ACCE
AMERICAN COLLEGE OF CLINICAL ENGINEERING

Learning from Cybersecurity Tabletop Exercises at the Health System Level

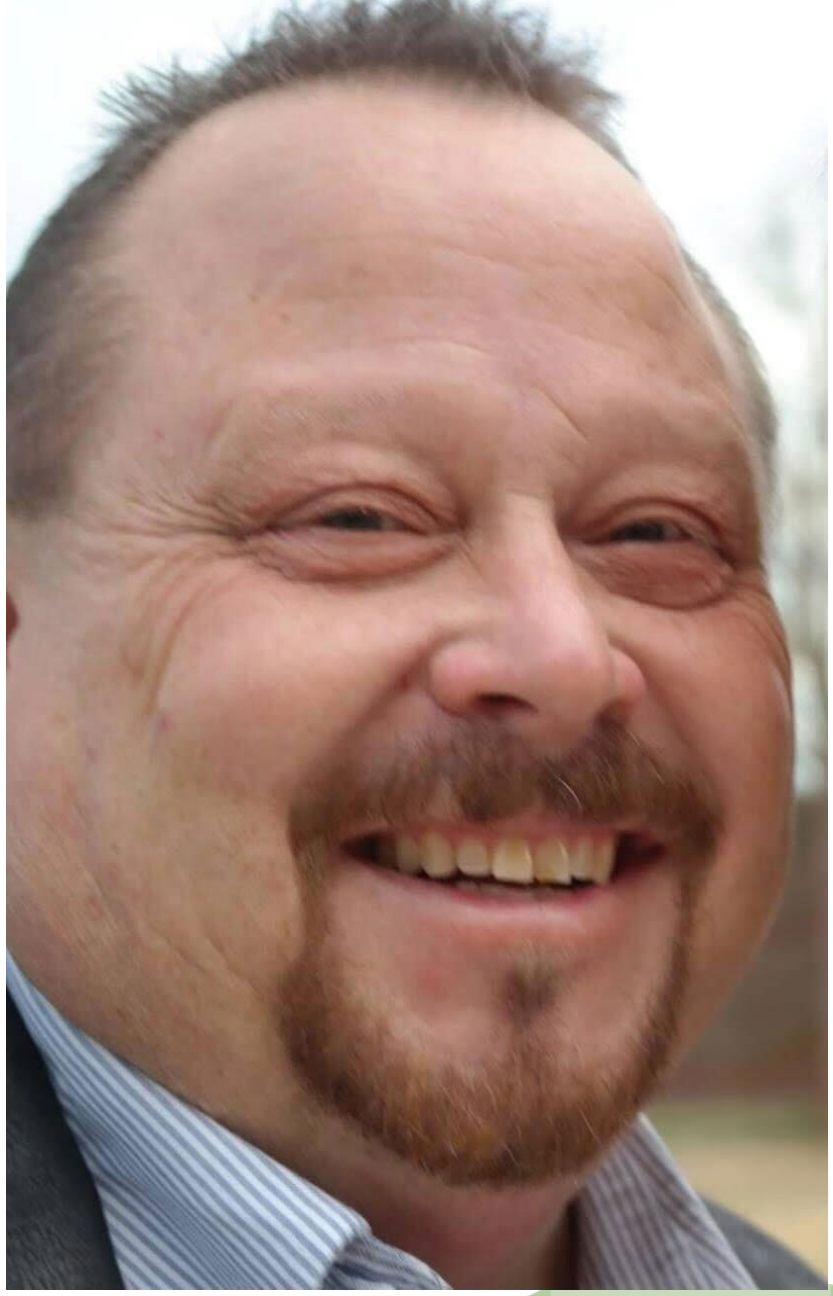
- From Concept to Implementation & Continuous Improvement

Mark Elliott
Director Solutions Engineering
Asimily

Eric Maze
Medical Device Security Engineer,
Rush University Medical Center

Mark W Elliott

- Director of Solutions Engineering, Asimily
- Graduated with a BS Mathematics and Computer Sciences from USCGA. Master in Conflict Resolution from Norwich University. He has held certifications such as CISSP, CWNA, CWSP, ISPS and certified in numerous NAC, SIEM and other network security tools.
- 30 years of experience in Cybersecurity across numerous industries: financial, engineering, manufacturing, medical, healthcare, and primary and secondary education.
- 30 years experience as a Network and Security architect
- Spoken at HIMSS, DARPA, SPOC, AAMI, MDEXPO.



