Red Teaming Analysis of a Catastrophic Cyber Attack on Critical Infrastructure
An Expert Panel Discussion

PART 2

MARCH | 2023

Catastrophe and Climate

SOA Research INSTITUTE

Red Teaming Analysis of a Catastrophic Cyber Attack on Critical Infrastructure

An Expert Panel Discussion

AUTHORS   Unal Tatar, PhD
Brian Nussbaum, PhD
Omer F. Keskin, PhD
Doug Clifford
Elisabeth Dubois, MBA, PMP
Dominick Foti, MBA
Brianna Bace
Rian Davis

Give us your feedback! Take a short survey on this report. Click Here

SOA Research INSTITUTE

CONTENTS

Red Teaming Analysis of a Catastrophic Cyber Attack on Critical Infrastructure

An Expert Panel Discussion

Executive Summary

With the expansion of cyber threats, the ability for a catastrophic event impacting organizations and government grows. Cyber incidents are causing increasing financial, operational, and reputational losses to entities worldwide. Given this, there is a need to manage catastrophic cyber risks using validated methods, to determine the implications such risks have for insurance companies, reinsurers, regulators, government, consumers, and society.

This report is the second output of a series of four multi-disciplinary panel discussions that employs red teaming techniques to gather insights from a diverse set of experts regarding evolving catastrophic cyber risks and how to plan ahead, mitigate, and respond to them.

The objectives of this panel discussion were to:

- Elicit and synthesize insights from experts on the potential impacts a catastrophic cyber attack targeting a critical infrastructure (CI) sector would have on the insurance industry, economy, and the nation.

- Further develop red teaming techniques for catastrophic cyber risks to better grasp the impact of the catastrophic cyber event on stakeholders, initial concerns following an incident, and information sharing and collaboration needs.

Using the red teaming methodology, this report conducts a series of tabletop exercises and related debriefings on a scenario impacting CI. The participating experts were split into three groups – Insurance industry, CI, and Government – to discuss the cyber incident in the eyes of that particular stakeholder. There were three areas that the discussions of each group covered, including an analysis of the impact of the catastrophic cyber event, initial concerns and responses, and information sharing and collaboration needs among various stakeholders.

Findings of the discussions include insights regarding the impact of the incident, concerns, and communication channels. The impacts discussed by panelists largely centered around financial impacts caused by an accrual of losses and the legal consequences of a ransom payment. Overall, the insurers would be impacted by costs associated with the ransom payment, hiring breach coaching, Information Technology (IT) forensics vendors, notification costs, and business interruption losses including the mass ripple effects the attack would have throughout the U.S. population due to its impact on the supply chain. The participants also highlighted the importance of communication in the aftermath of such a catastrophic cyber incident.

Based on the findings of this report and expert feedback, another red teaming exercise will be established which will be disseminated with the third report of the series. The remainder of this document provides further details of the panel's discussion on these topics.

Section 1: Introduction

The growing catastrophic risks that an entire town, country, or even world may face due to cyber-attacks can severely impact technological infrastructure, public health and safety, economic security, and political stability.[1] According to the first report of the series, catastrophic cyber risks are the risks that impact "the quality of life for a large number of people, impacts the confidentially, integrity, and availability of information, or causes a wide-scale business interruption"[2]. Yet, it emphasizes that despite several definitions of catastrophic cyber risk, there is no one size fits all solution. Catastrophic cyber risks are critical since it is challenging to calculate the likelihood and consequences as opposed to traditional risk events the insurance companies are used to handling. A disruption in the critical infrastructure (CI) sectors, such as the power grid or communication, can highly affect many other sectors because of the interdependency of the CI systems and can lead to a catastrophic incident. By considering all these aspects of catastrophic cyber risks, a multi-disciplinary approach is necessary to handle them.

