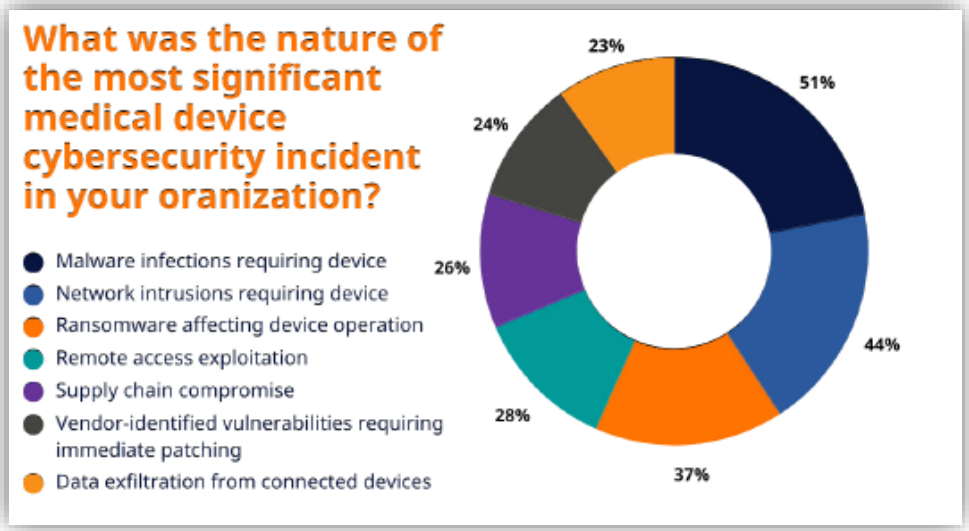
- Imaging and Lab = external openness
- Monitoring and Pumps = number of devices

What worries me?

- Surgical Equipment
- Implantable Devices



Survey Insights



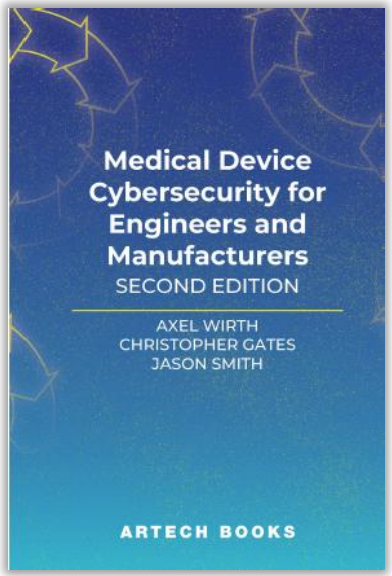
Malware infections (51%) and network intrusions (44%) are the primary weapons, forcing healthcare organizations to quarantine critical devices and isolate entire systems from their networks.

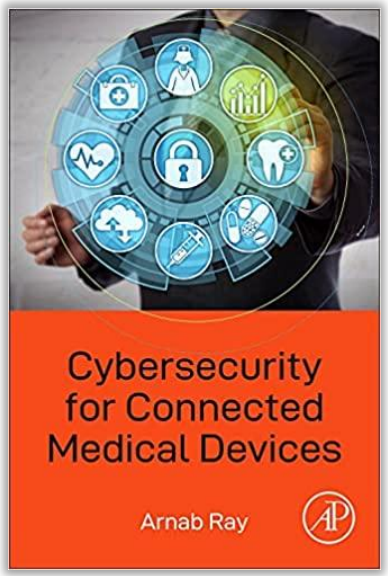
BUT report states ransomware specifically designed to disrupt device operations?
My interpretation: ransomware exploit that fit the device profile.

Thank you!

