Cybersecurity: The Next Steps for the Medical Imaging Industry

Patrick Hope
DITTA Chair and Executive Director,
Medical Imaging & Technology Alliance (MITA)

Wednesday, November 29, 2017
RSNA
INTRODUCTION

• **DITTA, the global voice of the medical imaging, radiation therapy, and health IT industry**

• **MITA, the leading organization and collective voice of medical imaging equipment, radiopharmaceutical manufacturers, innovators and product developers in the United States**
Cybersecurity

- Cybersecurity is a high priority for manufacturers of all internet-connected devices
- DITTA/MITA is leading efforts to strengthen cybersecurity for imaging systems
Goal #1 - This presentation will provide a industry’s domestic and global perspective on cybersecurity and what industry should be doing internationally to prepare

Goal #2 – Understand that our belief is the best way to protect patient safety & privacy is through a regulatory and standards environment that best enables the protection of the confidentiality, integrity, and availability of medical imaging devices
Cybersecurity Principles

- ***Cybersecurity is a shared-responsibility between all stakeholders, incl. manufacturers, healthcare providers, patients, and others***
- Manufacturers should not be held responsible or accountable for other parties’ negligence.
- ***The role of global standards needs to be recognized. Global standards should be relied upon instead of new regulation. Standards are the backbone of industry self-regulation and are often updated more frequently than regulation, allowing for adaptability to a changing landscape***
- Avoid reference to specific cybersecurity risk-mitigation tactics. Cyber threats are constantly evolving as are risk-mitigation tactics. What is relevant or best practice now, might be irrelevant even in a few years
Cybersecurity Principles

- Recognize that technology alone cannot provide security. **Organizational measures** must also be in place to ensure good cyber hygiene.

- Recognize medical device’s do not last forever. The physical life of a device & the cybersecure life of a device might be very different. Develop policies to incentivize the transition of **legacy products**.

- **Information sharing** policies should have clearly established legal guardrails & incentives for participation. Information sharing requirements, if implemented, should also extend to owners/users of medical devices.
Cybersecurity

Merck hit by new global ransomware attack

By Rachael Z. Arndt, Jun 27, 2017
(Updated on June 28)

It's happening again.

A new variety of ransomware is wreaking havoc around the world, and Merck & Co. is one of the first U.S. companies to report being hit. This strain of ransomware, which Kaspersky Lab has dubbed NetPonya, follows the WannaCry ransomware attacks in May that took down thousands of computers worldwide.

The drugmaker wrote on Twitter that its computer network was “compromised today as part of global hack.”

Two other U.S. organizations, Heritage Health System and Nuance Communications, also may have been affected. The former, a Beaver Dam, Wis.-based health system, wrote on its Facebook page that it was operating “as normal,” while Nuance stated that its facilities were being restored.

CIO: HHS faces 500 million hack attempts per week

By Chase Gunter, Jun 20, 2017

By virtue of possessing millions of medical records, the Department of Health and Human Services is a prime and frequent target for attempted cybersecurity intrusions.

According to HHS CIO Beth Killian’s estimation, the department faces “500 million cyber hack attempts each week” and cautioned that already staggering number is only going to swell in the future.

“Things are going to get worse,” said Killian.

WannaCry timeline: How it happened and the industry response to ransomware attack

By Shannon Muchmore, Jun 26, 2017

May 19, 2017 | 12:02 PM

Anthem to pay record $115M to settle data breach lawsuit

Anthem will pay a record $115 million to settle a class-action lawsuit stemming from a 2015 data breach in which the personal information of nearly 80 million members and employees was stolen.

The company agreed to set aside funding for cybersecurity improvements as well as cover two years of credit protection and $15 million worth of out-of-pocket costs for those affected.

In a statement, the payer did not admit to any wrongdoing or any harm to people as a result of the cyberattack, but said it is “determined to do its part to prevent future attacks.”

Fears of hackers targeting US hospitals, medical devices for cyber attacks

By Dan Harris, John Kapetanias, Robert Zepeda and Lauren Effron
Jun 24, 2017 11:15 PM ET
Before:

• Information was shared person-to-person

Today:

• Information is shared online

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

• Internet access everywhere, on everything!
Why does it matter?

• Healthcare data is very valuable
• In 2015, Rising Cyber Attacks Cost U.S. Health System $6 Billion
• Cyberattacks compromised 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!**
Why is DITTA/MITA focused on cybersecurity?

- ***Patient Safety***
- Imaging department has increased risk profile compared to rest of hospital
- New paradigms create new concerns:
  - Medical imaging systems interconnected with each other
  - Danger of attacks not only in disclosure of e-Personal Health Info (ePHI), but in compromised patient safety and access to care
- Prevention requires specialized cybersecurity awareness and training for personnel but also manufacturing products that can be updated
Cybersecurity in Medical Imaging

  - 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
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
Four Components of medical imaging cyber security:

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.

4. **The Responsible User** - Effective training and education of staff is essential!
Towards a cyber-secure future

Summary

- MITA/DITTA is leading the way for medical imaging industry to help create a cybersecure environment
- Cybersecurity is a shared-responsibility between all stakeholders: government, industry, health care providers
- International community must come together to share information, strategies, and develop/adopt standards
Thank you!

Patrick Hope
phope@medicalimaging.org
@MITAonline