Is My Organization Ready for a cybersecurity threat?
Assessment and setting up plans

INHEL REKIK MS, DIRECTOR OF HEALTH TECHNOLOGY SECURITY,

MEDSTAR HEATH

JON MCKEEBY D.SC MBA CPHIMS CPHI, CHIEF INFORMATION OFFICER,

NIHCLINICAL CENTER

Background

- Director of Health Technology Security at MedStar Health
- Oversees the security program for medical devices and IoT
- Clinical engineer with over 10 years of HTM experience and most recent role being the CE manager at MedStar Georgetown University Hospital
- Bachelor’s degree in Computer Engineering from Laval University and Master’s degree in Biomedical Engineering from Polytechnic School of Montreal
- Active member of AAMI Healthcare Technology Leadership committee, AAMI Next Generation Task Force and author of Tech Tips column in TechNation magazine

Background

- Chief Information Office, NIH Clinical Center
- Oversees EHR with 5,000 users
- Oversees Clinical Center IT with over 2,200 Employees, Contractors and Volunteers
- Doctorate in Computer Science from George Washington University
- Member HIMSS, AHIMA, CHIME

News Items

- About 47% of US had personal healthcare data compromised in 2015.[1]
- September 2017,Equifax reported breach of 143 million consumers. A virus-like software exploited a vulnerable Apache server. *Patch was available in March*. Vulnerability discovered months after exploit. *Cybercrime, Cybernuisance* [2]
- May 2017, WannaCry ransomware malware attack infected over 75,000 computers in 99 countries demanding ransom payments. Vulnerable MS OS computers. *Cybercrime, Cybernuisance* [3]
- March 2016, MedStar affected by virus/ransomware causing computer systems across 10 hospitals and 250 outpatient centers for up to a *week* forcing the use of paper based processes. A virus-like software was used to scan the Internet for vulnerable JBoss servers. *Cybercrime, Cybernuisance* [4]
- March 2014 to May 2014 , the United States Office of Personnel Management (OPM) was breached with over 21 million people affected. Besides data they also retrieved about 6 million fingerprints. *Breach was discovered 2015. DoD cost was* $132 million to protect credit of people affected that were part of DoD. Vulnerable legacy systems. *Cyberespionage, Cyberwarfare* [1]

1. Institute of Critical Infrastructure Technology. (2016). Hacking Healthcare IT in 2016: Lessons the Healthcare Industry can learn from the OPM breach.
2. Newman, L. (2017). Equifax officially has no excuse. Wired. https://www.wired.com/story/equifax-breach-no-excuse/
3. CISCO. (2018). Cisco 2018 Annual Cybersecurity Report | The attack landscape.
4. Blake, A. (2016). MedStar hackers exploited 9-year-old flaw to hold hospital data for ransom. The Washington Times.

Cybersecurity Risk Strategy

Rich Baich, Wells Fargo Chief Information Security Officer

Risk = Vulnerabilities X Threat X Asset Value

Modified (McKeeby & Inhel, 2018)

Risk = Vulnerabilities X Opportunity/Attack Surface X Threat X Asset Value

Hiner, J. (2017). The 4 types of cybersecurity threats and a formula to fight them. https://www.techrepublic.com/article/the-4-types-of-cybersecurity-threats-and-a-formula-to-fight-them

Risk = Vulnerabilities X Opportunity X Threat X Asset Value

Asset Value

- Highly Sensitive Information
- Proprietary/Competitive Edge Information
- Protected Health Information (PHI)
- Personally Identifiable Information (PII)
- Financial Information

Risk = Vulnerabilities X Opportunity/Attack Surface X Threat X Asset Value

Threat

Threat Types

- Cybercrime – Financially motivated. Get money off of transactions, selling data, identity theft. Banks, retail, people.
- Cyberespionage – Information motivated. Steal trade secrets as well as proprietary and sensitive information have to worry about the most. So, pharmaceutical companies and government agencies like the NSA are the most at risk.
- Cybernuisance – Statement motivated. Hacktivist, deface web sites, identify companies or organizations are not prepared.
- Cyberwarfare – Nations attacking private and public organizations entities for national interests.

