Medical Physicist role in Cyber Security: Threats, Vulnerabilities and Preventions

Rishabh Kapoor, MS
Assistant Professor of Radiation Oncology
Virginia Commonwealth University
Richmond, VA

Objectives

- Discuss why cyber security is critically important for in healthcare and its current state of affairs.
- Illustrating common threats and methods used by cyber criminals
- Simple and effective things a clinical physicist must do to proactively prevent such situations
- Discuss implementation of best security practices from the vendor systems

2014

MIT Technology Review

Intelligent Machines

Hackers Are Homing In on Hospitals

Computer criminals are increasingly capturing valuable information stored on hospital computer networks.

by **Mike Orcutt** Sep 2, 2014

Cybercriminals are increasingly targeting the computer networks of hospitals—one recently announced theft involved data from 4.5 million people who had received treatment from Community Health Systems (CHS), a company that runs more than 200 hospitals. Malware attacks are on the rise in many industries, but researchers from the security firm Websense say the rate at which attacks on hospitals has grown during the past year is unparalleled.

2014

MIT Technology Review

Intelligent Machines

Hackers Are Homing In on Hospitals

Computer criminals are increasingly capturing valuable information stored on hospital computer networks.

by **Mike Orcutt** Sep 2, 2014

Cybercriminals are increasingly targeting the computer networks of hospitals—one recently announced theft involved data from 4.5 million people who had received treatment from Community Health Systems (CHS), a company that runs more than 200 hospitals. Malware attacks are on the rise in many industries, but researchers from the security firm Websense say the rate at which attacks on hospitals has grown during the past year is unparalleled.

2016

Anthem: Insider theft exposes data of 18,000 Medicare members

Anthem's Medicare insurance coordination services vendor discovered in April that an employee was stealing and misusing Medicaid member data from as early as July 2016.

2014

MIT Technology Review

Intelligent Machines

Hackers Are Homing In on Hospitals

Computer criminals are increasingly capturing valuable information stored on hospital computer networks.

by Mike Orcutt Sep 2, 2014

Cybercriminals are increasingly targeting the computer networks of hospitals—one recently announced theft involved data from 4.5 million people who had received treatment from Community Health Systems (CHS), a company that runs more than 200 hospitals. Malware attacks are on the rise in many industries, but researchers from the security firm Websense say the rate at which attacks on hospitals has grown during the past year is unparalleled.

2016

Anthem: Insider theft exposes data of 18,000 Medicare members

Anthem's Medicare insurance coordination services vendor discovered in April that an employee was stealing and misusing Medicaid member data from as early as July 2016.

2017

NHS cyber attack: Everything you need to know about 'biggest ransomware' offensive in history

2017

PA Security Breach from Missing External Hard Drive Affects 4.1K

Recent potential healthcare security breaches include a missing external hard drive, improper disposal, and a cybersecurity attack.

2017

PA Security Breach from Missing External Hard Drive Affects 4.1K

Recent potential healthcare security breaches include a missing external hard drive, improper disposal, and a cybersecurity attack.

2018

MedEvolve Cops to Healthcare Data Breach With PHI on 200K at Risk

Recent healthcare data breaches include MedEvolve admitting to previously reported breach of PHI on its public FTP server and two breaches involving employee misconduct.

2017

PA Security Breach from Missing External Hard Drive Affects 4.1K

Recent potential healthcare security breaches include a missing external hard drive, improper disposal, and a cybersecurity attack.

2018

MedEvolve Cops to Healthcare Data Breach With PHI on 200K at Risk

Recent healthcare data breaches include MedEvolve admitting to previously reported breach of PHI on its public FTP server and two breaches involving employee misconduct.

2018

HealthEquity Email Hack Breaches Data of 190K Patients

This is the second breach reported by the health savings trustee this year. In June, an unauthorized user breached the data of 16,000 individuals.

2017

PA Security Breach from Missing External Hard Drive Affects 4.1K

Recent potential healthcare security breaches include a missing external hard drive, improper disposal, and a cybersecurity attack.