Eric Maze

- Medical Device Security, RUSH University Medical Center.
- Bachelors of Science in Technical Management – DeVry University
- Associates in Electronics and Computer Technology – DeVry University
- 20 years in Clinical Engineering including leadership roles. The last 5 years as a security engineer focused on medical device security and IOT
- Certifications- SANS- GISF, GSEC
- Professional organization affiliations AAMI, HISAC, HIMSS
- Previous papers or presentations

ACCE
AMERICAN COLLEGE OF CLINICAL ENGINEERING

Session Objectives

Introduce cybersecurity TTE at a health system level	Headlines TTE objectives and relevance IS roles in IR and BCDR
Conducting a cybersecurity TTE	TTE methodology NIST 800-61 role notifications Health system roles & responsibilities
Cybersecurity TTE at a Health System	TTE at a health system Scenario Injects 1-5
Lessons learned	TTE conclusion & debrief Plan, processes, and other documentation References

Ripped From The Headlines

I. In 2022, the number of patient records breached increased by 18 percent compared to 2021 to 59.7 million, according to a new report from healthcare analytics company Protenus Breach Barometer.

II. Hacking incidents rose for a seventh year in a row, with 712 incidents occurring throughout 2022.

III. U.S. healthcare organizations suffered an average of 1,410 weekly cyberattacks per organization.

IV. Artificial intelligence and automation programs saved healthcare organizations more than $3 million as these tools can help identify and contain a breach nearly a month faster than those that don't have these tools.

V. Common Spirit Health has incurred $150 million in losses as a result of an October 2022 ransomware attack, the health system's unaudited quarterly report stated. "The Cybersecurity Incident has had an estimated adverse financial impact of approximately $150 million to date, which includes lost revenues from the associated business interruption, the costs incurred to remediate the issues and other business expenses, and is exclusive of any potential insurance related recoveries,"

VI. As the Covid-19 pandemic swept the world over the past three years, cybercriminals took advantage of the chaotic situation and repeatedly shut down hospitals' networks at a time when they were least able to respond. That has meant curtailed emergency services, canceled operations and more deaths

VII. According to data from the CyberPeace Institute, the average cyberattack on a health care system leads to 19 days of patients unable to receive some form of care. In one case, a cyberattack led to around four months of disrupted medical care.

VIII. In September 2019, FDA said medical devices that use 3rd party decades-old software called IPnet are at risk as the Urgent/ 11 vulnerability may allow anyone to remotely take control of the medical devices.

Relevant Joint Commission Standards

❑Cyber Security risks are addressed in the Hospital Emergency Management (EM) chapter, this includes:

- The Hazard Vulnerability Assessment (HVA) (EM.11.01.01)
- Emergency Operations Plan (EOP) (EM.12.01.01)
- Continuity of Operations Plan (COOP) (EM.13.01.01)
- Testing of the EOP and COOP (EM.16.01.01)

❑ Identify Risks at Your Organization

- Some standard frameworks could help you conduct a cyber security risk assessment and develop robust recovery plans to minimize impacts of cyber attacks
- You will not be given all the relevant information and at times, you may think that the scenario is a little too creative (it really can get like this in real life). The full agenda and additional context of the scenario will only be provided as the exercise unfolds.

❑ Outcome

- Better understanding of various roles, responsibilities, activities, and dilemmas that are required in real-life cybersecurity incident or disaster. It will help you assess the readiness of your team and organization.