Hiner, J. (2017). The 4 types of cybersecurity threats and a formula to fight them. https://www.techrepublic.com/article/the-4-types-of-cybersecurity-threats-and-a-formula-to-fight-them/

Risk = Vulnerabilities X Opportunity/Attack Surface X Threat X Asset Value

Threat

- People
  - Internal
    - Not following security aspects
    - Specific Attack
  - External
    - Based on Threat Type
- Mechanism
  - Web Browser
  - Email Phishing
  - Scan Devices and Exploit Vulnerabilities
    - 2015, Java was second biggest security vulnerability (Zaharai, 2015).
    - 2015, Adobe's Flash plugin was first (Zaharai, 2015).

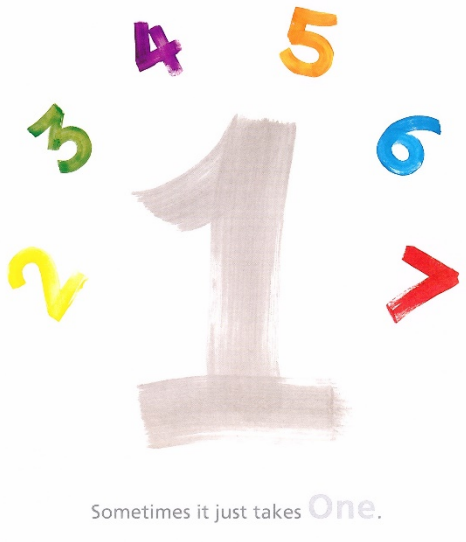
Zaharai, Andra. (2015). Why Java Vulnerabilities Are One of Your Biggest Security Problems. https://heimdalsecurity.com/blog/java-biggest-security-hole-your-computer/#

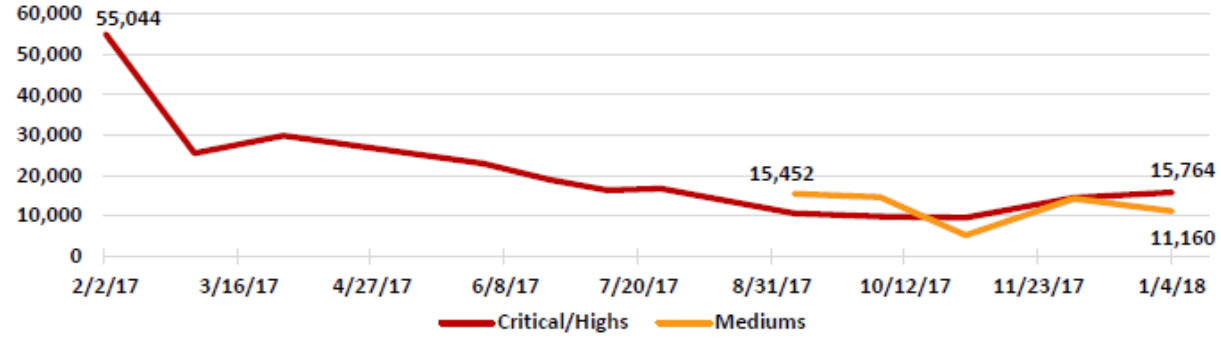
CISCO. (2018). Cisco 2018 Annual Cybersecurity Report | The attack landscape.

Risk = Vulnerabilities X Opportunity/Attack Surface X Threat X Asset Value

Opportunity/Attack Surface

- **High Number of System (Many not designed with security in mind)**
  - Legacy, Niche Systems
  - Internet of Things (IoT)
- **Variations of Systems**
  - Many Different Vendors
  - Many Different Operating Systems, Hardware, Software
- **Restrictions by Vendors**
  - Operating System
  - Patch Level
  - Anti-virus, Security Agents, other software on devices
- **Access**
  - Number of Users, Types of Users
  - Locations
  - Wired/Wireless