Given the need for a multi-disciplinary approach to cyber risks, expert opinions are needed from the insurance industry, government, private sector, and academia. The purpose of this project is to conduct a series of multi-disciplinary panel discussions by employing the red teaming technique to derive and analyze feedback from a diverse set of experts regarding the current and evolving catastrophic cyber risks and how to mitigate them. This report serves as the second deliverable of a series of four, eliciting discussions on the likelihood and consequences of a potential catastrophic cyber incident to CI, how to mitigate it, and how it might evolve. The first report, using the discussion from an October 2022 meeting, developed an outline for future red teaming exercises and sought to synthesize the definitions of catastrophic cyber risk, how catastrophic risks are handled, and catastrophic cyber risk scenarios.[3] On January 12th, 2023, the project research team, with the support of the Society of Actuaries (SOA) Research Institute, gathered a similar panel of experts to elicit information via a red teaming scenario aimed at a cyber event impacting CI.

Participants were selected based on their professional or academic backgrounds in cybersecurity risk management in an actuarial or insurance context, with a reliance on several experts from the first report. Sixteen experts participated, representing actuarial sciences, the insurance industry, the risk management domain, the cybersecurity domain, and academia. The panel discussion was conducted on Zoom. The current report uses the red teaming methodology which is a combination of small tabletop exercises and related debriefings for selected scenarios. The panelists were split into three groups –an Insurance Company, the Critical Infrastructure Sector, and Government, each of which was sent to separate breakout rooms to discuss the questions at hand within smaller groups. For the final section, panelists participated in a plenary session.

The objective of this panel discussion was to answer the question: "*What are the potential impacts of catastrophic cyber attacks targeting a CI sector would have on the insurance industry, economy, and the nation?*" Within this, several research questions regarding a catastrophic cyber incident targeting CI were stipulated:

- What would be the impact of a catastrophic cyber incident targeting a CI sector?

---

[1] Ruffle, S. J., Bowman, G., Caccioli, F., Coburn, A. W., Kelly, S., Leslie, B., & Ralph, D. (2014). *Stress Test Scenario: Sybil Logic Bomb Cyber Catastrophe* (Cambridge Risk Framework, p. 45). Centre for Risk Studies - University of Cambridge. https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/crs-sybil-logic-bomb-cyber-catastrophe-stress-test.pdf

[2] Tatar, U., Nussbaum, B., Keskin, O. F., Dubois, E. V., & Foti, D. (2022). *Setting the Scene: Framing Catastrophic Cyber Risk An Expert Panel Discussion (Catastrophic Cyber Risk: An Expert Panel Discussion Series). Society of Actuaries.* https://www.soa.org/resources/research-reports/2023/cat-cyber-risk/

[3] Tatar, U., Nussbaum, B., Keskin, O. F., Dubois, E. V., & Foti, D. (2022). *Setting the Scene: Framing Catastrophic Cyber Risk An Expert Panel Discussion (Catastrophic Cyber Risk: An Expert Panel Discussion Series). Society of Actuaries.* https://www.soa.org/resources/research-reports/2023/cat-cyber-risk/

- What are the initial concerns and responses of the insurance industry, government agencies, and private sector in responding to a catastrophic cyber incident?

- How could public and private sector stakeholders collaborate to respond to a catastrophic cyber incident?

- What role would the insurance industry play in mitigating the effects of a catastrophic risk event affecting a CI sector?

This document summarizes the methodology and discussion that occurred during the two-hour expert panel. To encourage openness during the discussion, the facilitators assured the participants that this report would not attribute comments to individuals or companies, so no names appear in the body of the report. The names of those who participated are included in the Acknowledgements Section of the report.

Section 2: Methodology

2.1 RED TEAMING

This project adopts the methodology of red teaming, commonly used in policy and security circles, to think about catastrophic cyber risks. Red teaming is defined as "the simulation of adversary decisions or behaviors, where outputs are measured and utilized for the purpose of informing or improving defensive capabilities."[4] While red teaming is based on adversarial hazards and focuses on defensive measures,[5] it is easily adapted to broader risk management questions when dealing with adversarial actors – as is often the case in cybersecurity. There are myriad cybersecurity-related risks, some adversarial (involving an opponent or bad actor) and some non-adversarial (from part failures to natural disasters). While the non-adversarial risks are certainly challenging, engineering robustness and resilience to such risks are a normal part of the creation and adoption of most computer technology. It is the endlessly complex and strategically changing adversarial threats that are often the hardest to mitigate the risks of. Cybersecurity pioneer Dan Geer has said that cybersecurity "is the most difficult intellectual occupation on the planet as we have the dual challenges of rapid change and sentient opponents."[6] The adversarial nature of cybersecurity threats and the disproportionate percentage of catastrophic cyber threats that are tied to adversaries – whether criminals, hacktivists, nation-state espionage, or military attacks – make red teaming a natural fit for the problem.

