Cyber Crisis Management Readiness Methodology for Maritime Ports and Terminals

Version 2.5

Aug 2024

Version Control

Done by	Edit description	Version	Date
Deb Housen-Couriel	Writing and review	1.0	20 January, 2022
Deb Housen-Couriel	Writing and review	2.0	30 January, 2022
Deb Housen-Couriel, Maxim Shcherbina	Writing and review	2.0	13 February, 2022
Alina Mitelman-Cohen, Deb Housen-Couriel	Writing and review	2.0	23 June, 2022
Ram Levi	Review	2.1	28 June, 2022
Ronen Meroz, Alina Mitelman-Cohen	Review	2.2	28 June, 2022
Gadi Ben Moshe, Maxim Shcherbina	Review	2.3	28 June, 2022
Maxim Shcherbina	Update	2.4	23 February, 2023
Meital Drucker	Minor changes	2.4	07 March, 2023
Ram Levi	Modificaions	2.5	01 August 2024

About Konfidas

Konfidas is a leading cybersecurity and crisis management company established in 2013. We offer:

- Cyber crisis readiness with leading expertise in C-level training.
- Response to cyberattacks, crisis management, and incident response (IR).
- Managed Cybersecurity Services (MSSP) for SMBs using our cyberwar room that operates 24/7 (*8272).
- Support for compliance with regulatory requirements for cybersecurity and data privacy.
- Related professional services.

Konfidas has been repeatedly selected by top Israeli industry-leading firms for cybersecurity and crisis readiness and management projects (for example, Amdocs, ZIM, Clalit Health Services, Teva, Neema, etc.).

We excel at client-driven solutions, comprehensive cyber risk management and cyber crisis management, and on-time execution.

Konfidas has a proven track record of successfully managing complex and high-profile cyber crises that result from a wide range of cyber threats.

We are proud to be a gender-equal company!

10+
Years of Experience

250+
Clients

17
Industry Verticals

200+
Complex Cyber Attacks in Leading Organizations

10K+
Managed Licenses

150+
Weekly Cyber Intelligence Reports

Executive Summary

1. In the face of escalating cyber threats, maritime ports and terminals, with their complex interconnected systems and critical role in global trade, are particularly vulnerable. A cyberattack on a port can cause significant disruptions to operations, leading to financial losses, reputational damage, and potential safety and environmental hazards.
2. Recognizing the inevitability of such incidents, this document provides a comprehensive Cyber Crisis Management Readiness Methodology tailored to the unique needs of ports and terminals.
3. The methodology emphasizes a proactive approach, acknowledging that it's not a matter of "if" but "when" a cyberattack will occur.
   - 3.1. It outlines a structured crisis management framework, encompassing clear roles and responsibilities, effective communication plans, and pre-defined templates for key tasks.
   - 3.2. It underscores the importance of a robust Business Continuity Plan (BCP) to ensure minimal operational impact during a cyber crisis.
4. The BCP should include predefined decisions on critical processes, commercial strategies, and immediate action plans for handling operational disruptions.
5. The methodology also provides detailed guidance on incident response, recovery, and post-incident activities.
   - 5.1. It highlights the criticality of the first hours of incident response, emphasizing the need for swift action and collaboration among various stakeholders.
   - 5.2. It outlines the roles and responsibilities of key personnel, including the Board of Directors, CEO, Incident Manager, CIO, CISO, COO, CFO, Legal and Regulatory Compliance Team, Physical Security and Safety Team, Communication, Public Relations and Customer Support Team, HR and Union, Technical Forensics Team, Technical Containment and Recovery Team, Intelligence Team, and Negotiation Team.
6. The incident management steps are categorized into detection and analysis, containment and eradication, recovery, and post-incident activities. Each step is explained in detail, with examples of actions to be taken.
7. The methodology also addresses the legal and regulatory requirements that ports need to comply with during and after a cyber incident. It provides a template for an operational

timeline, port asset classification, management status meeting agenda, and sample communications for different stakeholders.

8. In conclusion, this Cyber Crisis Readiness Methodology offers a practical and actionable framework for ports and terminals to prepare for, respond to, and recover from cyberattacks. By adopting this methodology, ports can enhance their resilience against cyber threats, minimize operational disruptions, and safeguard their critical role in global trade.

Contact Konfidas today to fortify your cyber defenses and ensure operational continuity in the face of cyberattacks info@konfidas.com

Table of Contents

Introduction

1. The purpose of this document is to support the cyber crisis management readiness of marine ports and port terminals (“ports”).
2. It consists of principles for creating a business continuity plan (BCP) adapted to the specific requirements of ports when they are undergoing a cyber incident, and in the aftermath of the incident.
3. Since it is not a question of “if” a cyber incident will occur in a port but “when”, it is important for port managers to be able to answer the question: “Do we know what to do when a cyber incident occurs that targets our systems”?
4. It is recommended that the port management assume that the duration for initial recovery from such a cyber attack is at least 10-14 days, based on the overall statistics of cyber attacks that occurred during the past years.
5. This document details the implementation of the BCP during the course of such an incident and, to clarify, the process is not based on a risk management approach but rather on the assumptions made in the first moments after the incident’s occurrence.

Key elements of typical port structure

Port divisions

6. In a typical port, several unique divisions can be found:
   - 6.1. Marine Operations
   - 6.2. Yard and Gate Operations
   - 6.3. Rail Operations
   - 6.4. Operations Planning
   - 6.5. Engineering and Equipment Services
   - 6.6. Security and Safety
   - 6.7. Human Resources / Labor
7. As in any commercial organization, some or all of the following divisions also exist in a port:
   - 7.1. Sales, Marketing and Public Relations
   - 7.2. Business Development
   - 7.3. Customer Service

7.4. Finance

7.5. Legal Counsel and Regulatory Compliance

7.6. Risk Management and Insurance

7.7. Information Technology / Operational Technology (IT / OT)

Port Key Operational Processes

8. The main operational processes in a port can be categorized as follows:

8.1. Marine (quayside) processes:

8.1.1. Vessel berthing and unberthing

8.1.2. Container loading and discharge

8.1.3. Vessel husbandry and agency services

8.2. Yard Management processes:

8.2.1. Stacking and unstacking

8.2.2. Storage

8.2.3. Internal transport

8.2.4. Special cargo handling

8.3. Hinterland:

8.3.1. Gate services (“Gate in”/”Gate out”)

8.3.2. 3rd party Trucking operations (drop and pickup)

8.3.3. Rail operations

8.4. Planning:

8.4.1. Vessel and berth schedule management

8.4.2. Cargo planning

Port Systems

9. Modern ports are equipped with a large number of digitized systems which support the various port operational procedures. Those systems often interconnect with each other (as well as with other stakeholder systems); with the result that damage to one system is likely to affect the possibility for other systems to function, or to function completely.

10. The key operational systems in a port may include the following:

10.1. A Terminal Operating System (TOS), may include a computer terminal installed in cargo handling equipment and connection to GNSS tracking.

10.2. The Gate Operating System (GOS), may include LPR, OCR, CCTV, weighbridges, radiation detection system, damage control cameras, and automatic barriers and gates.

10.3. The Entry Permit System - a database that manages the Entry Permit to the port for truck drivers as well as for trucks, cars, and any other vehicles. This may in some cases be part of the GOS.

10.4. An Electronic Data Interchange (EDI) System for electronic message exchange with port stakeholders.

10.5. OT-related management systems (e.g. the cranes' PLC (Programmable Logic Controller) management system, Reefer electricity supply management, and monitoring, management systems for gauges, pumps, and valves (used to control the flow of wet bulk cargos).

10.6. A billing system for port dues and other payments.

10.7. An Operational Web Portal that may include cargo status inquiries, truck time slot appointments, and more.

10.8. A labor hiring and tracking system, especially in ports where hiring is done on a day-by-day basis.

10.9. Cargo handling and planning support utilities (e.g. BAPLIE viewer).

11. Ports that operate piloting services have additional systems, such as:

11.1. Vessel Traffic Service (VTS).

11.2. Automatic Identification System (AIS).

11.3. Radar.

12. There may be other electronic and IT / OT systems in use, that are less “port-specific”, such as:

12.1. ERP (Financial, HR, etc. some times may be several separated systems).

12.2. Document management system.

12.3. Email system.

12.4. Inventory management system for equipment and spare parts.

12.5. Building management systems (e.g. environmental control, access control, fire detection).

12.6. Security CCTV, including storage of footage.

12.7. Telecommunication systems (fixed, mobile, radio), including emergency or backup systems.

Port stakeholders

13. The stakeholder landscape involved in port activities and business processes (depending on the size, scope, and complexity of the operating environment) in the context of a cyber incident can be extensive and diverse.