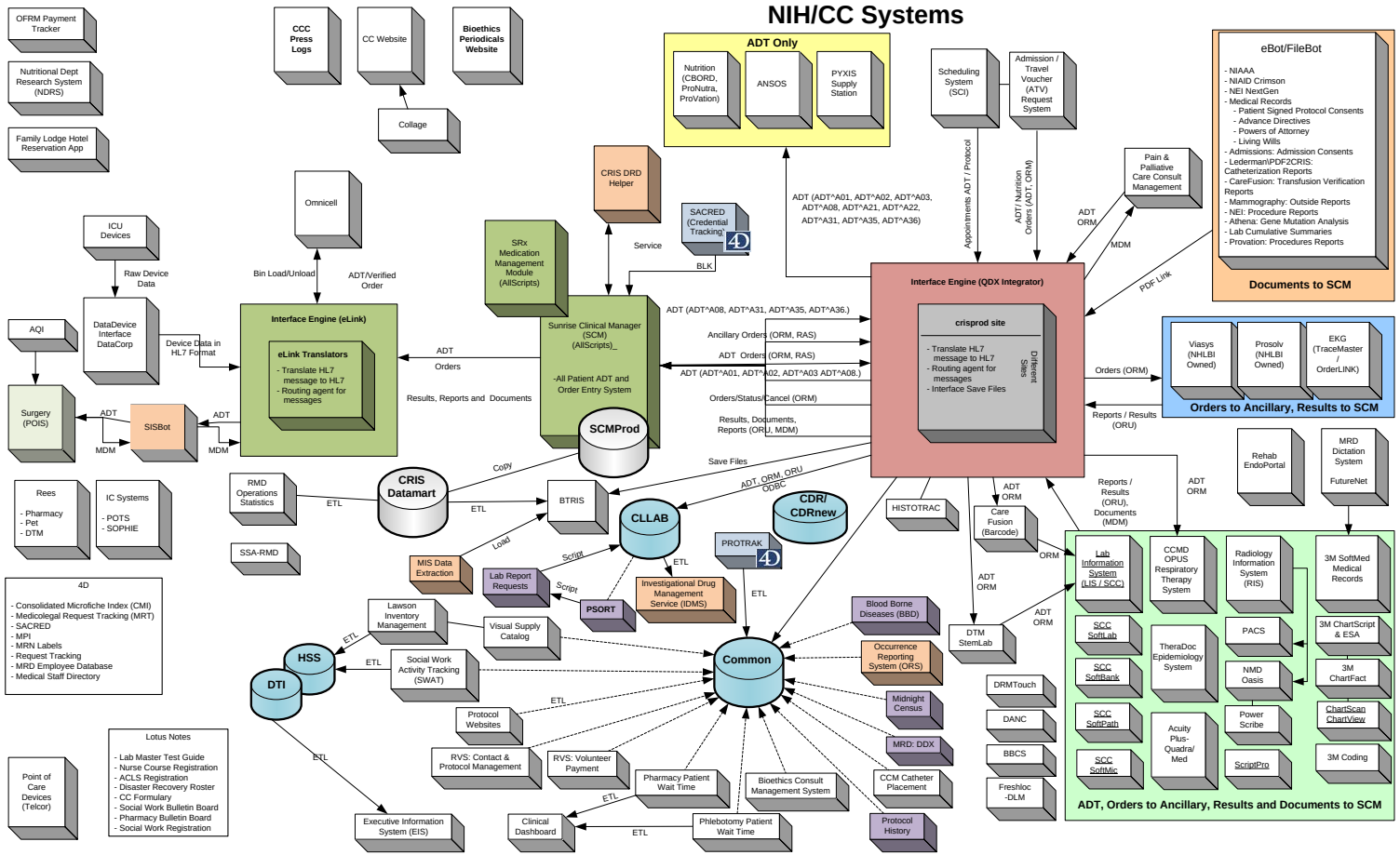


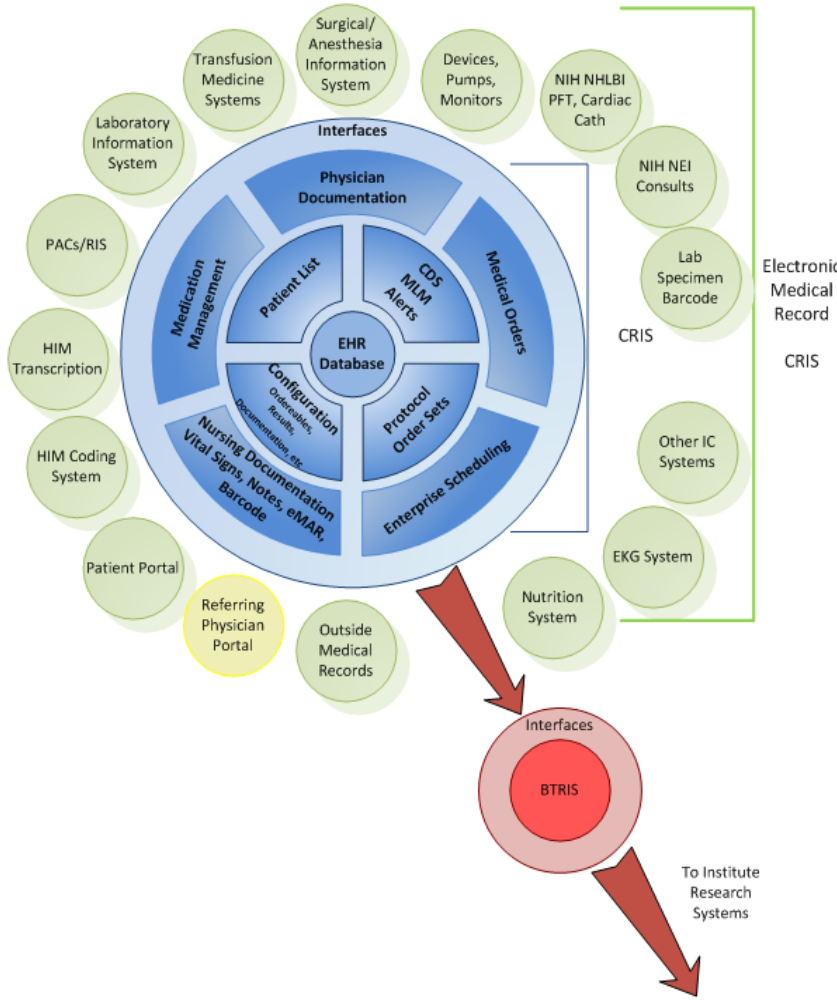


Risk = Vulnerabilities X Opportunity/Attack Surface X Threat X Asset Value

Opportunity/Attack Surface

A Typical Healthcare Architecture Set of Drawings





Risk = Vulnerabilities X Opportunity/Attack Surface X Threat X Asset Value

Opportunity/Attack Surface

A Typical Healthcare Environment

EHR Production

- 33 Servers
- 7 physical SQL servers
- 22 virtual servers
- 69 TB Storage
- Access: 447 WOWs, 632 Thin Clients, CITRIX
- 42 XenApp VMs that actually run the CRIS application
- 18 Servers to Support CITRIX Infrastructure

Data Center

Data Center Specifics	
Servers	801
Relational Database Systems	6
Disk Storage	932 TB

User Devices