There are many types of red teaming approaches laid out by the University at Albany's Center for Advanced Red Teaming (CART)[7] in their Red Teaming Radar – including penetration testing, tabletop exercises, field exercises, computational exercises, and functional exercises.[8] CART develops and employs new methodologies to assist a variety of sponsors in designing, conducting, and evaluating Red Teaming exercises. CART has done work using these methodologies with various the Department of Defense (DoD), the Department of Homeland Security (DHS), U.S. State Department, and industry partners. Given the topic of these expert panel elicitations, the best-fit approach is a combination of small tabletop exercises and related debriefings. A tabletop exercise is a "simulation, usually

---

[4] Ackerman, G. A., & Clifford, D. (2019). *Towards a Definition of Red Teaming*. Center for Advanced Red Teaming, University at Albany. https://www.albany.edu/sites/default/files/2019-11/CART%20Definition.pdf

[5] Longbine, D. F. (2008). *Red Teaming: Past and Present* (p. 89) [School of Advanced Military Studies Monograph]. United States Army Command and General Staff College. https://apps.dtic.mil/sti/pdfs/ADA485514.pdf

[6] Greer, D. (2015, May). *Driven by Data*. LangSec Conference. http://spw15.langsec.org/geer.langsec.21v15.txt

[7] For more information about the Center for Advanced Red Teaming (CART) and Red Teaming in general, visit the website at: https://www.albany.edu/cehc/cart

[8] The Center for Advanced Red Teaming. (2021). *Red Teaming Radar*. University at Albany. https://www.albany.edu/sites/default/files/2019-11/CART%20Infographic%20Radar.pdf

facilitated, based on structured discussion"[9] and designed to use scenarios and "injects" (fictional events or developments) to structure a discussion about how risk management processes might play out. In this case, a series of small tabletop exercises based on major adversarial classes – ransomware operators, nation-state APT attackers, insider threats at a large platform company – could be used to elicit, from the experts, ideas about how traditional "day-to-day" cyber risks could escalate or cascade to become catastrophic cyber risks. These facilitated exercises and the subsequent debriefings and structured discussions, enable these experts to engage with scenarios and their implications beyond what would be possible in traditional brainstorming approaches. The fundamental goal of this approach is to leverage the combined expertise of the panelists as well as the unique insights of the project team to provide insights into catastrophic cyber risks that neither side would be likely attained on their own.

The two-hour tabletop exercise conducted, was based on scenarios and topics elicited in meeting one, which involved soliciting key questions and areas of concern, as well as important drivers and shapers of cyber risk.[10]

2.2 SCENARIO & INJECTS

The exercise was created similar to a developing cyber event, where participants are expected to respond to a core scenario, after which they were given with two distinct injects that escalated the severity and catastrophic nature of the event. The core scenario was provided as a read-ahead scenario, highlighting a cyber event impacting a United States (US) CI. The injects built on the initial cyber event creating a larger threat and a greater impact. The scenario and injects are briefly discussed below and provided in-depth in the Appendix A: Core Scenario Read Ahead.

