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 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

Hackers Are Homing In on Hospitals

Cybercriminals are increasingly targeting the computer networks of hospitals - one would assume that they’d look for hospitals that store patient information, but a recent NBC News article revealed that the cybercriminals are going after hospitals that have networks of medical devices. One such hospital was discovered to have been hit by a cyber attack that stole patient information.

2016

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

Anthem’s Medicare insurance coordination services vendor,找到了数据, revealed that an employee was stealing and misusing Medicare member data from as early as July 2014.

2017

PA Security Breach from Missing External Hard Drive Affects 4.1K

Researchers from the Pennsylvania Department of Health announced that a missing external hard drive containing sensitive information on 4,100 patients was discovered. The missing hard drive contained patient demographic data and medical records.

2018

NHS cyber attack: Everything you need to know about the biggest healthcare cyber attack

The cyber attack on the NHS was one of the largest ever, affecting 1.9 million patients. It was caused by a malware that targeted the hospital’s computer systems.

2019

IBM Security report finds rising trend in healthcare cyber attacks

IBM’s latest report found that healthcare cyber attacks are on the rise, with a 20% increase in the past year. The report also highlights the need for stronger cybersecurity measures in the healthcare sector.
2017

**PA Security Breach from Missing External Hard Drive Affects 4,179**

Recent potential healthcare security breaches include a missing external hard drive, improper disposal, and a cyber security 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 4,179**

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

---

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 15,000 individuals.

---

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 15,000 individuals.
It’s not just about EHR!

**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 contain demographic information - names, historical information of where you live,
  - where you worked,
  - the names and ages of your relatives,
  - financial information like credit card and bank numbers
  - past medical history, including every doctor’s visit, made and diagnoses.

- The medical record is the most comprehensive record about the identity of a person that exists today.

- 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, cyberattack on a large metropolitan hospital network with 10 hospitals were reported.
  - 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

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

- 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, EHR 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 afterthought (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 anti-malware 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

- 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

- 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
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 moving 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