	Thin Clients	Desktops	Laptops	WOWs	Barcode	Printers	Total	Smart-Phone
2014	274	4,434	965	325	326	2,226	8,550	633
2015	296	4,140	1,160	435	326	2,145	8,502	699
2016	246	4,357	1,276	412	326	1,628	8,245	693
2017	414	3,734	1,253	447	326	1,504	7,678	777
2018	632	3,766	1,451	447	326	1,523	8,145	814

Years	Desktops	Laptops
< 3	2,389	432
3	499	194
4	247	58
5	616	127
6	192	68
7	98	70
> 7	254	109

Risk = Vulnerabilities X Opportunity/Attack Surface X Threat X Asset Value

Opportunity/Attack Surface

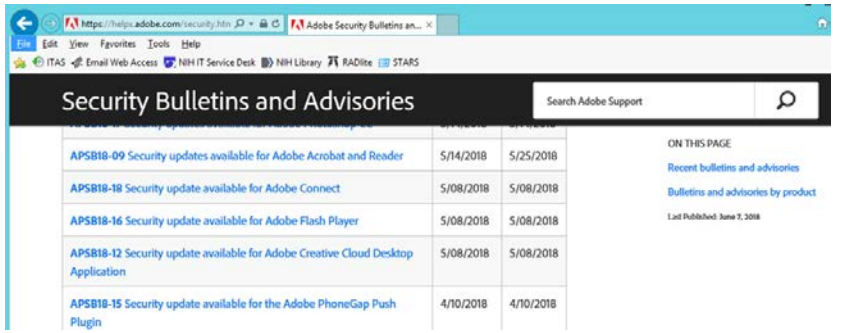
- Healthcare Security Posture
  - Low Level Maturity in Security Management
  - Limited Best Practices
    - Patch Management
    - Log Management
    - Data Loss Prevention
  - Limited Security Documentation Per System
  - Limited Security Staff