14. These entities may be characterized as the following:

14.1. Ocean transportation: shipping companies, ship agents, mooring service providers (pilots, tugboats,).

14.2. Hinterland transportation: trucking companies, rail operators, barge operators.

14.3. Regulatory and law enforcement authorities: national and regional cybersecurity authorities; the national coast guard; customs authorities; Police and local security agencies; as well as the governmental authorities responsible for immigration, health, agriculture, veterinary services, and environmental protection. If a personal data breach is implicated, the national and regional data privacy authorities will also be relevant.

14.3.1. In the United States, the relevant authorities will include specifically the Department of Homeland Security (DHS) / CISA, the Coast Guard and the regional Area Maritime Security Committee (AMSC), the Federal Maritime Commission, the Port Authority, and the local port Police.

14.4. Supply chain: importers and exporters, including their agents; freight forwarders, customs agents, and external warehouse operators.

14.5. Maritime-related authorities: Port Authority, Customs

14.6. Service providers, such as: bunkers providers, waste treatment companies, food providers, equipment technicians and others.

14.7. Data exchange platforms operators: Port Community System.

14.8. Employees and labor unions.

Cyber Attack Scenarios

15. Below are possible scenarios of cyber attacks that are relevant to ports.

16. Threat actors include the following, which will be treated in detail below:

16.1. Cybercriminals.

16.2. State and state-sponsored proxies.

16.3. Opportunistic (script-kiddies).

16.4. Hacktivists.

16.5. Insiders ("revenge" attackers).

17. Criminally-motivated attacks:

17.1. The perpetrators are cybercriminals motivated by financial gain.

17.2. The methods used include extortion, financial fraud, smuggling, and cargo theft.

17.3. Usual methods mimic the APT (Advanced Persistent Threat) groups, by using the same tools and methods used by them

18. Nation-to-nation hostile cyber activities:

18.1. Hostile cyber activities may be used as an element of a hybrid war (physical and cyber methods used as tools of warfare); or, outside of a war context, as a hostile act that may be categorized as an internationally wrongful act by an adversary nation-state.

18.2. Nation-to-nation hostile cyber activities (wartime activities and non-war hostilities) commonly result in, or are aimed, at the logical and/or functional destruction of computers, storage, and network devices.

18.3. There are different legal ramifications for the results of such nation-to-nation hostile cyber activities, as well as the choice of target (e.g. the port) by the adversary nation-state.

18.3.1. These ramifications should be thoroughly explored and analyzed by the targeted organization, in consultation with national security actors, as relevant; as they have direct implications for the targeted organizations response to the incident.

18.4. It is important to note that even if not specifically designated as such by a specific national legal regime, ports and related systems are generally considered critical infrastructure:

18.4.1. On their own; and

18.4.2. Because of the dependencies of other critical infrastructures and supply chains on their continued and robust operations.

18.5. Nation-state motivations for initiating a cyber incident are political; and proxy actors may be used by the nation-state, in order to make attribution more difficult.

19. Espionage:

19.1. Commercial, industrial, and state-sponsored.

19.2. Usually done with APT (Advanced Persistent Threat) methods.

19.3. Aimed at data exfiltration, including business data, intellectual property, and personal data.

20. Hacktivism:

20.1. Politically, socially or religiously motivated cyber groups activists, aiming to publicly embarrass the port administrator, the nation-state in which it is located, or selected shipping companies of a specific flag state that is utilizing the port facility.

20.2. Usually done by denial of service attacks, website defacement, and other infringement on public-facing interfaces/users. Sometimes with “spam” messages to employees and partners/customers.

21. “Revenge” attacks:

21.1. Usually executed by disgruntled employees or ex-employees.

21.2. Can be very destructive if the attack is carried out by employees with high privileges or IT / OT employees.

Impact Scenarios

22. Ransomware attacks are specifically characterized by the impact of data exfiltration, which is leveraged for extortion purposes (including protected private data of employees, customers, and suppliers; intellectual property; and operational data).

22.1. The perpetrators are cybercriminals motivated by financial gain, with some exceptions.

22.2. Methods include encryption of ToS and GoS-related servers; and encryption of administrative systems, the lack of which is liable to lead to a shutdown of key terminal administration functions (IT / OT, procurement, customer service, billing, and HR).

23. Scenarios causing Interruption/loss of access to critical systems or infrastructure

23.1. Such as gate operations (GoS), planning (ToS), terminal operations, and financial systems.

24. Impact that causes interruption or loss of access to safety and environmental systems.

25. Non-ransomware exfiltration and leakage of sensitive and/or personal data.

26. Beyond the specific nature of the incident - financial and reputational impact.

27. Financial and relational impacts on third parties, such as customers or suppliers.

Port activities before, during and after a cyber incident

Principles of Crisis Response in Ports and Terminals

28. The port terminal effective response to a cyber attack is based on 2 main principles:

28.1. Crisis Management.

28.2. Port operations continuity.

29. Crisis Management - should include the framework of the most suitable methodology for each terminal to effectively manage the crisis, in particular:

29.1. Crisis Manager.

29.2. Crisis Management team.

29.3. Roles and responsibilities.

29.4. Communication plan.

29.5. Templates for key tasks of the team (situation assessment, business impact analysis, etc).

30. Port operational continuity - the operational continuity framework is based on the operational and commercial strategy that each terminal should plan in advance, for a severe cyber attack.

30.1. Such strategies can range from total shutdown of the terminal, via marginal operations based on basic and ad hoc contingencies, and up to maximal operations based on dedicated contingencies that were prepared, tested and trained for such an incident.

30.2. The principles of the operational continuity should be as follows:

30.2.1. Mapping of the most critical processes in the terminal vs the less critical (for example: vessel discharge and loading - critical, customer support - critical, trucking gate reservation - not critical)

30.2.2. The next step is to agree on the commercial principles for each process. Examples: we perform vessel discharge only, and skip exports and empties ; we release only reefer and DG import units ; etc

30.2.3. After framing the key processes, the terminal should focus on the critical processes and develop tangible contingencies that can be deployed quickly and satisfactorily support the critical processes. Such contingencies may include development of dedicated IT solutions, training of employees, and so on. Examples:

30.2.3.1. The terminal planners and marine operations team will gain the vessel caro plan from the vessels and use it to continue the discharge.

30.2.3.2. The terminal understands that the finance team will be idle during a cyber attack since invoicing and payment activities will be shut down. The finance team can be used to reinforce the customer service team and provide the necessary support.

30.2.3.3. The terminal will reach out to the local customs authority and develop a mutually tangible plan to cooperate during a cyber crisis in a way that would enable the terminal to release imports.

30.3. Regardless of the chosen strategy that will be implemented in the case of a severe and long term event, a terminal should have an immediate action plan on the handling of the immediate operational implications on the terminal, including:

30.3.1. Handling of vessels stuck in middle of operations;

30.3.2. Handling of rail stuck in the middle of operations;

30.3.3. Handling of 3rd party trucking caught within the terminal premises;

30.3.4. Handling of trucking queues that may quickly form in front of the gates.

Crisis Management Approach In Shutdown Scenario

31. In cyberattacks that involve the shutdown of systems and services (such as ransomware and destructive cyber attacks), the first hours of incident response are critical.

32. The crisis management approach should be divided according to the following:

32.1. Initiation : 0-24 hours - urgent immediate response - all hands on deck.

32.2. Crisis Mode - 24/7 crisis mode - full crisis mode. BCP processes are activated.

32.3. Crisis mode with a gradual return to business as usual.

32.4. Partial crisis mode in parallel to business as usual. Initiating implementation of security configurations to close gaps identified during the breach.

32.5. “Hyper care” period - business as usual with a limited crisis team.

33. It should be assumed that during major impact incidents, like Ransomware, the IT / OT systems might not be available for a number of days. Business BCP processes should take it into account and be developed accordingly.

