TABLETOP EXERCISE HEALTHCARE AND PUBLIC SECTOR

Based on CISA Tabletop Exercise Packages

WISEFROG
‘s-Hertogenbosch, The Netherlands
Document date: 03/10/2024

CONTENTS

EXERCISE OVERVIEW

Exercise Name	Tabletop Healthcare and Public Sector Incident Simulation	
Exercise Date, Time, and Location	TBD	
Exercise Activities	**Time**	**Activity**
	30 Minutes	Threat Briefing and Opening Remarks
	90 Minutes	Module 1
	20 Minutes	Break
	90 Minutes	Module 2
	30 Minutes	Hotwash
Purpose	Examine the cyber resilience of the Client in response to a significant cyber incident.	
National Institute of Standards and Technology Cybersecurity Framework	Identify, Protect, Detect, Respond	
Objectives	Assess the cyber resilience of client during and following a cyber incident impacting network connected medical devices. Evaluate the impacts of a cyber incident on patient care and operations. Improve IT and OT cybersecurity coordination to enhance the cybersecurity posture of client. Evaluate client ability to restore operations after disruptions from cyber intrusions.	
Threat or Hazard	Phishing, Ransomware	
Scenario	A threat actor targets employees through phishing emails. Imaging equipment, patient records, and other medical equipment begin malfunctioning/displaying incorrect data. Personal Health Information (PHI) data is exfiltrated, and ransomware compromises computer systems and equipment.	
Sponsor		
Participating Organizations	Incident response team	
Points of Contact	Insert Organization POC(s) Contact Information	

GENERAL INFORMATION

Building Resilience

The purpose of the National Cyber Exercise Program's CISA Tabletop Exercise Packages (CTEPs) that will executed by WiseFrog Security are to increase your organization's resilience by assessing and validating capabilities and identifying areas for improvement. The National Institute of Standards and Technology (NIST) defines cyber resilience as "the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources

Participant Roles and Responsibilities

Players have an active role in discussing or performing their primary roles and responsibilities during the exercise. Players discuss or initiate actions in response to the scenario.

Observers do not directly participate in the exercise. However, they may support the development of player responses to the situation during the discussion by asking relevant questions or providing subject matter expertise.

Facilitators provide situation updates and moderate discussions. They also provide additional information or resolve questions as required. Key Exercise Planning Team members may also assist with facilitation as subject matter experts during the exercise.

Note-takers are assigned to observe and document exercise activities. Their primary role is to document player discussions, including how and if those discussions conform to plans, policies, and procedures.

Exercise Structure

This exercise is intended to be a multimedia, facilitated exercise. Players will participate in the following:

- Cyber threat briefing
- Scenario modules:
    - **Module 1**: This module introduces several events, including a suspicious email to employees and an unannounced vendor.
    - **Module 2**: This module includes a ransomware attack and the discovery of patient data theft.
- Hotwash

Structure Note: Modules, timeline dates, and discussion questions included in each module may be modified as desired

Exercise Hotwash and Evaluation

The facilitator will lead a hotwash with participants at the end of the exercise to address any ideas or issues that emerge from the exercise discussions.

MODULE 1 – HANDLING EXTERNAL THREATS

Scenario 1 – Joint Alert Warns of Surge in Healthcare Cyberattacks

The Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the Department of Health and Human Services (HHS) Health Sector Cybersecurity Coordination Center (HC3) release a joint alert regarding a rise in cyberattacks targeting healthcare organizations. The alert describes the tactics, techniques, and procedures (TTPs) used by cyber criminals, including phishing emails, ransomware, remote hacking, distributed denial of service (DDoS) attacks, and data exfiltration from healthcare organizations.

Scenario 2 – Employees Targeted by Phishing Email Posing as MSP HR Update

Organization employees receive e-mail notifications from your managed service provider (MSP) requesting they update their profiles prior to the launch of a new human resources (HR) system. The e-mail contains a link and attachment named Update_Form.docx. Employees working at remote workstations across facilities click the link and are asked to log into their web portal. Upon logging in, they are brought to a 404 Error Page. Some employees also open the attachment and click to allow macros to run.

Scenario 3 – Patient Monitor Updates Installed Successfully

Manufacturer's updates are pushed for installation on patient monitors. The updates are downloaded from the manufacturer's website and installed without issue.

Scenario 4 – Unannounced EMR Vendor Patches Vulnerability on Devices

A third-party electronic medical record (EMR) vendor shows up unannounced at your facility to update equipment. The vendor needs to patch a recently discovered vulnerability in software used on several devices, including workstations, imaging and radiology equipment, bedside monitors, and other clinical devices.

Discussion Questions

Discussion questions included in each module are designed to explore different aspects of your operational resilience. The questions may be modified as desired.