2.2.1   EXERCISE CREATION

The scenario for the tabletop exercise is shaped based on the inputs of the experts in the first expert panel meeting regarding the definition of catastrophic cyber incidents. The scenario is meant to be a high-impact and low-probability but plausible cyber incident against critical infrastructure. The transportation sector was selected to be the main target of the scenario due to its importance for many other sectors and to expect ripple effects. Ports play an important role in importing products for the retail sector, parts and materials needed for the manufacturing sector, and exporting goods and energy resources. Considering such dependencies, disruption of operations of multiple ports throughout the United States would create a catastrophic cyber risk scenario. While creating the scenario, historical cyber incidents[11], hurricane impact[12], similar hypothetical cyber attack scenarios[13,14], data

---

[9] The Center for Advanced Red Teaming. (2021). *Red Teaming Radar*. University at Albany. https://www.albany.edu/sites/default/files/2019-11/CART%20Infographic%20Radar.pdf

[10] Tatar, U., Nussbaum, B., Keskin, O. F., Dubois, E. V., & Foti, D. (2022). *Setting the Scene: Framing Catastrophic Cyber Risk An Expert Panel Discussion (Catastrophic Cyber Risk: An Expert Panel Discussion Series). Society of Actuaries.* https://www.soa.org/resources/research-reports/2023/cat-cyber-risk/

[11] Longbine, D. F. (2008). *Red Teaming: Past and Present* (p. 89) [School of Advanced Military Studies Monograph]. United States Army Command and General Staff College. https://apps.dtic.mil/sti/pdfs/ADA485514.pdf

[12] Timmons, H. (2017, August 31). *Houston's vital port will reopen on Friday, after being mostly spared by Hurricane Harvey*. Quartz. https://qz.com/1067032/hurricane-harvey-the-port-of-houston-is-reopening-after-being-spared-by-the-storm/

[13] Cambridge Centre for Risk Studies, Lloyd's of London, & Nanyang Technological University. (2019). *Bashe Attack: Global Infection by Contagious Malware* (CyRiM Report 2019).

[14] Lloyd's of London, Cambridge Centre for Risk Studies, & Nanyang Technological University. (2019). *Shen attack Cyber risk in Asia Pacific ports* (CyRiM Report 2019).

sources regarding the operations of ports[15,16,17,18,19], and other relevant documents by the government and other organizations[20,21] were utilized to have a realistic scenario to analyze.

The initial scenario starts with the ransomware attack against the cargo tracking software of four major ports of the US, two largest ports on the west coast, and two moderate-capacity ports on the east coast.[22] The capacity of the container ports is measured by the annual container throughput using the Twenty-foot Equivalent Unit (TEU). The ransomware attack in the scenario targets only the container ports. On the other hand, the major weather event targets another port, the Port of Houston, which is not the largest container port in the US, however, considering the other types of ports in the area, including energy transportation, this port is the second largest by tonnage.[23] The estimates for the duration of downtime are based on historical events, port capacity, and the recovery strategy. The initial loss estimates for the scenario are conducted based on the methodology provided by Lloyd's of London et al.[24] and adapting for the capacity, downtimes, and characteristics of the ports affected. Figure 1 provides a synopsis of the inputs provided to the panelists with each phase of the scenario.

Figure 1
SUMMARY OF INPUTS IN THE CORE SCENARIO AND TWO INJECTS

Core Scenario
- Attack against 4 major ports
- Ransomware – Cargo tracking system
- Operation shutdown

Inject 1
- MT ISAC Bulletin
- Ransomware: 2 more ports
- Hurricane landfall – Port of Houston is closed

Inject 2
- Albany Herald Post Article
- 5 Ports paid the ransom
- Nation-state backed

2.2.2 CORE SCENARIO

On Monday, September 18th, 2023, a ransomware attack hits the cargo management and tracking systems of four major U.S. ports. This attack caused a complete shutdown of operations of the Port of Los Angeles, Port of Long

[15] Lloyd's List. (2022). *One Hundred Ports 2022*. https://lloydslist.maritimeintelligence.informa.com/-/media/lloyds-list/images/top-100-ports-2022/top100ports2022_ebook.pdf?rev=bc3fa2a77e134864bcc7dde4518e07d9&hash=D54445A74F150E76C09174D21AB1ABA5

[16] United States Department of Transportation. Bureau of Transportation Statistics. (2022). *2022 Port Performance Freight Statistics Program: Supply-Chain Feature*. Not Available. https://rosap.ntl.bts.gov/view/dot/59826

