Introduction

The Insider Threat - A Brief Overview
Why Insider Threat Matters

- Cybersecurity is more than just making sure your antivirus definitions are up-to-date and looking to see what or who is trying to infiltrate into your organization.

- If you are looking for activity only on the outside, you only are addressing part of the equation.
  - The other side of the equation is what is happening on the inside of your organization, whether it is consultants, employees, interns, or others who may be snooping, committing fraud, or intentionally damaging or destroying data.
  - What are these “insiders” doing in terms of their behavior?
  - What information is being exfiltrated out of your organization (or is otherwise being improperly viewed or used)?
  - Is your cybersecurity posture reactive or is it proactive?
Who are the Insiders? What are they Doing?

• Insiders may be your employees, interns, volunteers, consultants, or anyone else with access to your organization’s information (e.g., janitors and security guards).

• Examples of activities:
  – An unlocked workstation, laptop, or mobile device may be accessed (e.g., an unlocked smartphone being charged and left out in the open).
  – Papers left on a desk or in an unlocked file cabinet may be taken.
  – A thumb drive left on a desk or in a computer may be taken.
  – A snapshot may be taken of a computer screen or paper.
  – Electronic eavesdropping and keylogging to obtain information.
  – Audio recording of information.
Insider Threat Detection

- Without appropriate procedures and processes in place to detect suspicious activity (the insider threat), your organization will most likely be unaware of insider threat unless it subsequently discovers the damage, destruction, loss, unauthorized disclosure, or misuse of sensitive, proprietary, and/or individually identifiable information.

- It is generally not possible or feasible to manually review access and system logs to assess whether there is a problem.

- You need intelligent tools to uncover retrospective and real-time activity across your systems (including EHR, PACS, scheduling, billing, etc.).

- You also need a good baseline to reliably detect insider threat at an appropriate confidence level.
  - Are the audit logs reliable?
  - Should you have tools to listen to your network traffic to help detect suspicious patterns of activity?
Responding to Insider Threat Reactively (Not Recommended)

• Consequences of not proactively addressing insider threat include the following (a non-exhaustive list):
  – Your organization may find that an insider threat has been acted upon after the person who is the subject of the information (the victim) has filed a complaint about it.
  – Your organization may find that a competitor has received sensitive/proprietary information about your organization through leaked information from someone with “insider” access.
  – Your organization may find that an insider threat has been acted upon only after a person has become a victim of medical identity theft or fraud.
  – Your organization may not realize that such activity has occurred until after its data have been damaged or destroyed by a malicious insider.
Responding to Insider Threat Proactively (Recommended)

- Prevent or protect your organization from the insider threat before a serious problem occurs.
- Detect potential incidents real-time and stop the suspicious activity, thereby preventing actual harm (e.g., theft, fraud, damage, destruction, leakage, unauthorized disclosure/”sharing”, misappropriation, etc.).
- Understand the insider threat motivators (e.g., curiosity, fame, financial gain, disgruntled workforce member, etc.) to help prevent such occurrences (including carefully selecting and vetting your employees and other “insiders”).
- Take into account not only your electronic assets (your data), but also information in other forms (e.g., paper, film, etc.) and examine your technical, physical, and administrative safeguards to safeguard the confidentiality, integrity, and availability of information.
Questions?

Lee Kim, BS, JD
Director, Privacy & Security
HIMSS
4300 Wilson Blvd., Suite 250
Arlington, VA 22203
(703)562-8806 (office phone)

lkim@himss.org