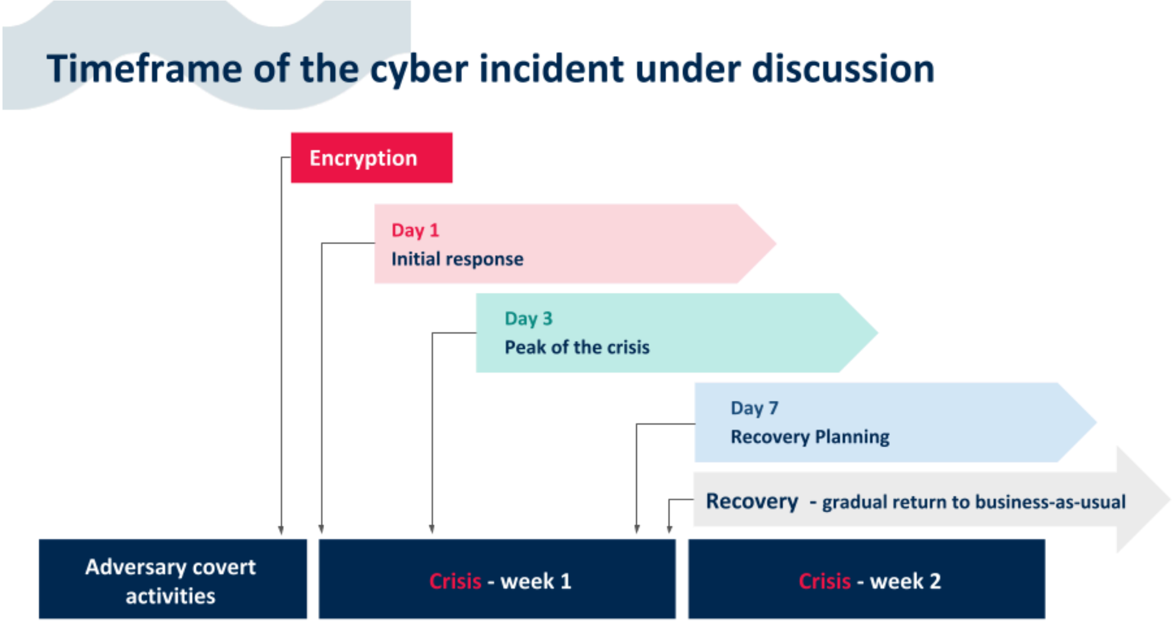
Timeframe of the cyber incident under discussion
Encryption
Day 1
Initial response
Day 3
Peak of the crisis
Day 7
Recovery Planning
Recovery - gradual return to business-as-usual
Adversary covert activities
Crisis - week 1
Crisis - week 2

Illustration of crisis management in a ransomware scenario

Organizational Roles and Responsibilities

34. During the incident, the management should provide directives and perform the main decision-making. The crisis will be mostly managed by designated situation rooms at different organizational levels.

35. [Organizational Structure Diagram for a corporate crisis] - TBD by the organization

Board of Directors

36. Pre-incident:

    36.1. The Board of Directors will approve the port company's Cyber Incident Management Policy, BCP, and related procedures.

37. During the incident:

    37.1. The BoD will monitor the performance of the CEO, Incident Manager, and the different work teams during the incident.

    37.2. In the event of a ransom and/or extortion incident - set guidelines for negotiation and decide whether to comply with or refuse the ransom demand.

37.3. Remain updated regarding the notification of the cyber insurance policy’s activation and the policy implementation; as well as overseeing the actual incident management.

37.4. Review of required reports to law enforcement and relevant government bodies during the crisis.

37.5. Overseeing financial reports during the crisis, ensuring added supervision as needed (eg, voice phone checks to verify recipients of payments).

38. Post-incident:

38.1. Reviewing and approving the post-incident report that includes an analysis of the crisis, examination of the company’s personnel involved in handling the incident, conclusions, and preparation for future incidents.

38.2. Review and supervise adjustments in policy as a result of lessons learned.

38.3. Review of required reports to law enforcement and relevant government bodies after the crisis has ended, including any necessary follow-up reports.

38.4. Examination of the company’s financial reports post-incident.

Chief Executive Officer (CEO)

39. Pre-incident:

39.1. Define the company's Cyber Incident Response Policy.

39.2. Verify the existence of BCP plans of all relevant departments.

39.3. Verify BCP drills, at least on yearly basis, are taking place.

39.4. Define the principles of work with the Board of Directors during a cyber incident.

40. During the incident:

40.1. Declaring a cyber incident and its severity.

40.2. Appointing an incident manager, if one has not been pre-appointed in the company's Cyber Incident Response Policy.

40.3. Defining the company's goals throughout the crisis and their priorities, for example - customer service continuity, minimizing reputational damage, minimizing financial damage, etc.

40.4. Approving the scope and channel of internal and external communication.

40.5. Approving cyber insurance activation.

40.6. Coordinate decision regarding the payment of a ransom to the attacker.

40.7. Remain updated regarding the financial situation of the company in the crisis context, and determine the credit framework that the organization may leverage in the crisis management interest.

40.8. Defining the criteria for ending the crisis.

41. Post-incident:

41.1. Verification for “post mortem” activities in all departments, resulting in the development of plans to close the gaps identified during the incident and updating incident response/BCP plans according to “lessons learned” during the incident.

Incident Manager

42. Pre-incident:

42.1. Take part in cyber incident drills and simulations, as preparation to perform the role during the cyber incident.

42.2. Preparing a replacement for the role in case of unavailability.

42.3. Prepare a platform for incident activities documentation and "project management".

42.4. Ensure existence of contact lists and alternative communication channels.

43. During the incident:

43.1. The IM will be responsible for setting up an incident response team (IRT), as detailed below; if said team has not been pre-appointed in the company's Cyber Incident Response Policy..

43.2. Reflect the overall situational assessment to the Board of Directors.

43.3. Manage decision-making processes, based on risk analysis.

43.4. Manage and supervise all response teams.

43.5. Adjust the organizational structure of the response team to the evolving situations (e.g. : appointment of positions as needed, adjusting relevant processes, etc.)

43.6. Ensure availability of communication channels and proper communication between the situation rooms.

43.7. Escalate and adapt the response to the evolving situation.

43.8. Support for the recruitment of assistance and resources, as needed (for example IT / OT and information security providers to be available for 24/7 response).

43.9. Plan and think ahead about unfolding and future optional scenarios.

43.10. Work closely with the CEO, assisting him or her with the organization's management.

43.11. Incident manager will appoint a PMO (if he or she has not been pre-appointed by the company's Cyber Incident Response Policy. who will work closely with him or her, and will assist with all project management activities, Including:

43.11.1. Task management

43.11.2. Schedule management

43.11.3. Documentation - decisions, execution, plans.

44. Post-incident:

44.1. Conduct a debrief and contribute to the organizational post-incident debrief and lessons learned.

44.2. The IM is responsible for carrying out the steps as specified in this methodology ("incident management steps"), including lessons learned at the end of the incident and recommendations for improvement of the incident response process.

Incident Response Team (IRT)

45. Each incident will be dealt with by an IRT that includes the relevant personnel for handling the incident according to the decision of the IM, eg. technical forensics, technical containment and recovery, incident management, legal and regulatory, HR, external IR team, and insurance; as well as any other experts (including external experts) who can assist in the analysis, containment, recovery, regulatory reporting and forensic investigation of the incident.

46. The IRT will be responsible for managing the incident, defining tasks and priorities for the various work teams, and performing the ongoing, comprehensive situational assessment with respect to the incident.

47. The team members will report to the IM and act subject to his other directives and approval for initiated activities (beyond his or her directives).

48. The team members will coordinate any action related to the incident with the IM and, as relevant, with other team members.

Chief Information Officer (CIO)

49. Pre-incident:

49.1. Verification of incident response and BCP procedures for all IT / OT functions, including that “incident readiness” tools and methodologies are in place - like infrastructure to collect logs and forensic data, tools/methodology to find Indicators of Compromise (IoCs) on systems and firewalls, tools/methodologies to effectively restrict network traffic from infected systems and networks, restoration systems from backups that might be infected, etc.

49.2. Appointment of IT / OT incident commander.

49.3. Overall responsibility for IT / OT preparedness to effectively handle cyber incidents including processes, tools, training and drills. Main topics:

49.3.1. Identifying the main attack scenarios.

49.3.2. Implementing tools and processes to streamline incident response and recovery:

49.3.2.1. Develop and maintain documentation - systems, networks and cloud.

49.3.2.2. Develop infrastructure to support forensic activities.

49.3.2.2.1. Sufficient logging to make forensic investigations easier and help to detect malicious activity during the event.

49.3.2.3. Procedures to perform isolation of networks and systems

49.3.2.3.1. network level filters, remote access, Internet connectivity, 3rd parties connectivity, individual systems disconnects.

49.3.2.4. Develop procedures for password resets.

49.3.2.4.1. Administrators, users, applicative users and connection strings/keys.

49.3.2.5. Develop procedures for main systems recovery including Active Directory, DB's, mail, web site, etc.

49.3.2.5.1. Procedures to include re-building the main systems from scratch - install new servers, OS, applications and copy the data from the backups.

49.3.2.6. Prepare alternative communication channels for cases where standard channels like mail and teams are not available.

49.3.2.7. Develop cyber threat intelligence capabilities.

49.3.2.8. Ensure the existence of tools to effectively implement IoC and Yara rules to detect attackers tools and attacker's activity.

49.3.3. Performing training and exercises for the IT / OT team to identify gaps in incident handling preparedness.

50. During the incident:

50.1. Appointment of IT / OT incident commander (in case one hasn't been pre appointed).

50.2. Overall responsibility for all technical aspects of the incident handling - containment and eradication of the attack, and full systems recovery.

50.3. Member of the CEO incident response team.

50.4. Report to the CEO incident response team:

50.4.1. Intelligence data about the attacker and attacker's operational tactics.

50.4.2. Forensic information about the impact to the systems, confirmed leaked data, stolen credentials and possible impact on 3rd parties.

50.4.3. Estimated timelines of the recovery activities including information about possible missing data that should be completed by the Business teams.