[17] U.S. Energy Information Administration (EIA). (2022, June 8). *Coal imports and exports*. https://www.eia.gov/energyexplained/coal/imports-and-exports.php

[18] U.S. Energy Information Administration (EIA). (2022, November 2). *Oil imports and exports*. https://www.eia.gov/energyexplained/oil-and-petroleum-products/imports-and-exports.php

[19] Verschuur, J., Koks, E. E., & Hall, J. W. (2022). Ports' criticality in international trade and global supply-chains. *Nature Communications*, *13*(1), Article 1. https://doi.org/10.1038/s41467-022-32070-0

[20] American Property Casualty Insurance, Association The Council of Insurance Agents and Brokers, CyberAcuView, & The Wholesale & Specialty Insurance Association. (2022). *Re: Potential Federal Insurance Response to Catastrophic Cyber Incidents*.

[21] US Government Accountability Office. (2022). *Cyber Insurance: Action Needed to Assess Potential Federal Response to Catastrophic Attacks* (GAO-22-104256; Report to Congressional Committees).

[22] Lloyd's List. (2022). *One Hundred Ports 2022*. https://lloydslist.maritimeintelligence.informa.com/-/media/lloyds-list/images/top-100-ports-2022/top100ports2022_ebook.pdf?rev=bc3fa2a77e134864bcc7dde4518e07d9&hash=D54445A74F150E76C09174D21AB1ABA5

[23] Timmons, H. (2017, August 31). *Houston's vital port will reopen on Friday, after being mostly spared by Hurricane Harvey*. Quartz. https://qz.com/1067032/hurricane-harvey-the-port-of-houston-is-reopening-after-being-spared-by-the-storm/
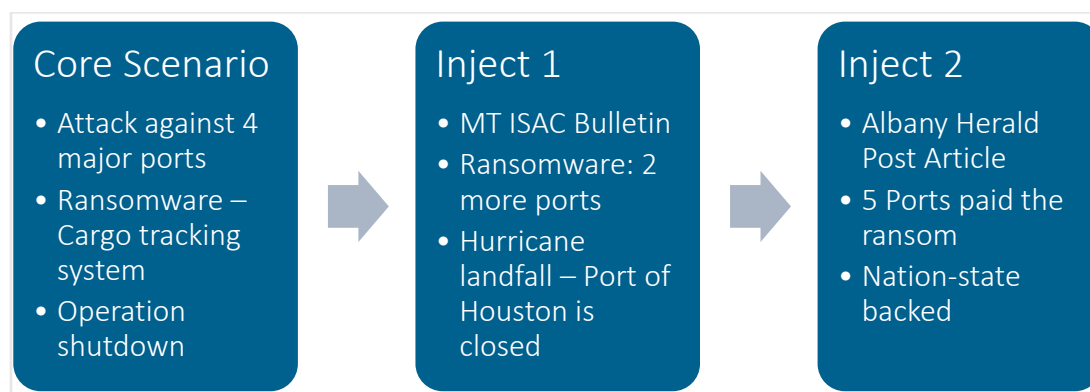
[24] Lloyd's of London, Cambridge Centre for Risk Studies, & Nanyang Technological University. (2019). *Shen attack Cyber risk in Asia Pacific ports* (CyRiM Report 2019).

Beach, Port of Savannah, and Port of Charleston. The port authorities are attempting to regain control of the ports in question. The actor #CyberPirates has taken credit for the attack. The immediate impacts of this attack are supply chain disruption, economic losses, and reputational damage. According to current reports, there is a hurricane approaching the Port of Houston.

2.2.2   INJECT 1: IMPACT INCREASES WITH NON-CYBER DISASTER

The first inject came as a Marine Transportation (MT) Information Sharing and Analysis Center (ISAC) Bulletin. The bulletin shared how two additional ports were attacked, and the remaining ports were still vulnerable to an attack. The Port of Virginia and the Port of Miami have joined the former four ports in a complete shutdown. It has been determined that the attack originated from a zero-day vulnerability. It is expected that the necessary patch to protect the remaining ports will not be ready for 48 hours. Alongside the cyber-attacks a hurricane hit the Port of Houston, requiring the port to close. The port closures and slowdowns in the retail sector are being seen across the nation. With 1.37% of the annual throughput of containers being transported by vessels, it is approximately a $13.7 billion industry.

