Cybersecurity: U.S.A. Perspectives & Experience

Patrick Hope, JD
Executive Director
Medical Imaging & Technology Alliance (MITA)

DITTA Medical Software Workshop
Brasilia, 7 March 2016

MITA®
MEDICAL IMAGING
& TECHNOLOGY ALLIANCE
A DIVISION OF NEMA®

Section 1

Introduction to Cybersecurity

Cybersecurity & Healthcare
Cybersecurity in Medical Imaging
Towards a cyber-secure future

What is cybersecurity?

- Cybersecurity definition –

  "the state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this."

- Everything that connects to the internet can be attacked through the internet

- Cybersecurity protects hardware, software, systems, and information online

Introduction to Cybersecurity

Why is cybersecurity important?

In the past:

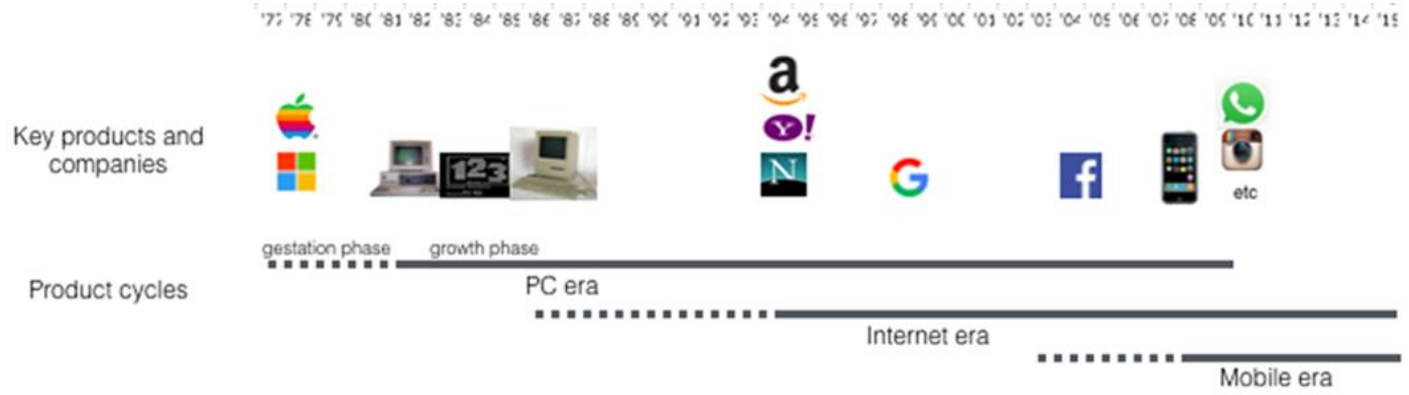
- Information was shared person-to-person

Now:

- Information is shared online

Over time, sharing information online increasingly easy, convenient, and efficient:

- Internet access everywhere, on everything!



Introduction to Cybersecurity

Why is cybersecurity important?

- Virtually all software, applications, systems and devices are now connected to the Internet
  - Financial institutions, hospitals, governments, corporations – and private individuals – increasingly internet-reliant
- This is a reality that cybercriminals recognize and are actively exploiting.

Introduction to Cybersecurity

Why is it important to healthcare?

- Hospitals, insurers, Electronic Health Records (EHR) increasingly targeted by cyber criminals
- Maybe you've seen the news...

Introduction to Cybersecurity

MITA MEDICAL IMAGING & TECHNOLOGY ALLIANCE A DIVISION OF NEMA

Hospital pays hackers $17,000 to unlock EHRs frozen in 'ransomware' attack

By Joseph Conn | February 17, 2016

(This story was updated on Feb. 18, 2016.)

A Southern California hospital's computers have been restored after it paid a $17,000 ransom in bitcoins to hackers who infiltrated and disabled its network. The gambit isn't new, but it appears to be on the rise.

By KRIS VAN CLEAVE / CBS NEWS / February 5, 2015, 6:45 PM

Anthem hack highlights desirability of stolen health records

26 Comments / 621 Shares / Tweet / Stumble / Email

Anthem, the nation's second largest health insurer, has warned up to 80 million Americans that their health care records could now be in the hands of criminal hackers.

