Cybersecurity Issues with Medical Imaging Equipment

Presented By
Gregory Goll BS CHTM CBET
Wellstar Health System
Marietta, GA

ICE2025
IMAGING CONFERENCE & EXPO
FEBRUARY 22-24, 2025 • ORLANDO, FL

How many people speak GEEK?

One of the first issues is making sure all departments and vendors are communicating correctly.

The easiest way technical staff confuse clinical staff is assuming they understand common IT terminology.

Take time to know your audience.

Basic Terminology

Operating System- Windows

Application software- Pacs

Network- Wireless verses Hardwired

Cybersecurity

Cybersecurity refers to every aspect of protecting a organization and its employees and devices against cyber threats.

As devices and networks become more complex the threats become more common and more difficult to remediate.

Different types of Cyber Threats

Network Security- most attacks occur over the network
Cloud Security- more organizations are using cloud computing
End Point Security- zero trust security, create segments around data
Mobile Security- addresses issues with devices such as tablets and smartphone
Application Security- anything directly connected to internet

Evolution of threats

Virus (Gen1)- attacks against stand alone computers
Network (Gen 2) – attacks over the internet, resulting in the development of the firewall
Applications (Gen 3)- vulnerabilities within an application, intrusion prevention systems
Payload (Gen 4)- malware, anti-bot
Mega (Gen 5)- large scale, multi-vector

Ransomware

Ransomware was first used to encrypt files.

Evolution into stealing data, used to extort the victim and customers.

Distributed Denial of Service (DDoS) attacks to incentivize victims to meet ransom demands.

Phishing

Phishing attacks have long been the most common and effective means by which cybercriminals gain access to corporate environments.

Email delivery of a message that resembles a real communication.

It is often much easier to trick a user into clicking a link or opening an attachment than it is to identify and exploit a vulnerability within an organization’s defenses.

Where to begin

Understanding of the connected device environment.

Identify the networking needs.

Find out what is on the network and ownership

Risk Assessment

Identify device vulnerabilities and network related risks.

What is the operating system?

Risk example: Microsoft will stop supporting Windows 10 on October 14, 2025.

Risk Assessment

Identify device vulnerabilities and network related risks.

What is the operating system?

Risk example: Microsoft will stop supporting Windows 10 on October 14, 2025.

Protection Connected Devices

Segregated networks isolating device helps minimize threats
Any different data transmission behavior can be identified and quickly addressed

Real World Issues

Passwords
HIPPA Information protection
User access
Unattended devices
Encryption
Software management

IT Cyber Security Roles

Insure regulatory compliance
Check security documentation
Change Management Policy
Data Backup Policy
Remote Access Policy
Incident Response Policy

Operating System

Documentation of operating system
Documentation of all installed vendor software

Windows 10 End of Life October 14th 2025

Recalls will address a specific software revision

3rd Party Software

Off The Shelf software

Application specific software, OBIX, EPIC MACLab

Basically any software required to obtain complete functionality of the system.

Recall Concerns and Remediation

Make sure of the level of criticality of the recall.

Who issued the recall: FDA, Vendor, ECRI

What documents were provided?

Software Backup Access

W ho has the operating systems software?

In the event of End of Life, determine a Plan B

Any onsite software is secure and labeled.

Patch Management

IT and vendors both will need to apply patches eventually.

Antivirus patches can create major issues

Document all changes

Patch Management

IT and vendors both will need to apply patches eventually.

Antivirus patches can create major issues

Document all changes

Access Management

User access
Password control
Internet/Network access
- Vendor
- End User

Documentation of Network Addresses

MAC Address
IP Address
Wireless Address
Port location

Documentation of Network Addresses

MAC Address
IP Address
Wireless Address
Port location

Network Monitoring

What tools does IT have for monitoring data on the Network

In the event of a data concern how is notification done?

Is there a universal system all parties can use for documentation and resolution.

Philips and Wellstar

Use of Philips Service connect for documentation

Remote access into major systems to diagnose and troubleshoot problems.

Access to recall documents

Thanks for attending

Any Questions