Cyber Security Summing Up! Simulation Exercise and Future Direction

- Dr. Nahm
- Darren Lacey
- Susan Martin
- Michelle Lardner

Overview

- If major incident happens (malware, ransomware, virus) how does the organization respond?
- Who and what departments are involved? What are their specific roles?
- What should clinicians know to be prepared?
- HHS Office of Civil Rights (OCR) has a quick response checklist on their website to guide impacted hospitals and business associates https://www.hhs.gov/sites/default/files/cyber-attack-checklist-06-2017.pdf

IT Security Response

- Darren will cover mitigation procedures and contingency plan, try to preserve forensic evidence, report the crime to law enforcement, report cyber threat indicators to federal and information –sharing and analysis organizations (ISAOs), notification to organizational leadership
- Darren – do you believe this ransomware youtube video will be useful for non IT users? Not healthcare focused but gives overview
- https://www.youtube.com/watch?v=FV-HW3NYdF8

System Administrators Response

- **Turn off access to impacted systems during investigative phase**
- **Communicate event to CIO and provide regular updates**
- **Consult with security team to mitigate spread of malware to other**
- **When malware has been remediated, restore system from backups**
- **Test functionality and validate accuracy before allowing users access**
- **Follow established plans to accept transactional data for tests performed and resulted during the system's downtime to have a complete record for the patient**

Hospital Leadership Response

- Communicate alterations in business process to staff and patients, this might include following downtime processes for the electronic health record
- Each of the clinical departments with connections to the EHR should have contingency plans for operations and provision of services using manual downtime procedures
- Notify business associates as appropriate, including vendor support teams
- If system is down >24 hours, establish command center to obtain frequent updates and modify communications and business operations as needed
- Engage Communications and Marketing staff to handle communications with the public and media

Privacy Office Response

- The Privacy Office has an important role after the event has been mitigated and thoroughly investigated
- If investigation reveals the event was a breach affecting >500 patients, the Privacy Office must notify OCR as soon as possible but no later than 60 days
- They must notify affected individuals and media unless law enforcement requests a delay

NIH Malware Standard Operating Procedure

- **NIH has a Malware SOP and checklist that covers the steps for remediating Malware from first detection to final data restorations for major clinical systems.**
- **Developed during the very public cybersecurity events in 2014 which caused multi-day downs for local and national hospitals.**
- **Every situation can be different, so the order may vary as needed.**

Malware Checklist Phases

Phase 1 – Malware Suspected and Initial Response

- **Identify/ Suspected Issue**
- **Open Conference Line with system admins, clinical database administrators and IT leadership**
- **Decision to take system down for isolation/identification/recovery tasks**
- **Communicate with Organizational Leadership and communicate with clinical departments to initiate down time process**
- **If multiple systems impacted or expected to last >24 hours, set up command center for Exec Ldrship per Emergency Management Plan**

Malware Checklist Phases Continued

Phase 2 – Isolation and Identification

- **Shut down affected application and isolate from the hospital network**
- **Verify original source has been remediated before bringing application up**
- **Evaluate integrity of the data**
- **Review all findings with IT leadership and make decision for recovery actions**

Malware Checklist Phases Continued

Phase 3 – Recovery (as needed)

- **Follow application contingency plan and initiate backup restore procedures**
- **Bring up restored copy for validation of data**
- **Perform regression testing on restored copy**
- **Make decision to bring application up to users again**
- **Notify users that system is available**
- **Notify Clinical Depts to begin data recovery process**

Planning for your future

- Do you know if your hospital has a plan?
- Do you know if your servers and applications are locally hosted i.e., on premises or remotely hosted?
- Prepare for the Joint Commission to ask you about this
- ONC Safer Guides
- HIMSS EMRAM Stage 7
- NIST Cybersecurity Framework

SECURITY JEOPARDY

Definitions	Vector	Steps	Who you Gonna Call?	Its Over, Now What?	Pictionary
100	100	100	100	100	100
200	200	200	200	200	200
300	300	300	300	300	300
400	400	400	400	400	400
500	500	500	500	500	500

Conclusions

- **Insert Dr. Nahm’s slides**