2.2.3   INJECT 2: NATION-STATE INVOLVEMENT

The second inject was a newspaper article titled "A Nation-State Backed Attack against U.S. Ports" published by Albany Herald Post. Since the initial attack, two days have passed. The Port of Virginia is busy trying to recover their systems from a backup, while the other ports that were shut down paid the ransom, but still require a week to get back to fully operational. The Port of Houston is still not-operational due to the hurricane. According to U.S. Intelligence, shell companies tied to sanctioned North Korea appear to have shorted U.S. logistics and retail stocks on international exchanges prior to the attack. An investigation is still ongoing regarding the flow of ransom money. There are widespread logistic impacts and ramifications to politics (e.g., retail slowdowns, gas prices, inflation). The impact of the attack attribution on economic recovery could include force majeure or an act of war or a government backstop.

2.3 ROLES & DISCUSSION QUESTIONS

Exercises using a Red Teaming approach can involve a range of different interactions between participants and the exercise mechanics. Due to the purpose of this exercise, the project team developed the core scenario and the adversary (Red) prior to the exercise, rather than have participants play the role of an adaptive adversary and determine Red actions. Each participant was assigned to one of three teams that were required to respond (Blue) to the actions of the adversary. These three teams include (1) a major insurance company, (2) the CI sector, and (3) the Department of Homeland Security (DHS). Each participant was selected to play the role of decision-maker in the specified groups or organizations but was instructed to draw from personal knowledge and experiences. This approach was chosen due to its ability to best elicit the expertise from the participants.

The first group represents the insurance industry. The participants in this group take on the role of leaders within one of the largest insurance companies in the insurance industry that holds 40% of the policies under exposure.

The second group represents the CI sectors under attack. The participants in this group act as an ad hoc crisis response group within the Marine Transportation Information Sharing and Analysis Center (MT-ISAC) including representatives from each port authority (attacked and not attacked), transportation sector associations, and representatives from affected critical infrastructure sectors including transportation, retail, manufacturing, and energy sectors. MT-ISAC promotes and facilitates marine cybersecurity information sharing, awareness, training, and collaboration efforts between private and public sector stakeholders. Our mission is to effectively improve cyber risk management across the entire MT community through effective information sharing for the improved identification, protection, detection, response, and recovery efforts related to cyber risks.

The final group represented the DHS and the U.S. Government. The participants in this group represented leaders in the Cybersecurity and Infrastructure Security Agency (CISA), Federal Emergency Management Agency (FEMA), United States Coast Guard (USCG), and other relevant DHS and government entities.

Based on the outlined scenarios and respective participant roles, the discussion questions that are raised include:

- What impacts will these series of events have on your organization?

- What are the initial concerns?

- What are the initial responses?

- What stakeholders would your organization collaborate with and in what manner? What would you ask or request from them or provide to them for effective incident response and mitigation?

The following section will provide a detailed account of what information was gathered using this approach and the analysis of the impact of and responses to a cyber-attack on CI.

Section 3: Findings

3.1 IMPACT OF CATASTROPHIC CYBER EVENT ON STAKEHOLDERS

3.1.1 INSURERS

The impacts discussed by panelists largely centered around financial impacts caused by an accrual of losses and the legal consequences of a ransom payment. The panelists noted that the aggregation of losses caused by the cyber event and the hurricane at the Port of Houston could threaten the company's solvency and ability to pay on its policies. These impacts could be exacerbated should the company possess several ports and/or port-dependent assets in its portfolio. Assuming that there is a tower of insurance and an insurance broker, discussions will occur to share the risk and further mitigate the impact. Given that the company possesses 40% of market shares, these financial impacts may cascade into the overall market as well, making communication with reinsurance and other carriers on the insurance tower paramount. If the ports involved only have a single line of insurance, the single insurance company will have to take the lead on response and recovery. This presents a risk of insolvency, which the catastrophic impact may make, so the insurance company is unable to pay out the claim.