Risk = Vulnerabilities X Opportunity/Attack Surface X Threat X Asset Value

Vulnerabilities

- Exploit Vulnerabilities
  - 2015, Java was second biggest security vulnerability (Zaharai, 2015).
  - 2015, Adobe's Flash plugin was first (Zaharai, 2015).

Top 5 Critical Vulnerabilities (30 Day)		Top 5 High Vulnerabilities (30 Day)	
Oracle Java SE Multiple Vulnerabilities	430	Oracle Java SE Multiple Vulnerabilities	1,050
7-Zip <18.05 Memory Corruption Arbitrary Code Execution (ID: 109730)	51	KB4103731: Windows 10 Version 1703 May 2018 Security Update (ID: 109611)	346
Adobe Flash Player <= 29.0.0.113) (Plugin ID: 108958)	33	Security Updates for MS .NET Framework (May 2018) (ID: 109652)	187
Intel Management Engine Insecure Read/Write Operations (ID: 97997)	17	MS15-116: Security Update for MS Office to Address Remote Code (ID: 86823)	89
Mac & MacOS X Multiple Vulnerabilities (Security Update 2018-002) (ID: 108787)	15	MS KB2269637: Insecure Library Allow Remote Code Execution (ID: 48762)	88



Zaharai, Andra. (2015). Why Java Vulnerabilities Are One of Your Biggest Security Problems. https://heimdalsecurity.com/blog/java-biggest-security-hole-your-computer/#

CISCO. (2018). Cisco 2018 Annual Cybersecurity Report | The attack landscape.

Security Plan Components

- **Define Environment**
  - Define assets (Data/Systems)
  - Prioritize items to secure
  - Document environment
- **Develop Infrastructure to Protect Assets**
  - Firewalls/DMZ
  - Server hardening
- **Develop Policies/Processes**
  - Remote access policy
  - System use policy for each system
  - System hardening process
  - Vulnerability resolution process
  - Breach/Malware resolution process
- **Ensure Best Practices**
  - Patch management
  - Centralized logging
  - Vulnerability scanning
  - Data loss prevention program
- **Security Awareness Training**
  - Train developers on specific environments
  - Train system administrators, database administrators, network, user support on specific systems
  - Train users
- **Continuous Improvement**
  - Review vulnerability trends
  - Review new tools
  - Review existing processes semi-annually
  - Independent vulnerability testing

Incident response guidelines

Incident response capability should include the following:

- Creating a formal incident response policy and plan
- Developing procedures for performing incident handling and response
- Setting guidelines for communicating with outside parties regarding incident
- Selecting a team structure and staffing model
- Establishing relationship and lines of communication between incident response team and other groups, both internal (legal) and external (law enforcement agencies)