50.5. Updating IT / OT incident response team with management directives.

50.6. Approval to activate external teams - like the forensic team and Active Directory specialists.

51. Post-incident:

51.1. Verification of "post mortem" activities in all IT / OT functions/teams,

51.2. Verification of updating incident response/BCP plans according to "lessons learned" during the incident.

51.3. Verify the creation of plans to add controls for environment hardening, especially the path that led to the compromise.

51.4. Follow-up on the execution of the plans.

Chief Information Security Officer (CISO)

52. Pre-incident:

52.1. The CISO is responsible for updating this methodology in accordance with the investigation of past incidents, as well as any organizational or technological changes in the company.

52.2. In order to prepare for a cyber incident, the CISO will regularly document threat scenarios relevant to the company based on findings arising from risk surveys, penetration tests, and intelligence reports.

52.3. The CISO will plan and conduct exercises for the company's employees and response teams, in accordance with the threat scenarios that are developed.

52.4. Maintain an up-to-date contact list of critical employees and suppliers for handling the cyber incident, the list will be available even in the event of systems and network shutdown.

52.5. Overall responsibility to ensure IT / OT preparedness to effective handling of cyber incidents, including, but not limited to:

52.5.1. Development and maintenance of documentation - systems, networks, and cloud.

52.5.2. Preparation and practice of relevant technical procedures for handling a cyber incident such as - Active Directory recovery, email recovery, and cross-organizational password reset.

52.5.3. Ensuring proper operation of backup systems and practice recovery processes including recovery from off-line storage (e.g. tapes) and recovery from cloud-based backups.

52.5.4. Procedures to perform isolation of networks and systems - network-level filters, remote access, Internet connectivity, 3rd parties connectivity, individual systems disconnects.

52.5.5. Preparation of infrastructure that will allow a full forensic investigation - the infrastructure will include logs from various components of the network such as FW, routers, servers, databases, endpoints, email service, and application logs from main business-operational systems.

53. During an incident:

53.1. The CISO has the overall responsibility for handling the technical aspects of cyber incidents.

53.2. The CISO will verify the completeness of containment activities and will approve activities during the recovery phase including the process to approve reconnection of the restored system to the network, opening of specific communications (internal and external), approval for VPN access for IT / OT/3rd parties to handle the event

53.2.1. In general, no significant IT / OT operation during the crisis should be done without CISO review and approval.

53.3. The CISO will define compensating controls during the event to reduce the risk arising from the fact that the attacker might still have a hold in the environment

53.3.1. For example, if the decision is not to replace service account passwords, CISO will define monitoring activities that will ensure that those accounts are not used for malicious activities.

53.3.2. Another example can be the decision to open Internet access to internal systems. CISO should define compensating controls to reduce the risk of the attacker starting to communicate with compromised systems within the network.

53.4. The CISO will work closely with the forensic team and SoC and guide them in the investigation and monitoring aspects. The main outcome should be:

53.4.1. Identification of "patient zero" - initial compromise

53.4.2. Identification of tools/methods that are allowing the attacker to control systems within the network (persistence),

53.4.3. Identification of Indicators of Compromise (IoC) - fingerprints of tools, accounts and network activity used by the attacker.

53.5. Ensuring that SoC is capable of verifying and updating the identified IoCs (Indicators of Compromise) on relevant systems.

53.6. For SoC, CISO will define the criticality and urgency for handling alerts sent to the SoC (e.g. triggered IoC, authentication failures of the privileged account, multiple RDP sessions from a single host, etc.).

54. Post-incident:

54.1. At the conclusion of a cyber incident, the CISO will participate in the investigation and lesson-learning process,

54.2. Recommend to the CIO on the required adjustments in the defense system and BCP plan, based on the incident investigation (lesson learned implementation).

Chief Operating Officer (COO)

55. Pre-incident:

55.1. The COO shall prepare an operational Business Continuity Plan to minimize the operational impact of a cyber attack. This plan shall include predefined decisions in several aspects, such as:

55.1.1. The members and responsibilities of the "operations war room".

55.1.2. Coordinate with IT / OT possible backups for manual operation: pre-printed or offline pre-saved information (vessel and train unloading/loading lists, yard inventory)

55.1.3. Coordinate with customs for gate-out manual approval.

55.1.4. Coordinate with train operator alternative ways for information exchange.

55.1.5. Set prioritization parameters for deciding which cargo/vessel to handle.

55.1.6. Arrange agreements with nearby terminals to forward vessels to them.

56. During the incident:

56.1. When a cyber-attack which causes failure in information systems occurs, the COO's responsibility is to assess the operational situation and take actions to minimize the operational impact.

Please notice that there are several major operational concerns for the ports' COO to take into account:

56.1.1. Handling the vessels/trucks/trains in the middle of operation.

56.1.2. Handling the vessels outside the port waiting to be docked.

56.1.3. Handling the trucks outside the port waiting for Gate in.

56.1.4. Handling cargo in the yard (especially reefers).

56.1.5. Handling vessels/trucks/trains that are planned to arrive at the port in the systems down period.

56.2. For each of these concerns, the port shall have a predefined decision. A "war operations room" shall be established for coordinating the ongoing operation. The planning division may be a good candidate for the coordination activity.

Some of the possible actions are as follows:

56.3. Handling the vessels in the middle of operation.

56.3.1. Using pre-printed unloading/loading lists.

56.3.2. Using offline pre-saved unloading/loading lists.

56.3.3. Using unloading/loading information that the ship/ship agent has.

56.3.4. Adding clerks for a manual update of the unloading/loading lists and manually generating EDIs to be sent as systems get back or by a standby system or by alternative methods (e.g. e-mail).

56.4. Handling the trucks in the middle of operation.

56.4.1. Allocating and loading/unloading cargo using pre-printed yard inventory.

56.4.2. Allocating and loading/unloading cargo using offline pre-saved yard inventory.

56.4.3. Unloading cargo to a dedicated temporary area.

56.4.4. Adding clerks for manual coordination with customs for gate-out approval.

56.4.5. Adding clerks for a manual update of the yard inventory and manually generating EDIs to be sent as systems get back or by a standby system or by alternative methods (e.g. e-mail).

56.5. Handling the trains in the middle of operation.

56.5.1. Allocating and loading/unloading cargo using pre-printed yard inventory and loading lists.

56.5.2. Allocating and loading/unloading cargo using offline pre-saved yard inventory and loading lists.

56.5.3. Unloading cargo to a dedicated temporary area.

56.5.4. Adding clerks for manual coordination with customs for train gate-out approval.

56.5.5. Adding clerks for a manual update of the yard inventory and manually generating EDIs to be sent as systems get back or by a standby system or by alternative methods (e.g. e-mail).

56.6. Handling the vessels outside the port waiting to be docked and those which are planned to arrive at the port in the systems down period.

56.6.1. A predefined decision which vessel to: Handle manually or forward to a nearby port with which there is an adequate prearranged agreement or to notify it cannot be served until further notice.

56.6.2. For those to be handled manually, the actions are as for handling the vessels in the middle of the operation described above.

In addition, adding clerks for manual coordination with health and security administrations for vessel docking approval.

56.7. Handling the trucks outside the port waiting for gate in and those which are planned to arrive at the port in the systems down period.

56.7.1. A predefined decision which truck to: handle manually or forward to a nearby port with which there is an adequate prearranged agreement or to notify it can't be served until further notice.

56.7.2. For those to be handled manually, the actions are as for handling the trucks in the middle of the operation described above.

56.8. Handling trains that are planned to arrive at the port in the systems-down period.

56.8.1. A predefined decision which trains to handle manually or forward to a nearby port with which there is an adequate prearranged agreement or to notify it can't be served until further notice.

56.8.2. For those to be handled manually, the actions are as for handling the trains in the middle of the operation described above.

56.9. Handling cargo in the yard.

56.9.1. Allocating and transferring cargo using pre-printed yard inventory.

56.9.2. Allocating and transferring cargo using offline pre-saved yard inventory.

56.9.3. Adding personnel for frequent inspections in reefer and dangerous goods areas.

56.9.4. Adding clerks for a manual update of the yard inventory and manually generating EDIs to be sent as systems get back or by a standby system or by alternatives methods (e.g. e-mail).

57. Post-incident:

57.1. After the cyber crisis, when information systems get back online, the main responsibilities of the COO are to:

57.1.1. Validate the inventory accuracy by stocktaking all the cargo in the yard and updating the TOS accordingly.

57.1.2. Sending and receiving the EDIs of the actions during the incident.

57.1.3. Completing all the activities stopped/delayed because of the incident.

57.1.4. Update the operational business continuity procedures according to the lessons learned from the cyber crisis actions.

Chief Financial Officer (CFO)

58. Pre-incident:

58.1. Mapping payments and expenses that must be paid even during an incident and defining the method of payment in case of systems shutdown.