Following the injects, the insurance group highlights that there will be significant losses beyond the ports. Overall, the insurers would be impacted by costs associated with the ransom payment, hiring breach coaching, IT forensics vendors, notification costs, and business interruption losses. The focus of the insurers will be on minimizing these losses, performing a cost-benefit analysis of potential responses, and formulating a plan to continue port operations.

Breaching the U.S. Department of the Treasury Office of Foreign Assets Control (OFAC) guidelines would also prompt legal consequences, though the panelists noted that it is unlikely the ransom would be paid without coordination with federal authorities. The insurance company could also face class action lawsuits or other forms of litigation from port-dependent businesses, though contingent business interruption (CBI) is unlikely to be triggered in this case.

3.1.2 CRITICAL INFRASTRUCTURE SECTOR

A catastrophic cyber incident against ports would have immense ripple effects on the rest of the transportation sector and other sectors including manufacturing, retail, and public health. This reality has been the main focus of panelists playing the role of critical infrastructure owners in the red-teaming exercise.

When presented with the scenario, the panelists identified that according to loss estimates, business interruption made up about 66% of the losses. It was their opinion that the first order of business is to recover operations at the ports in order to lessen revenue loss. While revenue loss was their primary concern, panelists also recognized that it was important to consider the reputational damage an incident like this would cause, even though it is much harder to calculate. Another further loss item is the contingent business interruption which is about the loss of revenue of the businesses that are dependent on the operation of the ports.

Other immediate thoughts included determining if the ports had a contingency plan, incident response plan, or downtime procedures in place to assist in the recovery, creating a contingent business interruption claim, and gathering information to determine if the attack will spread to other ports.

Following the first inject, it became apparent that this attack was worsening. Panelists began to consider the mass ripple effect the attack would have throughout the U.S. population due to its impact on the supply chain.

3.1.3 GOVERNMENT (DHS)

What became quickly clear to the DHS team was that there was not an obvious consensus on what role (if any) DHS and its components would play in a scenario like the one in the simulation. There were questions about whether the event made it to the level of catastrophic, and according to whose definition - "One person's catastrophic is not another person's catastrophic." There were questions about whether DHS (mainly CISA, but also Coast Guard and other components) had either the capability or authority to actually engage in any response activity, as opposed to coordinating national objectives such as situational awareness, incident triage, and information sharing. One participant referred to DHS as a "trusted broker of information" between entities with authority and specific objectives. There were also questions about how DHS's role would relate to other elements of a federal government response including its connection to a Unified Coordination Group (UCG) at the White House and to the Department of Defense.

3.2 INITIAL CONCERNS & RESPONSE EFFORTS

3.2.1 INSURERS

The panelists in the insurance group indicated that the company's first response would be to establish a war room to assess lines of coverage and policy positions. During this assessment, each port authority's policy will be reviewed to determine the extent of coverage and any potential limitations, particularly when investigating cyber exclusions in non-cyber policies. At the same time, the insurance company should immediately check their portfolio to see if they insure additional ports and if so, provide assistance to those that have yet to be affected to lower the insurers' financial risk and mitigate the risks to the port(s).

The insurance company would also coordinate a common initial breach response, barring any pre-negotiated exclusions allowing ports to name their own breach coaching and IT forensics vendors. Initial investigations will focus on determining how the ransomware was triggered if the encryption can be reversed without ransom payment, and how quickly backups can be brought online. This information may then be utilized in a cost-benefit analysis to determine the best course of action. The panelists noted that the cost of paying the ransom versus business interruption losses would be a major consideration, though ransom payment could not be viewed purely

through this economic lens. Consequences of breaching OFAC guidelines and other war exclusions mean that a legal perspective is also required.

Almost immediately, a reservation of rights will be issued as the company investigates if warranty statements for affected applications allow for a denial of claims. It will also be determined whether or not the port authorities purchased products from security vendors, as third-party systems or IT vendors those entities may provide partial coverage in the case of cyber-attacks.