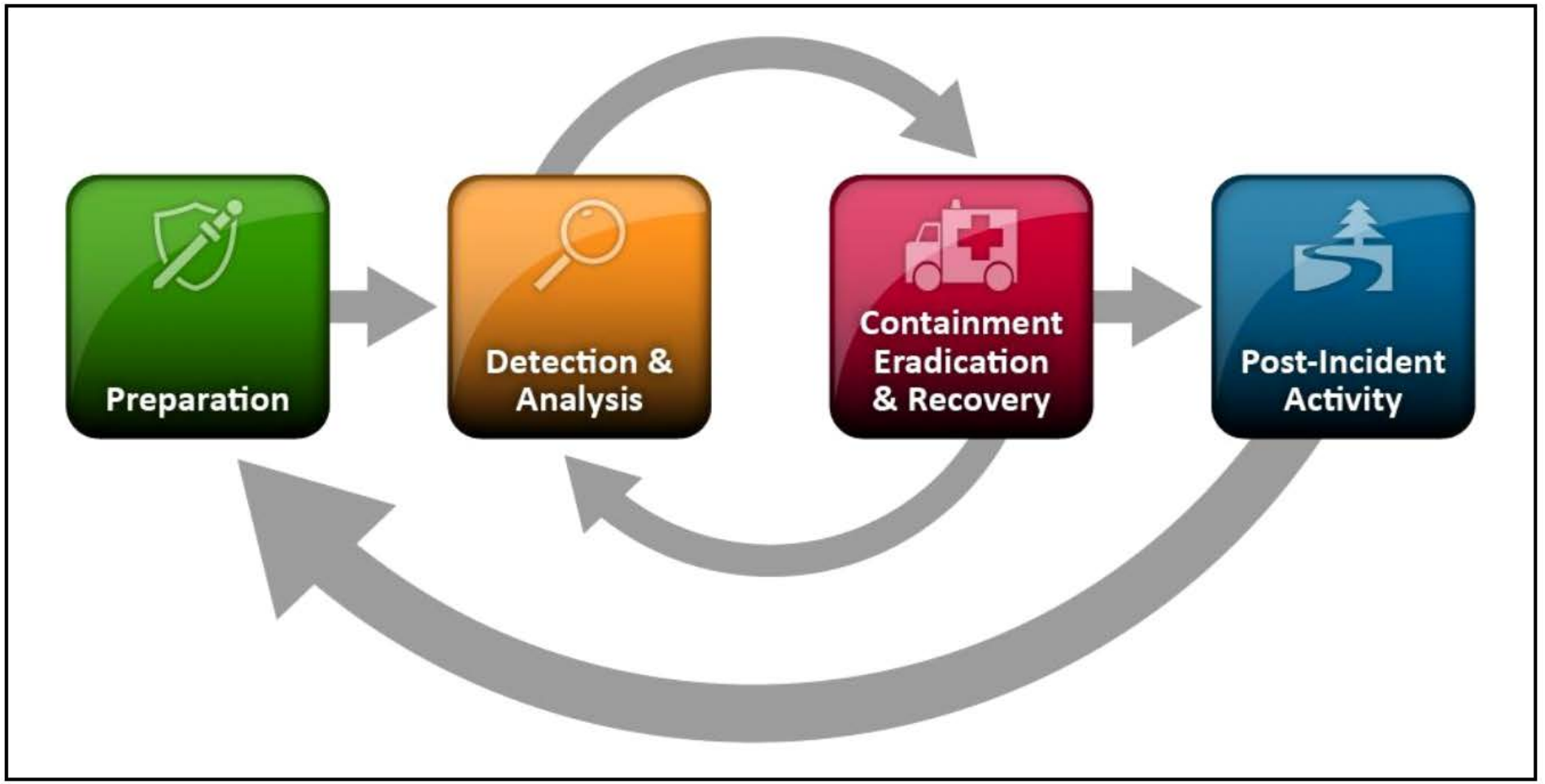
Organizations must create, provision, and operate a formal incident response capability. Federal law requires Federal agencies to report incidents to the United States Computer Emergency Readiness Team (US-CERT) office within the Department of Homeland Security (DHS).

Computer Security Incident Handling Guide by NIST

Types of incident response

- Fully in house.
- Partially outsourced: Some organizations perform basic incident response work in-house and call contractors to assist with handling incidents, particularly those that are more serious or widespread.
- Fully outsourced: The organization completely outsources its incident response work, typically to an onsite contractor.