58.2. Mapping and backing up critical financial data to allow critical financial operations during a cyber incident that involves systems shutdown, such as suppliers payment details.

58.3. Examine options (manual\technical) for stopping automatic payment instructions during a cyber incident.

58.4. Prepare for ransom payment by engaging with an external crypto company, and consider opening an account.

59. During the incident:

59.1. Decide which payments (manual/automatic) to stop or allow based on the incident status and progress.

59.2. Handling payments and expenses that must be paid in order to allow business operation.

59.3. Approving any financial expenses required for incident handling such as payment for external services (incident response team, negotiation, PR, etc.), as well as payment of ransom demand or other payments related to the incident.

59.4. Assessing the financial damage to the company as a result of the attack, the assessment will be carried out throughout all steps of incident management.

59.5. The CFO will validate the integrity of the company's financial reports during the incident; and verify submission of any time-sensitive required reports (or arrange for a delay in their submission).

59.6. If the company, during a cyber incident, will not be able to issue invoices, collect payments or other financial related activities, define what data must be collected and in which alternative methods.

59.7. Conducting a BIA - business impact analysis during the cyber incident.

59.8. Insurance aspects:

59.8.1. Approval of operating external teams and services under the cyber insurance policy (eg., forensics teams, negotiators);

59.8.2. Defining how to contact and activate the insurance policy for cyber coverage of the incident - including any requirement to contact law enforcement as part of its activation;

59.8.3. Obtaining the CEO's approval before activating the insurance policy;

59.8.4. Tracking and documentation of port expenses as a result of the incident, for the purpose of the insurance claim.

59.8.5. Handling payments and receipts, such as:

59.8.5.1. Billing customers;

59.8.5.2. Suppliers' payments;

59.8.5.3. Employees' salary payments, including incident-related overtime.

60. Post-incident:

60.1. Assessing the financial damage to the company as a result of the attack including its future consequences.

60.2. Updating the systems with the operations that were performed manually, such as:

60.2.1. Billing.

60.2.2. Suppliers' payments.

60.2.3. Employees' salary payment.

60.2.4. Ransom payment (if paid).

60.3. Validating the integrity of the company's financial reports.

60.4. Conduct a debrief and contribute to the organizational post-incident debrief and lessons learned.

Legal and Regulatory Compliance Team

61. The Legal and Regulatory Compliance Team, which includes the Chief Legal Advisor, staff, and any external legal counsel, is responsible for managing and mitigating the legal and regulatory exposures of the cyber incident.

62. Pre-incident:

62.1. Carrying out an initial mapping of all potential legal and regulatory requirements, including regulatory notifications. An example is included in Appendix 3, for the United States/ State of New Jersey regulatory context.

62.2. Follow up with any relevant issues with the state or national regulatory authority for the maritime sector, in order to achieve clarity. The US authorities in this context are the Coast Guard and the Federal Maritime Commission.

63. During the incident:

63.1. Appropriate documentation must be implemented throughout the incident, in order to prepare for any potential legal claims against the organization as a result of the cyber incident.

63.2. The legal and regulatory notifications that are relevant during a cyber incident are divided into five categories:

63.2.1. Notifications to cybersecurity regulators - both required and optional (such as CISA in the United States).

63.2.2. Notifications to data privacy regulators - on a state-by-state, regional or national basis, as relevant with respect to the data subjects whose personal data has been compromised;

63.2.3. Local law enforcement notifications - such as the local or regional Police.

63.2.4. Federal, regional or international law enforcement bodies, such as the FBI, Interpol and Europol.

63.2.5. Contractual notifications, as per the conditions agreed with specific suppliers regarding the obligation to notify of the occurrence of a cyber incident and/or personal data breach.

63.3. In addition to these five categories, ports that are registered as companies on stock exchanges may have obligations to submit reporting to the stock exchange and / or shareholders under its specific regulatory regime. These reports are likely to follow a specific format.

63.4. In a different context of potential legal exposure, should a ransomware payment to the attackers be considered, the legality of the ransomware payment and the relevant legal vetting by the Chief Legal Advisor, are critical, and these are addressed below in Appendix 4.

63.5. Additional issues to be considered by the Chief Legal Advisor include:

63.5.1. Notifications to vendors and suppliers that are not required as part of contractual obligations, yet are determined to be significant for maintenance of the positive business relationship.

63.5.2. Similar notifications to customers.

63.5.3. Review of any notifications to employees and/or unions.

63.6. During the attack, this Team's responsibility entails duly reporting to the regulatory authorities that have jurisdiction over the cyber incident, including any breach of protected personal data (see below) or ensuring that such reporting takes place via the designated operational channel; and contacting enforcement bodies as necessary, all subject to the IM and CEO decisions and in coordination with the Communication and Public Relations Team;

63.7. As well, this Team will monitor and determine the legality of any ransomware or other payments to the attacker, together with other relevant stakeholders such as the organizational insurer.

63.8. The Team will participate in the drafting and approval of any external notifications, including regulatory and contract-related notifications, as well as those of Public Relations and Human Resources, in order to ensure both overall compliance with legal requirements and the standardization of the notification texts.

64. Post-incident:

64.1. Following the attack, this responsibility entails full follow-up with the authorities mentioned above, as well as managing any legal claims that may have resulted from the cyber incident.

64.2. In summary, the Team will be responsible for legal and regulatory notifications, addressing legal issues that arise following the incident such as privacy lawsuits, insurance, and ransom demand payment; as well as review external notifications including to the media, customers, and employees.

64.3. Appendices 3 and 4 provide additional details.

Physical Security and Safety Team

65. Pre-incident:

65.1. Identification and mitigation of hazardous situations that will include ensuring safety messages and briefings are made.

65.2. Preparation and approval of on-boarding list for all external entities that should take part in supporting the organization during the crisis.

65.3. Review and prepare safety measures during potential crises, based on operational malfunctioning analysis if some of related systems will not be available.

66. During the incident:

66.1. Reinforcement of security personnel at the ports' gate/perimeter may be needed, especially if the security supporting systems like CCTV are compromised.

67. Post-incident:

67.1. Update the business continuity procedures for physical security, according to the lessons learned from the cyber incident.

Communication, Public Relations and Customer support Team

68. Pre-incident:

68.1. As part of company preparedness, this Team will formulate a plan for managing the company's reputation during the incident, including preparation of "staggered" notifications as the incident progresses, as well as Q&A for use on the website or other public-facing materials (see Appendix).

68.2. The Team's plan will include:

68.2.1. Adding personnel to the support team to handle the increased number of calls/trouble tickets to handle.

68.2.2. In case the regular means of communication (support phone numbers/email/dedicated website) are not functional: operating a predefined alternative and notifying the stakeholders.

68.2.3. Notifications to specific stakeholders with instructions about planned Vessel/Truck/Train arrivals to the port.

68.2.4. Periodical status update emails, in which general content will be predefined in templates that relate to the timing of their release during the incident, to a predefined list of stakeholders. These stakeholders should include employees, customers, suppliers, and the public. See Appendices 6 and 7 for examples)

68.2.5. Periodical status update calls with a predefined list of stakeholders.

68.3. Press announcements should also be prepared, including possible live interviews.

68.3.1. Personnel who are interviewed should be prepared in advance with messaging statements.

68.3.2. Follow-up with the media should take place, as needed.

69. During the incident:

69.1. Perform the activities as per the Team's prepared plan (as described above).

69.2. This Team will formulate the internal and external communications regarding the cyber incident and its status, in coordination with other teams and with the approval of the IM, Legal, and the CEO (as relevant).

69.2.1. These will not include the regulatory and legal notifications which are the responsibility of the Legal Team, but should be coordinated with them.

69.3. Press announcements and interviews.

70. Post-incident:

70.1. Internal and external communications regarding the recovery process and the incident aftermath.

70.2. Update the Team's plan according to the lessons learned from the cyber incident

HR and Union

71. Pre-incident:

71.1. Preparing an alternative payment process for employees and suppliers to a situation where the company's network and systems are not available.

72. During the incident:

72.1. Handling logistical aspects required for work in a 24/7 format during the crisis - food, accommodation, showers, etc.

72.2. Addressing employee's inquiries regarding the incident and its impact on them.

73. Post-incident:

73.1. Update the HR business continuity procedures according to the lessons learned from the cyber incident.

73.2. Continue to communicate as needed with personnel and with the Union regarding the outcomes of the incident.

73.3. Consider a dedicated meeting post-incident with Unions to adjust expectations and work procedures in the future.

Technical Forensics Team

74. The Technical Forensics team, which shall be appointed by the Incident Manager in consultation with the CEO, CLO, Insurance and any other relevant entlties, will be responsible for:

    74.1. Identifying and closing the attacker's entry point ("patient zero");

    74.2. Identifying the attack tools used by the attacker to deploy the attack, and deleting them completely from the company's assets;

    74.3. After identifying the systems that were affected in the attack and damaged by it, the team will perform the required tests before returning the systems to use;

    74.4. Identifying user accounts (including generic users) that were created or used to carry out the attack.

Technical Containment and Recovery Team

75. The Technical Containment and Recovery Team will be responsible for recommending and carrying out containment and recovery activities.