2018

MedEvolve Cops to Healthcare Data Breach With PHI on 200K at Risk

Recent healthcare data breaches include MedEvolve admitting to previously reported breach of PHI on its public FTP server and two breaches involving employee misconduct.

2018

HealthEquity Email Hack Breaches Data of 190K Patients

This is the second breach reported by the health savings trustee this year. In June, an unauthorized user breached the data of 16,000 individuals.

2019 Healthcare Cyber-Physical System

SECURITY

FDA Warns of Insulin Pump Cybersecurity Vulnerabilities

The Food and Drug Administration's recommendations comes after several external cybersecurity experts found dangerous vulnerabilities in the technical design of some Medtronic insulin pumps.

BY KATE PATRICK, INSIDEHOUSTON.COM - JULY 2, 2019

It's not just about EHR!

HEALTH CARE'S HUGE CYBERSECURITY PROBLEM

Cyberattacks aren't just going after your data

By Nicole Wetsman | Apr 4, 2019, 9:30am EDT
Illustration by Alex Castro / The Verge

SHARE

The patient lying on the emergency room table in front of Paul Pugsley was having a stroke. Time was running out. Pugsley, an emergency medicine resident at Maricopa Medical Center, knew he needed to send the patient for a CT scan.

But when Pugsley looked over at the computer screen at the side of the room, he saw a pop-up message demanding bitcoin payment. A few minutes later, he was told that the same message had shut down the scanner — he'd have to help the patient without knowing whether the stroke was caused by a bleed or a clot, information that's usually vital to the course of treatment.

Why is Cyber Security Important?

- On the black market
  - Social Security # - 10 cents
  - Credit Card # - 25 cents
  - Electronic Medical Health Record - $1000
- Electronic Health Records contains
  - demographic information - names, historical information of where you live,
  - where you worked,
  - the names and ages of your relatives,
  - financial information like credit cards and bank numbers
  - past medical history, including every doctor's visit made and diagnosis
- The medical record is the most comprehensive record about the identity of a person that exists today
- EHR data is immutable, hackers can potentially blackmail patients for a lifetime
- Sensitive protected health information (PHI) such as cancer diagnoses, sexually transmitted diseases, or psychological conditions, you could be subject to public embarrassment

State of affairs

- In 2016, 450 breaches occurred, affecting 27 million patient records
- A 2017 study by Filkins et al showed that 94% of health care institutions have been victims of cyberattacks.
- 72% were directed against hospitals, clinics, large group practices and individual providers
- In 2016, cyber attack on a large metropolitan hospital network with 10 hospitals were reported.
  - All radiation oncology patient appointments were cancelled for 3 days
  - Numerous hours spent by the clinical physicist and dosimetry staff to QA the data before patient treatments resumed on the 5th day.

Thus, it is necessary to protect healthcare records and systems from cyber attacks and cyber-physical attacks.

Cyber Security – Introduction

- What is Cyber Security?
  - *"Cyber Security, also referred to as information technology security, focuses on protecting computers, networks, programs and data from unintended or unauthorized access, change or destruction."*
  - With the growing volume and sophistication of cyber-attacks, ongoing attention is required to protect sensitive business, customer and other information.
  - In Radiation Oncology in very IT intensive and we collect, processes and stores a great deal of confidential information on computers and transmits that data across our network to other computers.

Cyber crime – Common Threats

Malware

Data Leakage

Email

Cyber Crime - Common Threats

- Malware
  - Malicious software
  - Computer Virus
  - Worms
  - Trojan Horses
  - Spyware
  - Dishonest adware
  - Crime ware
  - Pop-ups with fake anti-virus software

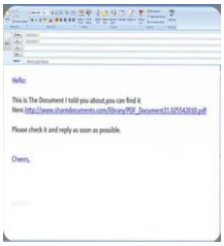
Cyber Crime - Common Threats

- Malware
  - Untrusted wireless access points (hotels, coffee shops, etc.)
  - Botnets
  - Keylogging