Criminal attacks are now leading cause of healthcare breaches

Ponemon Institute, May 2015

The *Fifth Annual Benchmark Study on Privacy and Security of Healthcare Data* by the Ponemon Institute, sponsored by ID Experts, reveals a shift in the root cause of data breaches from accidental to intentional. Criminal attacks are up 125%

npared to five years ago replacing lost laptops as the leading eat. The study also found most organizations are

Cybersecurity: effective strategies must protect medical devices

February 25, 2016
By Ken Zalevsky

Medical devices are a critical component of th care infrastructure, accounting for about $350 annually. The U.S. Department of Health and H than one billion patient encounters (visits to ph emergency departments) annually in the United

HealthData Management

Why cyber attacks compel new approaches to security

By Joseph Goedert

Published February 17 2016, 11:03am EST

THE WALL STREET JOURNAL.

TECH

Health Insurer CareFirst Says It Was Hacked

Cyberattack involved database of 1.1 million members' information; China suspected

By ANNA WILDE MATHEWS and DANNY YADRON
Updated May 20, 2015 5:57 p.m. ET

CareFirst BlueCross BlueShield said Wednesday that hackers had gained access to the personal information of more than a million consumers, becoming the third major health insurer this year to disclose a breach.

UCLA Health: 4.5 Million Affected

UCLA Health detected suspicious network activity in October 2014 and investigated with assistance from the FBI. At that time, it did not appear that the attackers had gained access to parts of the network that contain personal and medical information, the health system said. As part of an ongoing investigation, UCLA on May 5, 2015, determined that attacks had accessed parts of its network and may have had access as early as

Introduction to Cybersecurity

Why is it important to healthcare?

- Healthcare data is very valuable
- In 2015, Rising Cyber Attacks Cost U.S. Health System $6 Billion
- Cyberattacks will compromise 1-in-3 healthcare records in 2016
- Some 94 percent of medical institutions said their organizations have been victims of cyber crime
- Majority of attacks avoidable!
- Proper procedures and training are key!

Section 2

Introduction to Cybersecurity
Cybersecurity & Healthcare
Cybersecurity in Medical Imaging
Towards a cyber-secure future

Cybersecurity & Healthcare

Hospitals first to:

- Create networks, connecting devices and systems
- Standardize communication between all devices, systems, platforms on a network (DICOM)

Healthcare providers increasingly sensitive to cyber threat due to increasing:

- Digitalization of devices; connectivity between devices
- Complexity of systems, networks
- Patient information and hospital administration data shared and stored online

Cybersecurity & Healthcare

Hospital IT security lapse can have dangerous consequences:

- breakdown of function/component, affecting the provision of medical care
  - Defibrillator, ventilation, interventional diagnosis, reporting, orders --billing , trials, outbreak
- loss of medical data, also: compromising, forging data
  - confusion of entities (e.g.: patient, image, order)
  - concepts for diagnosis (wrong diagnosis encoding)
  - units of measure (e.g.: milligram / microgram in prescription dosage)

Cybersecurity & Healthcare

Standards, regulations, processes developed for special security concerns of clinical settings:

- 1999 “Programmable Electrical Medical Systems,” 2005 FDA, 2007 FDA & IEC
- IEC/ISO 80001-1 published as international standard in October 2010
  - Implementation is not a legal requirement but “state-of-the-art”
  - Message: Hospitals shall perform Risk Management for their IT-Networks with connected medical devices.
- IT risk management shall focus on the INTENDED USE of that IT-Network
  - Sending and processing orders
  - Sending, reporting, storing and retrieving images
  - Patient administration and collecting / processing claims
  - Collecting and managing medical files
  - Sending alarms (IP-Telephony as patient- added-value? general internet surfing?)
- Hazards affect the “Key Properties:” Safety, Security, Effectiveness
  - regarding the network‘s intended use
- Hospital top management remains responsible – no transfer/delegation
- Manufacturers shall document IT-network risks of networked products

Cybersecurity & Healthcare

Cybersecurity in healthcare – status varies

- Healthcare providers and insurers' level of security preparedness varies widely among organizations:
  - Adoption of security technology slower than other industries
  - Implementation of staff training and patient education remains a challenge

Cybersecurity & Healthcare

Cybersecurity in medical devices –

- Medical device industry proactive:
  - Potential threats to patient safety being addressed now, before catastrophe
  - August 2015: FDA issued alert of security flaws in transfusion pump; product taken off the market
  - Message to medical device manufacturers: products must be secured and maintained during entire life cycle, from deployment to retirement

Section 3

Introduction to Cybersecurity
Cybersecurity & Medical Devices
Cybersecurity in Medical Imaging
Towards a cyber-secure future

Cybersecurity in Medical Imaging

Why is MITA focused on cybersecurity?