axel@medcrypt.com

General Resources - For Medical Device Manufacturers

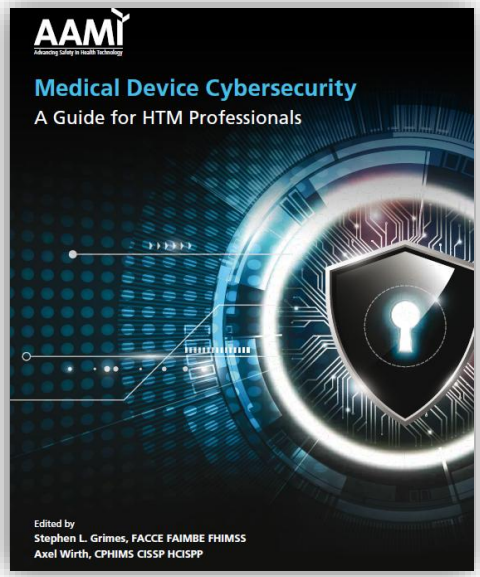




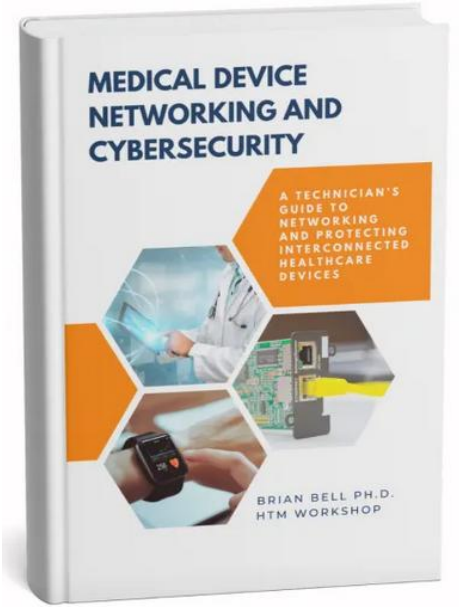
US: https://us.artechhouse.com/Medical-Device-Cybersecurity-for-Engineers-and-Manufacturers-Second-Edition-P2416.aspx
UK: https://uk.artechhouse.com/Medical-Device-Cybersecurity-for-Engineers-and-Manufacturers-Second-Edition-P2354.aspx

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

General Resources - For Healthcare Delivery Organization

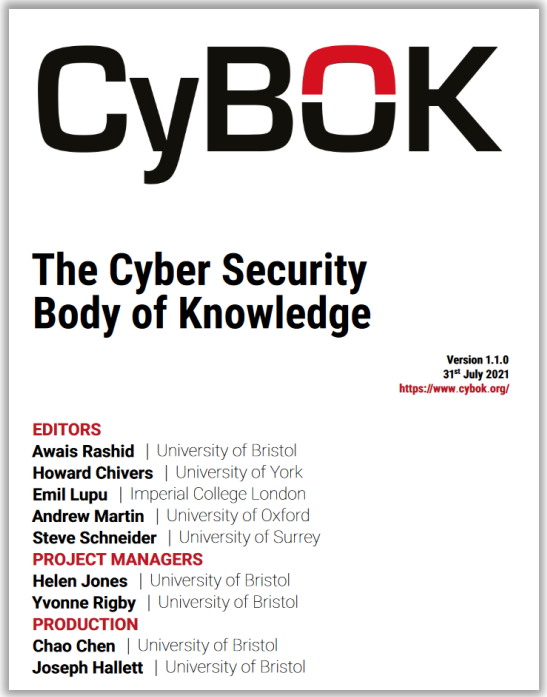


https://store.aami.org/s/store#/store/browse/detail/a152E000006j66qQAA



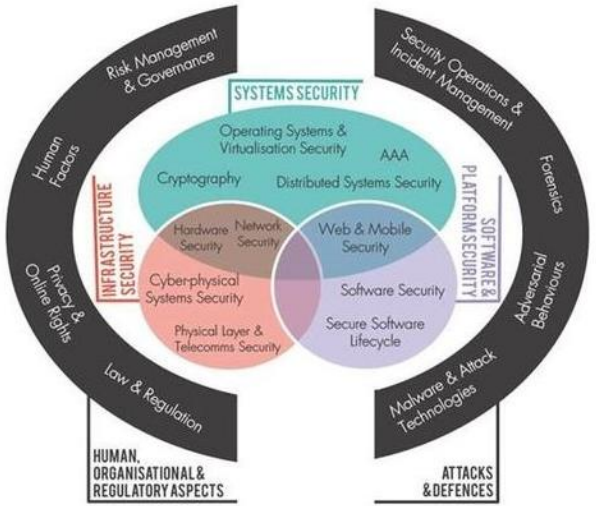
https://htm-workshop.com/shop/medical-device-networking-and-cybersecurity/

General Resources - CyBOK



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