1. What are the greatest cyber threats to your organization?
2. What cybersecurity threat information does your organization receive (e.g., information from CISA, Health-ISAC, HHS)?
    a. What cyber threat information is most useful?
    b. How is information disseminated throughout your organization and by whom?
    c. What actions would your organization take in response to an alert like the one presented in the scenario?
3. Has your organization conducted a risk assessment to identify specific cyber threats, vulnerabilities, and critical assets?
    a. What information technology (IT) systems or processes are the most critical to your organization?
    b. Describe your organization's asset management plan and how you prioritize critical assets.
    c. What improvements have been implemented to enhance cyber resilience following recent risk assessments?
    d. Does your organization have a vulnerability management program dedicated to mitigating known exploited vulnerabilities in internet-facing systems?
4. Describe your organization's cybersecurity training program for employees.
    a. How often are employees required to complete this training?
    b. What additional training is required for employees who have system administrator-level privileges?
    c. What type of training methods or approaches have you found most beneficial?
5. How are employees trained to recognize and report cyber threats such as phishing scams?
    a. What additional training does your organization require for those who fall for a fake phishing campaign?
6. How do users report suspicious emails?
    a. What procedures or plans would be followed once a suspicious email has been reported?
7. Describe your organization's cybersecurity posture.
    a. How frequently are users required to change their passwords?
    b. Does your organization use multi-factor authentication (e.g., something you know, something you have, something you are) to mitigate the potential effects of phishing?
8. What are your network access and authentication controls for users?
    a. Does your organization allow users to run document macros? If so, what compensating security controls do you have to mitigate the risk?

    b. What cybersecurity controls are present to mitigate the risk of users entering credentials into phishing websites?
9. What cybersecurity language is included within third-party vendor contracts?
    a. How do you evaluate the cybersecurity posture of your vendors?
    b. How often are contracts reviewed?
    c. How do your service level agreements address cyber incident notification?
    d. How do vendors notify you that patches or updates are required?
10. How do employees report suspected phishing attempts or other possible cybersecurity incidents?
    a. What actions does the IT department take when suspicious emails are reported?
    b. What feedback do employees receive after reporting a suspicious email or event?

MODULE 2 – RANSOMWARE AND PATIENT DATA THEFT

Scenario 1 – System Admin Closes Out Inactive IT Accounts

A system administrator discovers active accounts for IT employees that left the organization over the past 12 months. The administrator closes them out.

Scenario 2 – Incorrect Patient Records Reported by Nurses

Nurses on the floor report that patient records are displaying incorrect information about medication, diagnosis, and personal information.

Scenario 3 – Inaccurate Bedside Monitor Data and Infusion Pump Failures

Staff discover bedside monitor data is inaccurate and the infusion pumps are not operating properly and are failing to deliver infusions at the correct rate.

Scenario 4 – Ransomware Attack Locks Files with Extortion Message

Ransomware messages appear on computers throughout organization, and users report they are unable to access their files. A message is displayed that reads:

“Hello! Your files have been liberated. We have your data. But do not fear because for the sum of $1,000,000 your files will be returned. The decryption key will expire in 72 hours. Please submit payment to the wallet below or we will start selling patient data to the highest bidder.”

Scenario 5 – Patients Targeted by Extortion Calls After Data Breach

Current and former patients contact the hospital saying they received calls from someone claiming to have access to their medical records and offering to return them for a fee. The patients are provided enough information to verify the callers have their records.

Patients say the fees range from a few hundred dollars to more than a thousand and are demanding to know why these individuals have their records.

Some say they contacted law enforcement; others contacted the media. Many are threatening legal action.

Discussion Questions

1. Using your organization's existing incident response plan/cyber incident response plan (CIRP), describe the actions your organization would take at this time.
    a. Describe the training your employees receive on this plan.
    b. What guidance does the plan include on assessing the severity of the incident?
    c. How does incident severity level dictate response?
    d. How are critical systems and processes incorporated within your CIRP?
2. Does your organization have backups of vital records and EMRs stored in a location separate from your primary working files/copies?
    a. How frequently do you run backups?
    b. How long do you keep copies of archived files backed up?
    c. How long would it take to restore primary files from backups?
3. What redundant systems exist for when primary systems are compromised?
    a. What alternative systems or manual processes are implemented to continue operations if a critical system is unavailable for a significant period?
    b. Who can authorize use of alternate systems or procedures?
    c. How long can you perform manual or alternate processes on your critical systems?
    d. What additional resources are required to operate with manual processes?
4. Using your CIRP as a guide, how have your priorities changed based on these recent events?
5. Explain your organization's decision-making process regarding ransomware payment.
    a. Are ransomware policies/procedures included in your CIRP?
    b. Explain how your response partners, such as your cyber insurance provider or third-party vendors, are involved in your procedures.
    c. Discuss the advantages and disadvantages of either agreeing or refusing to pay the ransom.
    d. Discuss potential legal and reputational ramifications of paying or not paying the ransom.
    e. Describe the impact the sale or release of sensitive information or PHI would have on your response and recovery activities.
6. What security breach notification laws does your state or industry have?
7. Describe your organizational processes to respond to the media reports and inquiries.
    a. What pre-scripted messages have been developed for cyber incidents?
    b. How would public messaging be coordinated and disseminated during a cyber incident?
    c. How would you preserve and reinforce the public's confidence and trust in your organization during a significant cyber incident?
8. Based on discussion, what changes would you implement to increase the resilience of your organization?