Why are IoMT Device's Risk so Complex

❑Most devices use the Common Vulnerability Scoring System (V. 3)

- CVSS provides standardized vulnerability scores. When an organization uses a common algorithm for scoring vulnerabilities across all IT platforms, it can leverage a single vulnerability management policy defining the maximum allowable time to validate and remediate a given vulnerability
- The challenges in using CVSS to assess the severity of vulnerabilities in medical devicesis that CVSS and its associated rubric were developed for enterprise information technology systems and do not adequately reflect the clinical environment and potential patient safety impacts

❑ MITRE Risk Rubric

- To address these challenges, the MITRE Corporation, under contract to FDA, developed a rubric that provides guidance for how an analyst can utilize CVSS as part of a risk assessment for a medical device. This rubric was developed by MITRE in collaboration with a working group of subject matter experts across the medical device ecosystem, including FDA, medical device manufacturers, healthcare delivery organizations, security experts, and safety/risk assessment experts
- On October 20, 2020 FDA announced that the rubric was qualified as a Medical Device Development Tool (MDDT). An MDDT is a tool that FDA has evaluated "and concurs with available supporting evidence that the tool produces scientifically-plausible measurements and works as intended within the specified context of use."

Why are Healthcare Systems so Complex

❑Medical Devices do not share the same Lifecycle as other IT devices:

- Computers are replaced every 3-5 years and depreciate over 7 year
- Medical devices persist for decades long past the normal life expectancy of other devices
- Every year past its depreciation threshold is pure profit for the healthcare systems

❑ Medical Device Security is more complex

- This long life ensures a majority of its life will be running on their unsupported legacy OS
- Legacy operating systems makes the securing of these devices difficult requiring on man-power intensive layer-2 micro-segmentation
- Most common IoMT attacks make the device or the fleet of devices go out of service, device availability will definitely impact patient care
- Most common IR steps such as unplugging a suspected device is not reasonable for devices such as respirators. IR steps must take in effect the impact on clinical care
- Example if you have 2 identical CT machines, one in an outpatient facility and one in an ER, they must have different criteria on the IR steps you can take on those devices

Cybersecurity Tabletop Exercise (TTE)

❑Goal

- Provide insight into cybersecurity incident management and forensics and business continuity / disaster recovery.
- Provide insight into the roles, responsibilities and related regulatory requirements likely to follow a cyber-attack.