Cyber Crime - Common Threats

- Data Leakage
  - Unintentional release of secure information to an untrusted environment
  - Use of unencrypted data storing devices such as thumb drives, hard drives etc.
  - Loss of data storing devices

Cyber Crime - Common Threats



- Email
  - Sharing patient health data (images, RT records, case history etc.) via unencrypted email messages
  - Malicious email attachments
  - Embedded malicious links
  - Spam email
  - Clicking link within email, especially from unknown senders
  - Opening attachments from unknown senders

Current state of medical device industry

- Vendors Naïve about the risks and security of their products
- 80% of medical device companies have less than 50 employees
- Lacking general technology resources, processes and security knowledge
- Primary research and development and testing is focused on producing patient care functionality.
- Security is an after thought (often not considered)
- Currently no competitive advantage to being more secure than the competition.

Possible vulnerabilities in your clinic

- Does the medical devices use default user names and passwords? (These can be easily found on the internet) Can they be changed?
- Who maintains/updates antivirus and antimalware protections?
- Can the vendor gain remote access? How secure is that process?
- Are there unsecured USB/CD/DVD ports?
- Are the medical devices connected to the open internet?

Vulnerabilities on devices include hard-coded passwords and no encryption of patient data.

A recent study determined that many facilities fail to change the generic usernames and passwords that are supplied with equipment software.

The study found that among the most common passwords were "operator," "scan", "SysAdmin" and "service."

Cyber Security – Prevention

Proactive steps for prevention

Simple & Effective Things You can do

- Use of strong passwords, >12 with #s and special characters that are changed on a regular basis
- Log on as a user and not as an administrator
- Use multiple passwords, keep personal and professional passwords different
- Keep your operating system and applications updated
- Always use clean media
- Use encrypted thumb drives for data communication
- Limit the use of internet on medical device computers (discourage the use of personal email, social media and free to use file transfer websites)

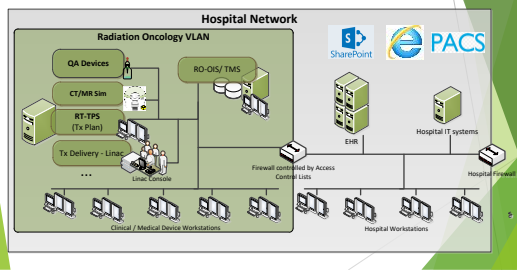
Simple & Effective Things You can do for your clinical environment

- Unique and individual login for all users
- Disable / modify generic vendor provided user accounts
- Password protected screen savers, with timeouts of 5-10 minutes.
- Do not run foreign and unknown applications on local workstations
- Regularly update anti-virus software and security patches for safeguarding workstations
- On the technical side, firewalls, virtual private networks and encryption are essential tools.
- Physical measures include device isolation, access restriction and methods to back up data.

Simple & Effective Things You can do for your clinical environment

- Two factor authentication process, encrypted USB drives and biometric identification for access to medical computer systems.
- Encourage vendors to integrate their login system to the hospital / enterprise based active directory system for enabling single sign on.
- Ability to use whitelisting (creating a list of the entities that are allowed to access a device or network);
- Medical Devices should not be directly accessible to the Internet
- Many IT systems do not allow non-registered computers to be connected (hard wired) to hospital networks. Computers may be tied to a single jack. This may prevent roving systems such as QA devices to be used at multiple treatment rooms.
- Work with the information security office to identify computers who should be excluded from the above.

Radiation Oncology Department Network



Simple & Effective Things that Vendor systems should do

- Use safe operating system
- The ability to upgrade operating systems
- The ability to upgrade third-party/open source applications
- Encryption of data communications between vendor devices
- Use industry standards such as NIST's FIPS-140-2 for device data encryption
- Use Site to site VPN for vendor support
- No hard-coded or default passwords and
- Ensuring a device meets account use best practices — meaning it has no non-expiring passwords, no regular accounts with elevated administrator privileges and so on.

Thank you for your attention