- Imaging department has increased risk profile compared to rest of hospital
  - *Can't hide behind hospital IT*
- New paradigms create new concerns:
  - Film-based to all-digital imaging
  - Medical imaging systems interconnected with each other, hospital & internet
  - Danger of attacks not only in disclosure of e-Personal Health Info (ePHI), but in compromised patient safety
- Prevention requires specialized cybersecurity awareness and training for personnel

Cybersecurity in Medical Imaging

- MITA Cybersecurity in Medical Imaging White Paper: http://www.nema.org/Standards/Pages/Cybersecurity-for-Medical-Imaging.aspx#download
  - A collaboration between manufacturers and users
  - Active engagement between MITA and American College of Radiology (ACR), professional society for radiology professionals
  - Key to usefulness: perspectives and support from both technology manufacturers and personnel that operate the technology
- Advancing cybersecurity measures in healthcare and public health: a 'whole of community' approach:
  - Shared ownership and responsibility between regulators, manufacturers, service providers

Cybersecurity in Medical Imaging

Cybersecurity in Medical Imaging

- Cybersecurity involves a continuum:
  - Products –

    …must be designed to be cyber-secure
  - Procedures –

    …plans developed for avoiding, and responding to cyber attack
  - People –

    …users and operators understand and follow risk-mitigation procedures

Cybersecurity in Medical Imaging

Four Components of medical imaging cybersecurity:

1. Device Security
   - Manufacturers test security of their devices against simulated threats and unintended use
2. External Security
   - Equipment operators take steps to protect their networks medical devices: firewalls, antivirus, etc.
3. Securing Communication
   - Internal and external communication must be secure; should use existing standards: HTTPS–TLS, DICOM
   - Manufacturers increasingly considered Business Associates (BAs) HIPAA Security Rule Part 45 of the CFR if their devices interact with patient data

Cybersecurity in Medical Imaging

Four Components of medical imaging cybersecurity:

4. The Responsible User
   - Best-in-class protective technology and risk assessment tools to prevent attack:
     - VPN, encryption, thin client technologies, high availability IT infrastructure, data back-up mechanisms, firewalls, standards ISO 80001, ISO 14971, and EN ISO 14971
   - Effective training and education of staff is essential!
     - Training is often the weak link in cybersecurity
     - A robust cybersecurity plan is achieved only when processes for cyber prevention are clearly defined and effectively followed by staff thoroughly trained in cybersecurity.

Section 4

Introduction to Cybersecurity
Cybersecurity & Healthcare
Cybersecurity in Medical Imaging
Towards a cyber-secure future

Towards a cyber-secure future

U.S. government, civil society, and enterprise lead the world in internet privacy and security

- With the goal of enhancing internet safety and innovation, high-quality cybersecurity resources have been developed and made available for free online:
  - HITRUST Alliance HITRUST Common Security Framework (CSF)
  - NIST HIPAA Security Toolkit Application
  - HIMSS Risk Assessment Toolkit
  - HIMSS Privacy & Security Toolkit—additional Privacy and Security Toolkits
  - HIMSS list of Security Standards and Baselines
  - SANS 20 Critical Security Controls
  - HIMSS/NEMA HN 1-2013 Manufacturer Disclosure Statement for Medical Device Security
  - NEMA CPSP 1-2015, Supply Chain Best Practices

Towards a cyber-secure future

IN CONCLUSION:

Cybersecurity of any organization depends on preparedness of both technology and people

- Efforts made by governments, corporations, and civil society around the world to continually improve cybersecurity
  - Example: United States Department of Homeland Defense - Cyber Storm Exercises I-V. Partners in international, federal, state, local govts; private sector including healthcare now involved
  - Continual cycle of testing, troubleshooting and training is needed to ensure systems are secure

Towards a cyber-secure future

- Cybersecurity in medical imaging is a shared responsibility between healthcare providers and manufacturers.
  - Imaging staff must be aware of cybersecurity threats and best-in-class practices.
  - Processes must be defined and implemented, and the proper technology must support ultimate zero-breach cybersecurity goals.

Towards a cyber-secure future

- MITA, representing medical imaging device manufacturers, will continue to be a valuable resource in the field of cybersecurity standards and regulations, in collaboration with professional organizations representing medical imaging and IT professionals.

MITA Cybersecurity White Paper

DITTA Medical Software Workshop – Brasilia, March 2016

Thank you!
Obrigado!