❑ Activity

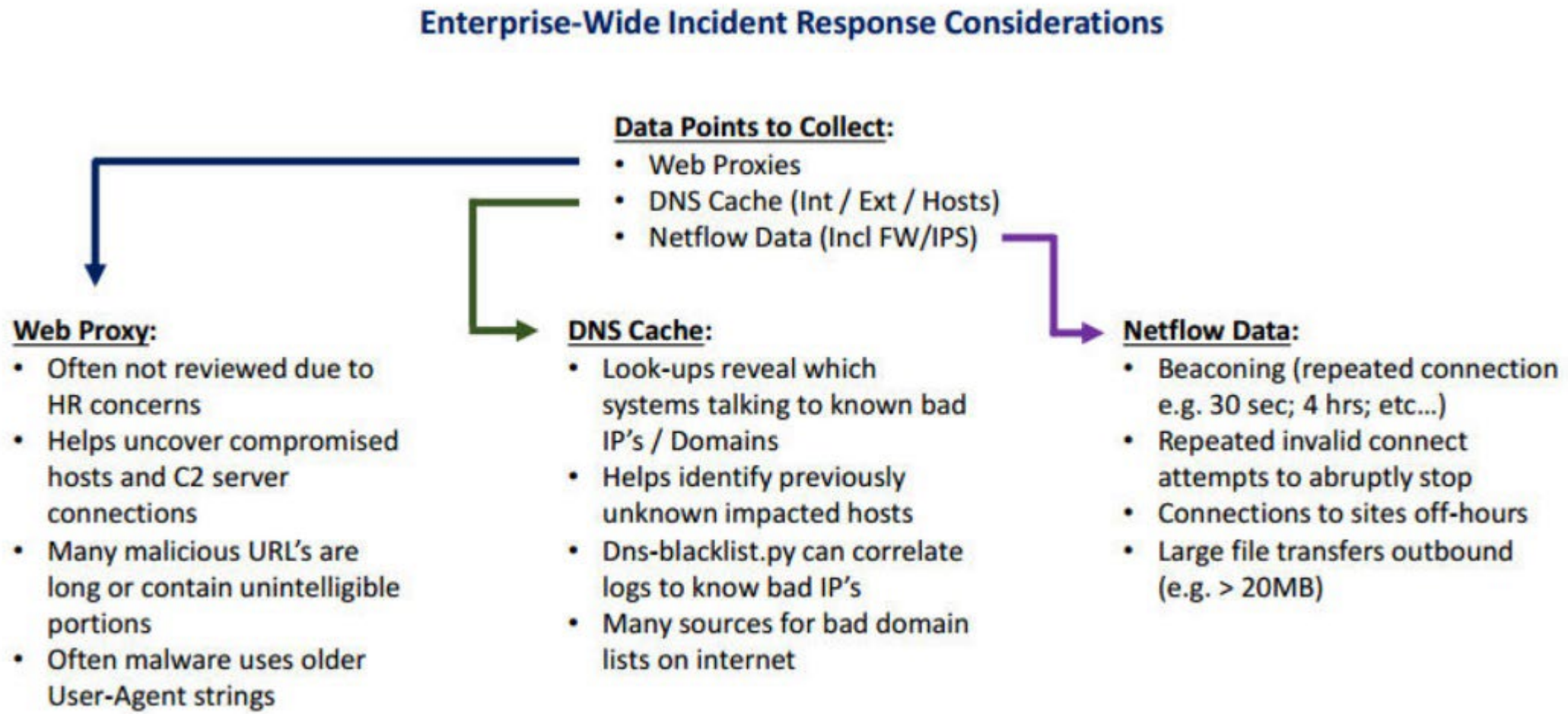
- Play an abridged and accelerated cyber-attack crisis management scenario. You and your team will own all decisions and be responsible for ensuring that all issues are covered.
- You will not be given all the relevant information and at times, you may think that the scenario is a little too creative (it really can get like this in real life). The full agenda and additional context of the scenario will only be provided as the exercise unfolds.
    - **Joint Commission:** Hazzard Vulnerability Analysis (HVA)
    - **NIST:** Risk Management Framework (MITRE ATT&CK Framework)
    - **ONC:** Security Risk Assessment Toole (SRA)

INCIDENT RESPONSE CYCLE

Preparation – Identification – Containment – Eradication – Recovery – Lessons Learned (PICERL)

ACCE
AMERICAN COLLEGE OF CLINICAL ENGINEERING

INCIDENT RESPONSE CONSIDERATIONS



Law Enforcement

- One reason that many security-related incidents do not result in convictions is that some organizations do not properly contact law enforcement. Several levels of law enforcement are available to investigate incidents: for example, within the United States, Federal investigatory agencies (e.g., the Federal Bureau of Investigation [FBI] and the U.S. Secret Service), district attorney offices, state law enforcement, and local (e.g., county) law enforcement. Law enforcement agencies in other countries may also be involved, such as for attacks launched from or directed at locations outside the US.
- The incident response team should become acquainted with its various law enforcement representatives before an incident occurs to discuss conditions under which incidents should be reported to them, how the reporting should be performed, what evidence should be collected, and how it should be collected.
- The Cyber Incident Reporting for Critical Infrastructure Act of 2022 states that Healthcare Institutions must communicate with the Cybersecurity and Infrastructure Security Agency (CISA) on any substantial cyber incidents that are likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the people of the United States, as determined by the Secretary of the Department of Homeland Security.
  - Not later than **72** hours after the affected entity reasonably believes that the covered cyber incident has occurred.
  - Not later than **24** hours after a ransom payment is made.
  - The FBI can be involved at any time and may stop you from making any public acknowledgements to help them respond to