76. The Team will formulate a systems recovery plan based on:

    76.1. Information about the damaged systems received from the forensics team;

    76.2. The criticality of the system to Port, activities;

77. The Team will recommend technical ways to improve the company's cybersecurity posture, based on lessons learned from the incident. These may include recommendations for updating this methodology.

Intelligence Team

78. The Intelligence Team, which shall be appointed by the Incident Manager in consultation with the CEO, CLO, Insurance and any other relevant entlties, will be responsible for characterizing the attacker that has targeted the port, including the wider geopolitical or economic context of the attack.

79. The Team will identify and monitor the internet and darknet for potentially leaked information and additional threats to the company.

80. The Team will initiate takedown of sites with leaked information from the company, as well as relevant social media channels, with the assistance of the national cybersecurity authority.

Negotiation Team

81. The Negotiation Team, which shall be appointed by the Incident Manager in consultation with the CEO, CLO, Insurance and any other relevant entltics, will be responsible for managing all communication with the attacker, in coordination with the CEO and the IM.

82. The goals of the negotiation process include:

82.1. Establishing a channel of communication with the attackers.

82.2. Reducing the ransom payment to a minimum.

82.3. Gaining information regarding the depth of the penetration of the attacks to the port's assets.

82.4. Gaining time for the purpose of improving the means of the company's defense and enabling further forensics investigation.

82.5. Understanding the attacker's motivations, whether financial, national or other.

83. The Negotiation Team will also work with the Insurance Team, the CEO, the CFO, Legal, and other relevant personnel to verify the "wallet hygiene" in the incident of a ransomware payment. This includes the determination by Legal of the legality of payment, as well as the establishment of no known connection between the attackers and bodies sanctioned by the relevant government entities, such as the United States Office of Foreign Assets Control (OFAC).[1]

Incident Management Steps

Detection and Analysis

84. Purpose: Preliminary clarification regarding the existence of a cyber incident, initial assessment of the extent of the damage, and rapid formulation of the actions required to stop and contain the attack.

85. From the moment a potential incident is identified/reported, the company's management will appoint an incident manager and set up an incident response team (IRT).

86. The IRT and the Technical Forensics team will perform a joint assessment regarding the nature of the incident, as well as an initial assessment of the damage.

87. The IRT will work in collaboration with an external incident response team to manage and handle the incident.

[1] See https://sanctionssearch.ofac.treas.gov/.

88. The IRT will operate other work teams depending on the nature of the incident (for example, in case of a ransomware attack, a negotiation team is required).

89. The IRT will contact the critical third-party suppliers required to handle the incident.

90. The Technical Forensics team will be responsible for investigating and analyzing the incident as detailed in the roles and responsibilities section.

91. The IM will define a documentation mechanism, in which the actions taken during the handling of the incident will be fully recorded, including the time of the action and who performed it.

92. The IM will define the communication channels of the IRT including a framework for reporting the findings and actions taken in handling the incident.

93. If necessary, the incident manager will order the collection of more detailed logs (for example, informational logs that were not collected before the incident) as well as a ban on changes to the systems necessary for investigation and documentation (forensics).

Containment and Eradication

94. Purpose: To gain control of the attack vector and tools in order to eliminate or minimize the damage to the organization.

95. The IM will approve the containment and eradication actions carried out by the technical containment and recovery team and will be responsible for documenting them.

96. Examples of containment and eradication actions:

96.1. Blocking outbound and/or inbound communications from the Internet;

96.2. Specific network traffic blockages within the organization network for example IP addresses and types of traffic discovered in the forensic investigation that was used by the attacker;

96.3. Disconnect specific servers and/or services from the network;

96.4. Update software and operating system versions;

96.5. Change access permissions and reset passwords across the network including applicative users;

96.6. System boot;

96.7. Delete files and software used by the attacker during the attack;

96.8. Update EDR and other security softwares with the attackers indicators (IoC's);

96.9. Initiating business continuity plans and alternative work methods in case of system shutdown;

Recovery

97. Purpose: To return to business as usual as prior to the cyber incident and return to full functioning of any activity or service that was disabled, restricted, or disrupted by the incident.

98. The IM will approve recovery actions carried out by the technical containment and recovery team and will be responsible for documenting them.

99. Examples of recovery activities:

    99.1. Checking the reliability of backups;

    99.2. Restore from backups;

    99.3. Removal of communication blockages performed at the containment stage;

    99.4. Setting up servers and reinstalling applications;

    99.5. Performing functional tests and penetration tests (PT) on the entire network, with an emphasis on the restored systems;

100. The incident manager will ensure the implementation of monitoring means to ensure non-recurrence of the incident.

Post-Incident Activities

101. The incident manager in collaboration with the CISO and the technical teams will lead an in-depth investigation of the incident which includes the following aspects:

    1.1. Accurate and detailed characterization of the incident.

    1.2. Factors - technical and processes, that made the incident possible.

    1.3. Accurate and detailed characterization of the compromised data.

    1.4. Function of the IRT, work teams, and involving parties during the incident.

102. The incident manager and the CISO will define schedules for dealing with the discrepancies found and will monitor and control their implementation.

103. The incident manager will formulate an official incident report that will summarize all incident aspects including -

    103.1. Forensics investigation;

    103.2. Containment and recovery actions;

    103.3. Legal and regulatory aspects;

    103.4. Business impact of the attack;

    103.5. Financial losses from the attack.

Final Wrap

104. The Cyber Crisis Readiness Methodology described in this document represents the distillation of tens of cyber simulations carried out with maritime entities, as well as expertise developed in the course of providing cybersecurity consulting services to a wide diversity of companies in the maritime sector and other sectors.

105. The Methodology has been tailored to the needs of marine ports and port terminals in times of cyber crisis. Yet there are other types of companies and organizations in the marine sector, such as shipping companies, for which parts may be relevant or readily adaptable.

106. Each entity using this Methodology will likely find the need to make adaptations to its own particular organizational priorities and cyber risk assessments,

107. The authors of this Methodology have aimed to provide a robust, proven basis for moving ahead with this critical task.

Appendices

Appendix 1 - Operational Timeline Template

Time	Action item	Notes
08:00	Containment and recovery status	Work plan for the coming day
10:00	Forensics and intelligence status	Updating the status of the investigation, new IOCs, associating and characterizing the attack group.
11:00	Monitoring status	Ensure that the monitoring team is in sync with what is happening in the incident and the work processes between the SOC and the organization are working properly.
13:00	Communication and PR status	If possible, reduce the number of statuses and incorporate in management status
14:00	Regulation status	If possible, reduce the number of statuses and incorporate in management status
16:00	Negotiation status	If possible, reduce the number of statuses and incorporate in management status
20:00	Management status	General situation overview with the management, including situational assessment from each work team and coordination of the following tasks.

Appendix 2 - Port Asset Classification

Category	System Name	Asset / Infrastructure Present in the Port (Yes / No)	Criticality to facility operations (1-Low; 5-Very high)	Could facility operate without the asset (Yes / No)	Does the asset have an alternative / Backup (Yes / No)	Is the asset connected to an IT Network (Yes / No)	Does the asset have good cyber protection (Yes / No)	System Owner
Physical Infrastructure - Land	Access or Internal Roads							
Physical Infrastructure - Land	Railway lines							
Physical Infrastructure - Land	Dock lighting							
Physical Infrastructure - Sea	Approach Channel							
Physical Infrastructure - Sea	Navigation lights							
Physical Infrastructure - Container lifting	Fixed cranes							
Physical Infrastructure - Container lifting	Gantry cranes							
Physical Infrastructure - Container lifting	Mobile cranes							

Category	System Name	Asset / Infrastructure Present in the Port (Yes / No)	Criticality to facility operations (1-Low; 5-Very high)	Could facility operate without the asset (Yes / No)	Does the asset have an alternative / Backup (Yes / No)	Is the asset connected to an IT Network (Yes / No)	Does the asset have good cyber protection (Yes / No)	System Owner
Physical Infrastructure - Container lifting	Straddle Carriers/top lifters							
Physical Infrastructure - Container lifting	Vehicles – Other							
Physical Infrastructure - Energy	Locally generated electricity							
Physical Infrastructure - Energy	Mains electrical substation							
Physical Infrastructure - Energy	Hydraulic/ Pneumatic power							
Physical Infrastructure - Buildings	Security/ Operations buildings							
Physical Infrastructure - Buildings	Other Office buildings							
Information System - Security	CCTV Cameras (operations)							
Information System - Operational	Billing							