Incident response steps



Computer Security Incident Handling Guide by NIST

Security Incident Plan

- We Run as a Project
  - Team Roles Defined
  - Checklist
  - PM Runs first few times then hand over to Security Team/Tech Team
- Steps
  - Identify Security Incident
  - Direct the Emergency Management Communication Center
  - Give overall Direction to Hospital Operations
  - Initiate Security Incident Team Resolution
  - Isolating and Identification Tasks
  - Data Recovery
  - Forensics/Investigational Tasks
  - Remediation
  - Lessons Learned

Security Incident Plan: Roles and Responsibilities

Resource/Team	Role & Responsibility
Exec Leadership	• Notifies Systems Monitoring team to initiate downtime communication processes • Primary DCRI decision maker based on input from entire team • Provides status updates to DCRI & CC Executive Leadership • Direct the Emergency Management Communication Center, give overall direction to hospital operations
Systems Monitoring	• Initiates notification to users through NIH page operators and email, contacts Opens conference phone line for technical team coordination and collaboration • Notifies identified resources (on-call, if off hours) • During off shifts and weekends • Notifies CCND AC to communicate down, address questions, may provide conference line number • Deliver flyers to patient care areas • Provide communication to user community (email & Phone) per downtime policy
Clinical Informatics	• Call 10 impacted clinical departments to communicate down, down strategy and address questions • Call patient care areas to communicate down and address questions • Make rounds throughout the CRC during downtime, per downtime policy • Deliver flyers to patient care units • Call patient care units, clinics, day hospitals & 10 identified clinical departments when back up

Security Incident Plan: Roles and Responsibilities

Resource/Team	Role & Responsibility
System Application Admin (i.e. DBA, Developer, Dept. Appl. Admin)	• If CRIS, Clinical DBA communicates expected availability of Sundown to members of conference line • Complete the Data recovery tasks for impacted system
System Admins	• Isolate user's account • Assist to identify impacted systems • Work with system owners, as needed • Complete data recovery
Security Team	• Facilitate the malware incident • Complete the checklist and post in SharePoint • Work with user to identify actions that lead to Malware, remediation & education • Submit and update the required reporting to NIH (IRT tickets)
User Support	• Remove impacted workstation(s) from network • Reimage impacted the workstation(s) • Complete additional tasks as directed based on type/expanse of event
Privacy Team	• Evaluate if data was removed, accessed by malware/virus perpetrators • Submit and update the required breach reporting to NIH/HHS

Exercise

- Breakup into groups of five
- Review Vignette 1
- Identify Roles
  - IT Executive Management
  - Security Team
  - Compliance/Privacy Team
  - Legal
  - PR
  - System Admin
  - User Support
- Develop a Solution
- Review Solution to Group
- Repeat for Next Vignette

Helpful Hints

- How will you communicate to Hospital Leadership?
- When you will you activate the incident response team?
- Who are the stakeholders that need to be involved?
- How will you isolate the issue?
- When and how will you communicate with the rest of the organization and other organizations?
- How will you work with manufacturers such as as Pyxis Stations?

Vignette 1

At 9 am this morning, a bus exploded on the 95 which resulted in the injury of several people that are now rushed to your hospital adult ED.

Nurses and physicians are rushing everywhere to resuscitate and stabilize as many patients as they can.

At the same time, a nurse at the nurse station sees a message flashing across her screen “we got a hold of your data”. Few minutes later more messages appear. “ we got a hold of your data. We are legions!.”

30 min later a security guard appears in the ED saying that there has been an anonymous message flashing in few computers in the peds ED next door.

Work through this incident. For each role describe what you will do.

Vignette 2

It’s 3 pm and there is over 200 workstations infected with the trojan.

IS security has advised shutting down workstations to contain the infection.

Patient care continues but several network connected medical devices with Microsoft operating system across several clinical services are now inoperable. These medical devices include EP lab workstations, EEG units, Pixys medication cabinets as well as some imaging devices.

At 5 pm, several PHI from your hospital are being sold on the dark web. A visitor takes a picture of the flashing screen and post it online saying that your hospital is under attack. Confidence in your hospital’s ability to deliver care is under scrutiny by Health and Human Services.

The investigation of the incident response vendor showed that the malicious code was introduced into your network through an unpatched workstation. The trojan used a vulnerability that Microsoft issued a patch for last month.

IS Security indicated that patching the workstations and an updated antivirus signature won’t completely eliminate the infection. All infected workstations will need to be reimaged. IS Security is also concerned about the administrative accounts on these workstations.

Major disruption of providing patient care is still ongoing. The clinical leadership is clamoring for a response to solving impacts to delivering patient care.

Work through this incident. For each role describe what you will do.