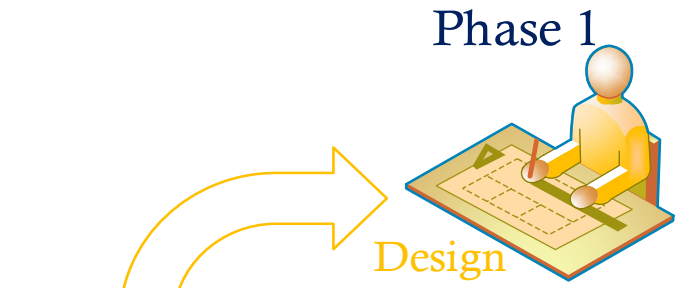
Incident Reporting Agencies

- Notification of a HIPAA breach must happen when unsecured and unencrypted PHI is shared with or lost to unauthorized parties. When this happens, covered entities must:
  - Notify their in-house HIPAA security authorities
  - Notify the OCR
  - Notify all patients they believe may be effected
  - Potentially notify the media
- Healthcare entities must send patient notices right away, regardless of any other factors. Media notices must also go out at once, where applicable. Covered entities have more leeway when it comes to contacting the OCR. Entities must also notify their states
- Federal Information Security Modernization Act (FISMA) requires Federal agencies to report incidents to the United States Computer Emergency Readiness Team (US-CERT),8 which is a governmentwide incident response organization that assists federal and civilian agencies in their incident handling efforts.
- All organizations are encouraged to report incidents to their appropriate Computer Security Incident Response Team (CSIRT). If an organization does not have its own CSIRT to contact, it can report incidents to other organizations, including Information Sharing and Analysis Centers (ISACs).

External Communication

- Organizations often need to communicate with outside parties regarding an incident, and they should do so whenever appropriate, such as contacting law enforcement, fielding media inquiries, and seeking external expertise. Another example is discussing incidents with other involved parties, such as Internet service providers (ISPs), the vendor of vulnerable software, or other incident response teams. Impacted organizations, individuals, and regulators will want immediate information – yet you don't know the who, why, how, when, or what?
- Conduct training sessions on interacting with the media regarding incidents, which should include the importance of not revealing sensitive information, such as technical details of countermeasures that could assist other attackers, and the positive aspects of communicating important information to the public fully and effectively.

Table Top Exercise Methodology



Phase 1

Design

Establish teams and scope the TT&E event

Introduce all participants

Understand TTE goal and level set expectations for all participants

Phase 2

Development

Develop all documentation necessary for the conduct of the TT&E event

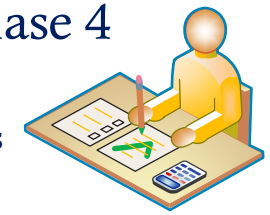
Understand R&R of key players, facilitators, and note takers

Phase 3

Conduct

Conduct the TT&E event

Assess the scenarios, discuss & present response and recovery actions



Phase 4

Evaluation

Document lessons learned from the event

Identify gaps between expected and actual outcomes of IR and BCDR processes

Ref: NIST 800-84

ACCE
AMERICAN COLLEGE OF CLINICAL ENGINEERING

Objectives and Rules of Engagement

- TTE is a **no-fault learning experience** where you think through your response priorities and activities.
- Think through how you would handle the situation presented:
  - What are the issues?
  - What questions do you have?
  - What information is missing?
  - What are your assumptions?
  - What are your priorities?
  - What is the business impact?
  - How do you manage this situation and impact?
  - What other staff do you bring in?
  - Who do you notify and when?
  - What are the required actions/ responses by role?
- Limit sidebar conversations.
- The main objective is to learn from each other by sharing your understanding of IR and BCDR processes after each scenario.