Category	System Name	Asset / Infrastructure Present in the Port (Yes / No)	Criticality to facility operations (1-Low; 5-Very high)	Could facility operate without the asset (Yes / No)	Does the asset have an alternative / Backup (Yes / No)	Is the asset connected to an IT Network (Yes / No)	Does the asset have good cyber protection (Yes / No)	System Owner
Information System - Operational	Cargo Planning System							
Information System - Operational	Domain Controllers							
Information System - Operational	EDI Systems							
Information System - Operational	**GOS**							
Information System - Operational	Life safety systems							
Information System - Operational	Equipment Management System							
Information System - Operational	**TOS**							
Information System - Operational	TOS Web Portal							
Information System - Operational	VTS/Port Information System							

Category	System Name	Asset / Infrastructure Present in the Port (Yes / No)	Criticality to facility operations (1-Low; 5-Very high)	Could facility operate without the asset (Yes / No)	Does the asset have an alternative / Backup (Yes / No)	Is the asset connected to an IT Network (Yes / No)	Does the asset have good cyber protection (Yes / No)	System Owner
Information System - Operational	Website (Gate Cameras / Vessel Schedule etc)							
Information System - Operational - Cloud based	BAPLIE viewer							
Information System - Operational - Cloud based	NYSA Labor hiring system							
Information System - Operational - Cloud based	Pay the cargo system							
Information System - Operational - Cloud based	Mainpac - inventory management system for equipment and parts							
Information System - Administration	Payroll system							
Information System - Administration	Email System							

Category	System Name	Asset / Infrastructure Present in the Port (Yes / No)	Criticality to facility operations (1-Low; 5-Very high)	Could facility operate without the asset (Yes / No)	Does the asset have an alternative / Backup (Yes / No)	Is the asset connected to an IT Network (Yes / No)	Does the asset have good cyber protection (Yes / No)	System Owner
Information System - Administration	ERP							
Information System - Administration	HR Systems							
ICT Infrastructure	IT Networks							
ICT Infrastructure	Wifi							
ICT Infrastructure	IT Servers							
ICT Infrastructure	Internet access							
ICT Infrastructure	Mobile phones							
ICT Infrastructure	Landline telephone							
ICT Infrastructure	Fax							
ICT Infrastructure	Radar equipment							
ICT Infrastructure	Radio system							
Gate systems	Radiation Detection System							
Gate systems	Weighbridges							
Gate systems	Gate LPR							
Gate systems	Gate OCR							
Gate systems	Gate camera							

Category	System Name	Asset / Infrastructure Present in the Port (Yes / No)	Criticality to facility operations (1-Low; 5-Very high)	Could facility operate without the asset (Yes / No)	Does the asset have an alternative / Backup (Yes / No)	Is the asset connected to an IT Network (Yes / No)	Does the asset have good cyber protection (Yes / No)	System Owner
Information System - Operational	Port Community System							

Appendix 3 - Management status meeting agenda during the cyber crisis

1. Situational assessment.
2. Work teams' update as follow:
   - 2.1. Incident response team
   - 2.2. Communication and PR team
   - 2.3. Legal and regulation.
   - 2.4. Negotiation
   - 2.5. Intelligence
3. Open issues for management decisions.
4. Next steps.
5. Off hours - transition between incident response teams.

Appendix 4 - Legal and regulatory requirements (for the New Jersey port example)

108. Below is an initial list of the five categories of legal and regulatory notifications, as follows: notifications to cybersecurity regulators; notifications to data privacy regulators (on a state-by-state basis, given exposure of PII of residents the relevant state; local law enforcement notifications; federal, regional or international law enforcement bodies, such as the FBI, Interpol and Europol; and contractual notifications, as per the conditions agreed with specific suppliers regarding the obligation to notify of the occurrence of a cyber incident and/or personal data breach.

109. The chart below provides details of each and the relevant considerations to be weighed.

110. Note that, in the US contexts, the Federal Maritime Commission is not relevant during a cyber incident, although it may be relevant for post-incident ramifications of the commercial aspects of the cyber incident's impact.

Regulator / Law Enforcement	Regulatory Framework	Notification required / not required
Coast Guard	Maritime Transportation Security Act of 2002 Coast Guard / DHS Area Maritime Security Plan and contact list Area Maritime Security (AMS) Committees: Established under the direction of the Captain of the Port (COTP) to provide advice and assist the development of the AMS Plan. Among other specified duties, the AMS	Notification to the Area Maritime Security Committee (AMSC) for the Port of New York and New Jersey is not required but recommended. Note: new requirements are currently being developed (check September 2022 potential deadline).

Regulator / Law Enforcement	Regulatory Framework	Notification required / not required
	Committee "**shall serve as a link for communicating threats and changes in MARSEC Levels and disseminating appropriate security information to port stakeholders.** Navigation and Vessel Inspection Circular #09-02, April 19, 2019	
Department of Homeland Security / CISA	DHS National Strategy for Maritime Security, including (from the Maritime Infrastructure Recovery Plan (MIRP)) - p.24. CISA reporting here. During an actual or threatened - Transportation Security Incident (TSI) declared by the Secretary of Homeland Security under the MIRP as a National TSI, federal authorities intervene.	Required only in the case of a national TSI, notification can be made via the AMSC. In such circumstances, DHS is authorized to join the incident management.
Port Authority of New York and New Jersey	https://www.panynj.gov/port-authority/en/help-center/contact-us.html New Jersey Marine Terminals 260 Kellogg Street, Port Newark, NJ 07114 - T: (973) 578-2192 F: (973) 589-5018	Notification to the Port Authority is not required, but recommended. See here.

Regulator / Law Enforcement	Regulatory Framework	Notification required / not required
Notifications to data privacy regulators (on a state-by-state basis where personal private information (PII) is impacted by the cyber incident (there is at present no requirement for notification at the federal level in the United States).	New Jersey example (N.J. Stat. § 56:8-161 et seq.): "Any Entity to which the statute applies **shall disclose any breach of security of computerized records following discovery or notification of the breach to any customer who is a resident of NJ whose PI was, or is reasonably believed to have been, accessed** by an unauthorized person....Disclosure of a breach of security to a customer shall not be required if the Entity establishes that misuse of the information is not reasonably possible. Any determination shall be documented in writing and retained for 5 years." **The above notification must be made "in the most expedient time possible and without unreasonable delay**, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system." In the wake of the exposure of PII, the data privacy law may also require that the organization notify consumer reporting agencies and police authorities. **This is the case for PII of New Jersey residents.**	The port may outsource these PII notifications to external legal counsel.

Regulator / Law Enforcement	Regulatory Framework	Notification required / not required
Law enforcement -Port Authority Police Department	1- 800-828-7273 or 1-201-239-3500	Examine whether required by insurance policy.
Law enforcement - FBI	Not required, complaint may be submitted to FBI's Internet Crime Complaint Center	Relevant especially for Ransomware incidents, in order to share information about ransomware attackers and potentially receive FBI assistance.
Contractual notifications	As required.	Critical contractors may need to be notified as a contractual / business matter.

Appendix 5 - Selected background documents

Date	Title	Author(s)	Link
November 2021	Cybersecurity Incident & Vulnerability Response Playbooks: Operational Procedures for Planning and Conducting Cybersecurity Incident and Vulnerability Response Activities in FCEB Information Systems	Cybersecurity and Infrastructure Security Agency	https://www.cisa.gov/sites/default/files/publications/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf
January 29, 2021	A Conceptual Cyber-Risk Assessment of Port Infrastructure	Kimberly Tam	https://pearl.plymouth.ac.uk/handle/10026.1/16704
2020 (revised)	Good Practice Guide: Cybersecurity for Ports and Port Systems	The Institution of Engineering and Technology, Department of Transport, United Kingdom	https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/859925/cyber-security-for-ports-and-port-systems-code-of-practice.pdf
2020	DCSA Implementation Guide for Cyber Security on Vessels v1.0	Digital Container Shipping Association	https://dcsa.org/wp-content/uploads/2020/03/DC

Date	Title	Author(s)	Link
			SA-Implementation-Guideline-for-BIMCO-Compliant-Cyber-Security-on-Vessels-v1.0.pdf
2020	Area Maritime Security Committee - Annual Report	Coast Guard	https://www.dco.uscg.mil/Portals/9/CG-FAC/Documents/AMSC%20Consolidated%20reports/2020%20AMSC%20Consolidated%20Report%20(signed).pdf?ver=GoScBvAV6FgPrrhAvkMsAA%3d%3d
March 25, 2020	NVIC 01-20, Guidelines for Addressing Cyber Risks at MTSA Regulated Facilities	US Coast Guard	https://mariners.coastguard.blog/2020/03/25/nvic-01-20-guidelines-for-addressing-cyber-risks-at-mtsa-regulated-facilities/
February 26, 2020	NAVIGATION AND VESSEL INSPECTION CIRCULAR NO. 01-20	US Coast Guard / DHS	https://www.dco.uscg.mil/Portals/9/DCO%20Docum

