TABLETOP EXERCISE MARITIME PORTS

Based on CISA Tabletop Exercise Packages

WISEFROG
‘s-Hertogenbosch, The Netherlands
Document date: 08/10/2024

CONTENTS

EXERCISE OVERVIEW

Exercise Name	Tabletop Maritime Ports 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 resilience of the client during and following a cyber incident impacting the maritime sub-sector. Evaluate the ability for Client to coordinate information sharing during a significant cyber incident. Identify areas of improvement in cyber incident response plans and overall organizational resilience during and following a significant cyber incident.	
Threat or Hazard	Cyber-Attack	
Scenario	A zero-day vulnerability leads to a cyber-attack impacting port and maritime transportation operations.	
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 joint advisory from CISA, the U.S. Coast Guard Cyber Command (CGCYBER), and the Federal Bureau of Investigation (FBI), and indicators of a potential network compromise.
    - **Module 2**: This module includes operational impacts to port operations, media inquiries, and the successful exploitation of vulnerabilities to an information system.
- 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 – JOINT CYBERSECURITY ADVISORY AND NETWORK RISKS

Scenario 1 – Cyber Attack on Major U.S. Port

A cyber-attack against a large U.S. port is reported across major national news outlets. A web server at the port was breached via an exploited vulnerability in the port's <authentication infrastructure>. The malicious actors obtained the log-in credentials for a type of popular password management software that allowed entry onto port networks. A CISA, CGCYBER, and FBI joint advisory notes that advanced persistent threat (APT) cyber actors are likely among those exploiting the vulnerability. The advisory further identifies this incident as part of an ongoing campaign targeting U.S. ports, transportation companies, and other transportation sector organizations using known exploited vulnerabilities (KEVs) in unpatched legacy systems to gain network entry. CISA, CGCYBER, and the FBI urge organizations to ensure password software is not directly accessible from the internet and strongly recommends domain-wide password resets.

Scenario 2 – Unauthorized Account Access

Multiple people are forcefully logged out of their accounts. They report their passwords have been changed by someone else and they cannot reset it as their security question answers were changed.

Scenario 3 – Phantom Vessel Alert

Vessel Traffic Controllers in the Harbormaster's Office (HMO) notice a vessel appearing to start into the port via the Vessel Traffic Information System (VTIS). Controllers attempt to contact the vessel; however, it does not respond. Controllers in the HMO notice the vessel no longer appears on VTIS. Visual inspections verify there was no vessel traversing the port.

Scenario 4 – MSP Cyber Incident Alert

A security researcher contacts your organization informing you that a trusted Managed Service Provider (MSP) in the Maritime Transportation Sector was recently the target of a significant cyber incident. You do not use this vendor but do employ other MSPs.

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 cybersecurity threats to your organization?
2. What cybersecurity threat information does your organization receive?
    a. What cyber threat information is most useful?
    b. How is information disseminated across your organization and by whom?
    c. What actions would your organization take following an alert like the one presented in the scenario?
    d. What mechanisms exist for your organization to share information across the subsector?
3. How does your organization assess risks in conjunction with maritime partners?
4. Describe the risks/advantages to maintaining legacy equipment/systems.
    a. How do you manage technology that is no longer supported by the manufacturer?
    b. What supply chain concerns do you have regarding legacy equipment/systems?
    c. Describe your organization's equipment decommissioning process.
    d. Describe your organization's equipment security commissioning process.
5. Describe your organization's patch management plan.10
    a. What processes are used to evaluate and maintain an allowed list of patches?
    b. How does risk inform decisions regarding allowed hardware, firmware, and software?
    c. What considerations (e.g., extended downtime, loss of data, impaired functionality, etc.) are addressed in the plan's risk management strategy?
6. How is your network configured (e.g., network segmentation, least privilege access, multi-factor authentication, etc.) to defend against malicious actors?
7. What tools (e.g., threat hunting, security audits, etc.) do you leverage as part of a proactive cybersecurity strategy?
8. What Indicator of Compromise (IOC) feeds does your organization use?
9. How does your organization baseline network activity?
    a. How do you distinguish between normal and abnormal traffic?
    b. What are your next steps when abnormal activity is detected/reported?
10. What is the role of cybersecurity in the review and selection of third-party vendor support?
    a. What cybersecurity language, (e.g., cybersecurity training and cyber incident notification requirements), is included within third-party vendor contracts?
    b. How do you evaluate the cybersecurity posture of your vendors?
    c. How often are contracts reviewed?
11. What level of access do your third-party vendors have to your organization's network?
    a. How often are third-party access rights and data logs reviewed?
12. How do your service level agreements address cyber incident notifications?

MODULE 2 – OPERATIONAL IMPACTS ON PORT OPERATIONS

Scenario 1 – Gate ID Card Reader Malfunction

All gate ID card readers begin to malfunction. Some gates are abnormally slow to open while others will not open at all. As a result, trucks attempting to deliver and pickup cargo are unable to enter or exit the terminals, causing major delays at gates and backups on local roadways.

Scenario 2 – VTIS Access Loss

Incoming vessels report they are not receiving information from the port on their assigned terminals. HMO controllers discover that they have lost access to VTIS and cannot identify vessels or their intended destination.

The lack of access to VTIS results in significant backups on the waterways.

Scenario 3 – Media Reports Cyberattack

Local news media begins to report on the delays at the port. Some news organizations are claiming to have insider information that the port is currently experiencing a significant cyberattack.

Discussion Questions

1. Using your organization's cyber incident response plan (CIRP), describe the actions your organization would take to minimize impact on current operations.
    a. What guidance does the plan include on assessing the severity of the incident?
    b. How does incident severity level dictate response?
    c. How are critical systems and processes incorporated within your CIRP?
2. How sufficient are your organization's current internal resources for responding to the cyber incidents in this scenario?
    a. What additional resources outside of your organization would be necessary for responding to the cyber incident?
    b. What are the processes or procedures for requesting additional resources?
    c. What external partners (e.g., CISA, FBI, etc.) would you contact for assistance?
3. How would you attempt to mitigate the issue with the gate card readers?
    a. What are the impacts of gate malfunctions on port operations?
    b. How long can the port operate with gates and card readers malfunctioning?
    c. Describe the process to implement manual override of the gates/readers and perform verifications on incoming/outgoing personnel and cargo.
4. What are the impacts on the port when VTIS is malfunctioning?
    a. What navigational backups can be utilized by the port and incoming/outgoing vessels?
5. What external organization(s) would you be engaged with?
    a. Are there any regulatory reporting requirements?
6. Describe your organizational processes to respond to the media reports and inquiries.
    a. What pre-scripted messages do you have for cyber incidents?
    b. How would public messaging be coordinated and disseminated during a cyber incident?
    c. How do you preserve and reinforce the public's confidence and trust in your organization during a significant cyber incident?
7. What plans and policies are in place for recovery and restoration of critical infrastructure operations and services?
    a. What are your priorities regarding recovery efforts?
8. Based on discussion, what changes will you implement to increase the resilience of your organization?
    a. Describe the "lessons learned" and corrective action processes you use.
    b. What measures will you take to secure your network from a similar incident happening in the future?

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.