NIST 800-61,84,184 Role Notifications

- CIO
- Head of information security
- Local information security officer
- Other incident response teams within the organization
- External incident response teams System owner
- Human resources
- Public affairs Legal department
- US-CERT
- Law enforcement

- Facilitators
  - They will be moving around the tables to assist the teams as needed.
  - Agree to adhere to the facilitation approach, scenario, timeline, and scope of discussion.
- Note takers
  - Each team will include a scribe/ note taker that will document the individual player's responses, ideas, and work with the team spokesperson on a thorough response.
  - At the end of the TTE, the note taker provides all notes to the facilitators.

Health System Roles & Responsibilities

Role	Actions for the Role
CISO/ Information Security	Accountable for the organization's security
Compliance/ Privacy	Ensures regulatory & privacy requirements are met
Supply Chain/ Vendor/ Supplier	Provides products and services to the organization
Information Technology	Provides availability of technology and services
Legal	Ensures compliance of applicable laws
Healthcare Technology Management/ CE/ Biomed	Ensures safety and reliability of clinical technologies
Corporate Communications/ Public Relations	Internal/ external messaging from the organization
Emergency Management	Manages organization's impacting incidents
Clinical Risk Management	Accountable for the organization's patient and caregiver safety
Nursing/ Physician Leadership	Manages nursing and physician teams and workflows for patient care
Note Taker	Records all responses for the team
Spokesperson	Shares responses from the team

Questions

(think of these based on your assumed role):

- What are the issues?
- What questions do you have?
- What information is missing?
- What are your assumptions?
- What are your priorities?
- What is the business impact?
- How do you manage this situation and impact?
- What other staff members do you bring in?
- Who do you notify and when?
- What are the required actions/ responses by role?

Background

Your company, **OMG Health Systems (OHS)**, recently completed a M&A with **NewGuy**, an organization about a third the size of yours in terms of hospitals, clinics, and staff. It will expand the organizations footprint into multiple states that until now had not been an area of focus for growth.

NewGuy, a 20-year-old health system was known for its great customer service and patient first mentality had approached **OHS** because they are known for bringing in technology to enhance the patient's diagnosis and quality of care. **NewGuy** was known for having antiquated technology, aging infrastructure, and home-grown billing and records systems.

The **M&A Team** want this acquisition completed by this weekend as stipulated in their agreements with governing organizations. The motto, "Get it Done" seems the key motivator

Scenario

Though the paperwork is complete, HR, logo's, and staff are all proud "**OMG Health Systems"** employees, the Information Technology (IT), Information Security (IS), and Clinical Engineering (CE) staff are struggling. **NewGuy** has had poor change control policies and hence poor documentation. This has led to outages, unhappy clinicians and patients at the old **NewGuy** locations.

The Networking Team has been scrambling to get any of their **OHS** Enterprise Security tools in to the environment but are finding the hardware/ software so old that their tools won't work or cause the systems to run slowly. The Identity and Access Management (IAM) team has completed phase 1 integration, all users log into the same **OHS** Active Directory (i.e., you can use your user name and password to log onto any machine).

This weekend the **NewGuy** networks will be brought into **OHS's** WAN and providers will be able to access patient records between their unique EMR systems .

Clinical Engineering made up of members from both systems have been hard at work conducting asset management, maintenance prioritization, and triaging medical devices to determine replacement timelines. The Ultrasound machines were found to have a large number of CVEs and FDA Recalls so the team has been performing upgrades in the field utilizing USB sticks with images of patch software

NewGuy is still using legacy medical devices (Windows XP, 7, 8) as an example their fleet of Peters Ultrasounds have not been used at **OHS** for at least 5 years

Inject 1 – 10 minutes

It's **Friday**, 3:30pm, over the last three weeks, clinical engineers and 3rd party professional services have been busy collecting the medical device information throughout **NewGuy** locations, today is the initial draft of the inventory report. As expected, old, out of date, un-patched medical devices are listed, with asset management anomalies.