TRAINERS

Nariman Aga-Tagiyev is an Application Security Architect with more than 20 year experience in software development. Have been working as full stack web application developer, backend developer, DevOps engineer, cloud developer and since 2016 fully involved in Application Security related activities.

https://www.linkedin.com/in/aganariman/

Serhat Altın has a strong focus on security by design and secure configuration by default. He excels at creating user experiences that prioritize security without compromising usability, ensuring that systems are both intuitive and inherently secure from the outset. With his deep understanding of secure design principles, Serhat integrates security best practices into every stage of product development, making it easier for users to adopt secure configurations effortlessly.

https://www.linkedin.com/in/serhataltin/

TRAINING LOCATION FACILITIES

The Table Top Exercise will take place at a location selected by the hiring company within the European Union. For locations outside the EU, special quotes can be provided upon request. The following facilities are required:

- A projector and power outlet for the trainer
- Adequate space to allow participants to form working groups of 3-4 people for independent hands-on exercises

CONTACT INFORMATION

We would be happy to have a short call with you to discuss your needs and answer your questions. We do not have aggressive marketing strategy and won't spam you if you get in touch with us.

Contact by email: security@wisefrog.nl

Contact by phone or WhatsApp: +31613732993

Schedule a 30 minutes call: https://calendly.com/aganariman/nariman-30-minutes

SUPPLIER INFORMATION

Company name	WiseFrog
Country of establishment	Netherlands
Address	Willemspoort 102, 5223WV, 's-Hertogenbosch, Netherlands
Email (Invoices)	Invoice@wisefrog.nl
Email (administrative)	info@wisefrog.nl
EU VAT-ID	NL003278436B94
KVK - Dutch Chamber of Commerce number	78029260
IBAN	NL92 ABNA 0876 9924 91
BANK SWIFT (BIC)	ABNANL2A
Contact person	Nariman Aga-Tagiyev
Contact person email	nariman@wisefrog.nl
Phone:	+31613732993

ABOUT WISEFROG

Our Story

Founded with a passion for innovation and a commitment to excellence, WiseFrog has been at the forefront of the digital landscape for over a decade. What started as a small team of visionaries has grown into a powerhouse of creative minds, dedicated to pushing boundaries and delivering cutting-edge solutions.

Our Approach

At the core of WiseFrog's philosophy lies a commitment to collaboration and innovation. We work closely with our clients, understanding their unique needs and goals, to deliver tailored solutions that drive tangible results. Our team of experts combines creativity with technical expertise, ensuring every project is executed with precision and attention to detail.

Our Mission

At WiseFrog, we bring together the dynamic worlds of creative media production, innovative product development, and robust cybersecurity. Our mission is to transform ideas into secure, impactful realities. Whether you're looking to create compelling content, develop cutting-edge products, or ensure the highest level of digital security, we're here to make it happen.

Our team consists of passionate creatives, product developers, and cybersecurity experts who are dedicated to excellence in every project we undertake. We believe that every story, product, and system deserves a meticulous and innovative approach. That's why we foster a culture of collaboration and ingenuity, ensuring that your vision is brought to life safely and effectively.

TERMS AND CONDITIONS

1. **Confidentiality**

All information shared by clients during the collaboration will be treated as confidential. Our trainers are committed to maintaining the privacy and security of any sensitive information provided. This data will not be disclosed, shared, or distributed to any third party outside of the training, except as required by law.

2. **Offer Validity**

The offer for this workshop is valid for a duration of 30 days from the date of issuance. After this period, the offer may be subject to change or withdrawal.

3. **Payment Terms**

Invoices for the training must be paid within 30 days following the completion of the workshop. Travel costs related to the workshop are not included in the quoted price and will be invoiced separately after the event. Late payments may incur additional charges or penalties as per WiseFrog's billing policy.

4. **Travel Costs**

Travel and accommodation costs incurred by trainers for on-site workshops will be billed separately after the workshop. These costs will be outlined in a detailed invoice sent to the client.

5. **Cancellation Policy**

Cancellations made up to 7 days before the scheduled training date will be eligible for a full refund. Cancellations made within 7 days of the training will not be eligible for a refund. However, substitutions or rescheduling may be allowed with prior notice.

6. **Liability**

While every effort is made to ensure the accuracy and relevance of the information provided during the training, we are not responsible for any consequences resulting from the use or misuse of the information provided. Clients are responsible for applying threat modeling practices in accordance with their own organizational policies and legal requirements.

7. **Intellectual Property**

All training materials, including presentations, handouts, and digital resources, remain the intellectual property of WiseFrog. Clients are not permitted to reproduce, distribute, or share these materials outside their organization without prior written consent.