Date	Title	Author(s)	Link
	Guidelines for Addressing Cyber Risks at MTSA Regulated Facilities		ents/5p/5ps/NVIC/2020/NVIC_01-20_CyberRisk_dtd_2020-02-26.pdf?ver=2020-03-19-071814-023
April 19, 2019	NAVIGATION AND VESSEL INSPECTION CIRCULAR NO. 09-02, Change 5 Guidelines for the Area Maritime Security Committees and Area Maritime Security Plans Required for US Ports - Change #5	US Coast Guard / DHS	https://www.dco.uscg.mil/Portals/9/DCO%20Documents/5p/5ps/NVIC/2002/09-02_Ch5.pdf
April 19, 2019	Cyber Incident Response Plan Template - Incident Reporting and Handling Requirements	US Coast Guard / DHS	@ pp. 175-178 (#3400)

Appendix 6- Ransom payment considerations

Type of risk / aspects	Without ransom payment	With ransom payment
Estimated time to return the port's business activities		
The level of risk that the attacker could use tools that may still be in the port's network		
Estimated financial damage		
Regulatory and legal aspects		
Reputation aspects		
Estimated level of risk from potential data leakage		

Appendix 7 - Incident Response Contact List Template

Company / Organization	Role	Contact Person	Contact Email	Contact Phone
Crisis Management Company	Ongoing incident management			
Police	Filing a complaint			
Privacy Authority	Personal data breach notification			
Threat intelligence Company				
Ransomware negotiator				
PR	PR			
External legal advisors	Legal claims, data privacy regulatory notifications			
Cyber insurance carrier	Insurance coverage, required notifications, forensics team,			

Company / Organization	Role	Contact Person	Contact Email	Contact Phone
	negotiation team			

Appendix 8 - HR and Public Relations Sample Communications

Stakeholder >	EMPLOYEES
Responsible for notification	HR, Legal
First stage of cyber incident	Greetings, We are contacting you to update that over the past few days, we have identified a security incident in some of the [company] computer systems. We immediately took a number of measures to reduce the impact of the incident on the port's operations, including disconnecting from certain operations, and proactively suspending certain computer operations. The handling of the incident is being done in a gradual and planned manner, in order to minimize any influence on our work and to safeguard [company] employees, as well as the relationship with our customers. In addition, we have notified the relevant authorities and we are working closely with law enforcement bodies and a leading team of experts and in coordination with our insurance company, in order to address these issues and restore the affected systems safely and as soon as possible. At this stage, there is no assessment of the actual impact on [company] systems. Until the situation is clarified and we can update on further developments, we thank you for your dedication to your work and appreciate your understanding that reality requires all of us to be flexible in order to maintain a high level of professionalism and customer service. With appreciation,

Stakeholder >	**EMPLOYEES**
	[signed- senior management]
Second stage	
Follow-up after incident has concluded	

Stakeholder >	**CUSTOMERS**
Responsible for notification	Business units, Legal, PR
First stage of cyber incident	Dear [name of customer], We are writing to inform you of a security incident at [company]. We recently identified suspicious activity in our computer systems, and immediately began an investigation with the help of an expert IT / OT forensics firm, as well as contacting the relevant regulators and law enforcement. Our investigation is ongoing, but we have determined that, on or about [date], an unauthorized third party gained access to certain information in our systems. We are taking several steps to protect you and your data. These include blocking the unauthorized party from our systems, temporary shutdown of certain systems until they can be safely rebooted, and the temporary suspension of some of our digital customer services. We will update with further information when relevant. If you have any other questions, or you need further assistance, please call XXX-XXX-XXXX.

Stakeholder >	CUSTOMERS
	Thank you, [name] [Chief Information Security Officer OR Business Contact]
Second stage	
Follow-up after incident has concluded	

Stakeholder >	Suppliers
Responsible for notification	Business units, Legal, PR
First stage of cyber incident	Dear [name of supplier], We are writing to inform you of a security incident at [company]. We recently identified suspicious activity in our computer systems, and immediately began an investigation with the help of an expert IT / OT forensics firm, as well as contacting the relevant regulators and law enforcement. Our investigation is ongoing, but we have determined that, on or about [date], an unauthorized third party gained access to certain information in our systems. Our business relationship is extremely important to us, and we are taking several steps to protect you and your data. These include blocking the unauthorized party from our systems, temporary shutdown of certain systems until they can be safely rebooted, and the temporary suspension of some of our digital customer services.

Stakeholder >	**Suppliers**
	We will update with further information when relevant. If you have any other questions, or you need further assistance, please be in touch with me directly.. Sincerely, [Primary business contact]
Second stage	
Follow-up after incident has concluded	

Stakeholder >	**General public**
Responsible for notification	PR, Legal, CEO
First stage of cyber incident	{Company] today announced that its IT / OT security systems identified a security incident on some of its systems, as a result of a cyber incident. As a preventive measure, operation of certain of its servers was halted, and some operations have been proactively suspended. This has been done in a gradual, organized manner, to minimize any disruptions to relations with its customers and suppliers. In addition, [company] has notified relevant authorities and is working closely with law enforcement organizations and with a leading team of experts, coordinated with its insurance providers, in order to address these issues and safely recover the

Stakeholder >	General public
	impacted systems as soon as possible. [Company] is implementing specific measures to prevent the expansion of this incident. At this point there is no assessment as to the actual effect on [company], nor its customers.
Second stage	
Follow-up after incident has concluded	

Appendix 9 - Sample Q&A for cyber incidents where personal data hasn't been breached

What has happened?

On [date], [company]'s monitoring systems identified that it was experiencing a cyber incident. After an initial inquiry into the matter, we formulated as quickly as possible the pattern of action necessary for the next steps in dealing safely and rapidly with the incident. In doing so, [Company] has hired the services of top-notch cyber experts specializing in cyber incident management, forensic research, intelligence research and crisis management. These teams have been working continuously since the discovery of the incident with the aim of minimizing its effects.

So far, the extent of these effects is still being clarified. We are conducting an in-depth analysis of the scope of the incident, its cause, the extent of the damage, and taking action to return to a quick return to full business activity.

We ask that [company] employees, customers and the general public to rely solely on the official announcements published on behalf of the company.

What has been affected so far?

Most of [company]'s activities are continuing to operate fully. There may be some limitations on certain operations, such as [add examples]. No payment systems have been affected, nor has personal data of customers been damaged, to the best of our understanding at the present time. All of the [company] customer service centers are available and active 24/7, at -----[add #].

Who are the attackers?

The ----- group has been in touch with [company] with a ransomware request. This group of cyber attackers is well-known, and according to the Federal Bureau of Investigation (FBI), ----- has attacked hundreds of companies in recent months.

Has any personal data of customers been leaked? If so - how much?

At present, we have not identified any personal data that has been leaked. Should this situation change, [company] will update regarding the changes and cooperate fully with the relevant regulatory authorities.

I'm a [company] customer - how can I find out if my personal data has been affected?

As of this moment, we do not have information about any leaked personal data (please see above, under "Has any personal data of customers been leaked?"). If this situation changes, please be sure that we will immediately take action to minimize the effects of any such leakage. [Please note that we do not hold any of your credit card or financial information.] We take ongoing measures to protect the personal data of our customers and suppliers, in conformity with applicable data privacy laws. You may contact us for more information at: * XXXX.

Do I need to cancel my credit card used for purchases with the Company?

No. As noted above, [company] does not retain any of your credit card or financial information.

What's being done to deal with the impact on [company], its customers, and its employees?

We implement measures to protect our computer systems and their data on an ongoing basis, subject to applicable laws and regulations. We are already engaged with responding to the cyber incident, together with top-notch cyber experts specializing in cyber incident management, forensic research, intelligence research and crisis management; who have been working with us continuously since the discovery of the incident with the aim of minimizing its effects. Employees, customers, and suppliers have been informed of the incident, and we have opened our customer service lines to respond to any questions.

The focus of the [company] management team is to take all actions in order to return to a safe and quick return to full business activity.

FOR ANY QUESTIONS, PLEASE CALL US AT *XXXX.

Disclaimer

This document was prepared within the framework of the agreement signed between ZK Cyberstar Ltd. ("Cyberstar") and __________. ("the Company") on__________ (the "Agreement"), and it constitutes part of the implementation of the Agreement by Cyberstar. For the avoidance of doubt, the disclaimers contained in the Agreement also apply to this Report.

This Methodology is addressed solely to whom it was shared with and may not in any respect be relied upon by, published, communicated, disclosed to or filed with any other person or entity without Cyberstar's prior written consent. It was prepared, *inter alia*, by request of the Company's legal advisers, in preparation for potential legal and/or regulatory proceedings; and/or the handling of existing regulatory and/or legal proceedings.

The methodology was prepared on the basis of the information known to Cyberstar the date of its commencing the work pursuant to the Agreement, and up to the date of this document's submission to the Company.

*****END OF DOCUMENT*****