The Biomed Manager reports that several of their technicians were disgruntled and had quit due to the large amount of overtime that was being forced on them

The new firewalls and security systems at NewGuy are reporting that some of legacy Windows 7 Peters Ultrasounds are attempting to reach a site called www.Peeters.com. They have asked Biomed if this is expected.

- ❑ **What systems do you have in place to detect this?**
- ❑ **What do you do?**
- ❑ **Who do you inform?**
- ❑ **What proactive steps should be in place?**

Inject 2 – 5 minutes

Monday 8am, The floor nurses and ER staff are reporting problems with the Philips ELITE ultrasounds running Windows 10. The systems are booting but do not appear to be operational nor can staff retrieve previous scans from the ultrasounds

The Network Team reports that some newer Windows 10 Ultrasounds have been sending a large amount of traffic to www.Peeters.com and want to know from the BioMed team if this is expected.

- ❑**What systems do you have in place to detect this?**
- ❑**What do you do?**
- ❑**Who do you inform?**
- ❑**What proactive steps should you perform?**

Inject 3 – 5 minutes

Monday, 11:30am practitioners are reporting that they are having trouble accessing ultrasound images within the EMR system. Ultrasounds on the floors and ER services are still down. The Biomed team reports the few older Windows 7 Ultrasounds do not appear to be effected by this event and that a majority of the Windows 10 Ultrasounds are not available with the exception of those at remote sites.

The network team reports they are seeing a lot of traffic between the Ultrasound machines and several are still sending data over FTP and SCP protocols to www.Peeters.com. They are asking for direction on quarantining and/or firewall rules?

The CISCO has asked the Biomed team for the list of CVEs impacting the entire fleet of Ultrasounds and what their criticality are

- ❑ **What systems do you have in place to detect this and provide information?**
- ❑ **What do you do?**
- ❑ **Who do you inform?**
- ❑ **What proactive steps should you perform?**

Inject 4 – 10 minutes

Monday, 2:30pm, It has become quite evident that your facilities are under attack. The EMR system is up but is extremely slow and most image files (not just ultrasounds) are not accessible with files being reported as corrupted. 85% of your Ultrasounds are not operational at this point.

The ER departments have started to turn away patients and ambulances as your facilities are swamped and at capacity. Surgeries are being rescheduled due to lack of scans. There are questions taht delayed treatment is leading to negative patient outcomes.

The Biomed team has requested permission to relocate the remote older Windows 7 ultrasounds to your main facilities.

The security team has informed you that the site www.Peeters.com is a rogue actor site mimicking the actual Peters site, **www.Peters.com**. Philips sent out a bulletin 3 weeks ago about reports of this site

- ❑ **What systems do you have in place to detect this?**
- ❑ **What do you do?**
- ❑ **Who do you inform?**
- ❑ **What proactive steps should you perform?**

Inject 5 – 5 minutes

Monday, 4:00pm, info@OHS.org receives an email stating that the group Anarchist for Booty (AFB) has launched a series of attacks on OHS and is demanding $600,000 in Bit Coin to stop their attack and release patient imaging records. If not they will perform additional attacks, corrupt all patient records and publish the stolen patient records to the Dark Web

- ❑ **What systems do you have in place to help with this?**
- ❑ **What do you do?**
- ❑ **Who do you inform?**
- ❑ **What proactive steps should you perform?**

Inject 6 – 5 minutes

Monday, 4:15pm, various local news channels have been contacting **OMG Health Systems** for comments on rumors from multiple sources that they have been “hacked”. Though they will not release their sources, it appears this is related to the original **NewGuy** sites reporting up to date wait times for their ERs. They want to give **OHS** an opportunity to share their side of the story before the 5pm news release.

- ❑ **What systems do you have in place to help with this?**
- ❑ **What do you do?**
- ❑ **Who do you inform?**
- ❑ **What proactive steps should you perform?**

Inject 7 – 10 minutes

Tuesday, 6:15am, an all hands meeting is called for 6:30 this morning at the OHS headquarters. As you drive into OHS facilities you see local and national news crew trucks setting up in the parking lot. There is a mix of white and black sedans with government plates also in the parking lot.

The immediate questions are concerning how do we get back to full operational capabilities, protect patient data and document OHS's "Due Diligence" prior to the event:

- ❑ Does OHS pay the ransom or can they recover the lost data, bring the Ultrasounds back on line and deal with the lost patient data?
- ❑ What was the Risk state of your devices prior to the attack
- ❑ What Vulnerability and Anomaly monitoring was done to be aware of possible threats
- ❑ What forensic data did you capture during the attack to help define the tactics and techniques used
- ❑ Did you inform the appropriate

TTE Conclusion: Debrief 15 Minutes

- ❑ Did they have a coordinated plan between Network Security and BioMed Security to diminish risk to the organization?
- ❑ Were best practices were followed in assessing the NewGuy's medical device inventory?
- ❑ What type of tool could have validated the CVEs impacting the NewGuy's medical device inventory?
- ❑ What type of tool could have monitored the NewGuy's medical device inventory for anomalous behavior that signaled the beginning of the attack?
- ❑ Why did OHS's Network Team not block or quarantine devices attempting to reach www.Peeters.com?
- ❑ Was there clarity around who was responsible for each decision and each action?
- ❑ What key players should have raised all the security issues expected in a M&A process?
- ❑ Did the incident raise any systemic problems in the healthcare organization?
- ❑ What drove the individual failures to stop this attack and who should have recognized this and stepped in?
- ❑ Who in the OHS organization has the responsibility to step in and adjust the M&A Team's expectations and timeline?
- ❑ Do you have the tools needed to avoid or respond to this type of cyberattack?
- ❑ Did they communicate appropriately during the evolving scenario

“A plan that is not written is just an idea” – Dwain Siady

PEOPLE

- Develop a RACI matrix
  - Responsibility Assignment Matrix
- Ensure that organizational policies are understood
- Exercise your Business Disaster and Recovery plans at least annually

BUSINESS PROCESSES

- Draft messaging and corporate communications
- Brainstorm with members of the healthcare organization
- Ensure that organizational policies are understood
- Identify required regulatory responses
- Exercise your CIMF and BCDR plans at least annually

INFRASTRUCTURE: Physical and IT

- Ensure that organizational policies are understood
- Restore backups on a scheduled basis and scan for malware.
- Exercise your CIMF and BCDR plans at least annually

SUPPLIERS

- Ensure that organizational policies are understood
- Synchronize cyber-attack preparation plans
- Establish mutual responsibilities before actively engaging with a TPV or a service provider
- Exercise your CIMF and BCDR plans at least annually

Develop an after-action report after the TTE to better understand and evaluate opportunities for improvement.

References

I. https://cybersecurity.wa.gov/tabletop-exercises

II. https://digital-forensics.sans.org/summit-archives/DFIR_Summit/Building-Maturing-and-Rocking-a-Security-Operations-Center-Brandie-Anderson.pdf

III. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-84.pdf

IV. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-184.pdf

V. https://www.acq.osd.mil/dte-trmc/docs/The%20DoD%20Cyber%20Table%20Top%20Guidebook%20v1.pdf

VI. https://www.cnbc.com/2019/10/01/fda-issues-warning-on-medical-devices-that-are-vulnerable-to-cyberattacks.html

VII. https://www.dotmed.com/news/story/48489?utm_campaign=2019-09-16&utm_source=DOTmed+News+Silo&utm_medium=email

VIII. https://www.mitre.org/sites/default/files/publications/pr_14-3929-cyber-exercise-playbook.pdf

IX. https://www.nist.gov/cyberframework

ACCE
AMERICAN COLLEGE OF CLINICAL ENGINEERING

HIMSS 23
17-21 April | Chicago

THANK YOU

Mark Elliott
Director Solutions Engineering
Asimily

Eric Maze
Medical Device Security Engineer,
Rush University Medical Center