Though given a loss estimate within the simulation, the panelists agreed that the insurance company would conduct its own modeling. It is stipulated that insurers would have to deal with cyber insurance issues first, then look at the impact on maritime, manufacturing, transportation, etc. contacting reinsurers and/or lawyers based on the model predictions. With a potentially catastrophic amount of loss, mitigation efforts to protect the market and the company's own solvency are critical. This may be achieved through utilizing catastrophe (CAT) bonds and/or reinsurance.

Following initial investigations, senior executives would be concerned with crafting a statement to publicize losses and potential market impacts. Statements may focus on communicating the estimated maximum loss, equity capital, and solvency, how losses will be handled, etc.

Following the first inject, the zero-day status of the vulnerability makes previously discussed application warranties inapplicable. In this case, prompt issuance of coverage is the likely course of action.

Aside from monitoring port systems from a Security Operations Center (SOC) perspective, the company would communicate recommended mitigation efforts to any other ports in its portfolio. Given the lack of an available patch and the potential for the ransomware to spread, the focus will largely center on backing up data.

The insurance company will likely investigate the benefits of adopting non-computer system-dependent operations, such as phone tree methodologies. If the port authorities ran tabletop exercises to develop a Business Continuity Plan (BCP) and/or a Disaster Recovery Plan (DRP) prior to the event, such procedures may have already been developed. Though slower and less efficient, such operations could be used to mitigate business interruption losses.

The panelists also discussed the impacts of the hurricane hitting the Port of Houston, agreeing that associated physical property damage would be considered the proximate cause under first-party property and casualty (P&C) coverages. Though they agreed that there is not a direct relationship between policies associated with the hurricane and the cyber event, concerns were raised over their indirect relationship. It was suggested that the aggregation of losses accrued over such a short period could impact the company's solvency. Complications may also arise if the cyber insurance is handled by one company and the property insurance by another.

Assuming reinsurance carriers stay solvent, the carrier would cover property loss caused by the hurricane. The insurance company would likely be concerned with who the reinsurance carrier is, where they are located, what their capital position is, the reliance of the carrier, and how much loss will rebound onto the company. At this point, the insurance company will have lawyers involved to determine the impact of the hurricane, to understand the war-exclusion guidelines, and to evaluate the ransom payment made to a nation-state.

Though not a primary consideration immediately following the cyber event and hurricane, there would be tangential concerns from the corporate perspective regarding impacts on overall financial markets and company assets. The company could face increased liabilities and pressure on solvency depending on how it invested its assets, especially if many assets include exposures to the ports.

Following the second inject, the panelists indicated concerns over ransom negotiations. Given the catastrophic impact beyond what could be absorbed by the insurance company, it would be likely that the ransom would not

have been paid if the insurer was acting on their own. If they did go ahead and pay the ransom it was emphasized that the parties involved should have negotiated a lower ransom.

Following attribution, legal consequences for breaching war exclusions and OFAC guidelines were a point of focus. Ultimately, panelists determined that payment without prior discussion with federal authorities is unlikely given the potentially catastrophic impacts on the economy. Federal regulators and insurance companies would likely broker discussion through backchannels, potentially reaching an understanding that payment is needed to protect the nation's economic interests.

Assuming that each of the port authorities had separate insurance policies, there would likely be significant retention of these policies that the insured is responsible for. Furthermore, it is improbable that business interruption coverage would be provided at a significant volume, with most insurance companies more likely opting to limit their per-policy exposure. Given that the insurance company holds 40% of the $1.6 billion catastrophic event, it is unlikely that they will face a catastrophe. Most likely any single insurance carrier will not put out coverage anywhere close to the expected losses (e.g., max payout of $25 million). Insurers will look upon the business interruption loss of the event, which may be challenging given the intricacies of ports. As a panelist shares, for a large insurance company, paying the $40 million ransom is not a large financial loss. While every day the ports are closed, they lose millions over what the paid ransom was. Despite the payment of the ransom, those representing insurers share that the costs of paying far exceed the $40 million due to ensuring litigation, forensics, business interruption, etc.

Contingent business interruption (CBI), or when a supply chain dependent business property experiences loss, is also difficult to determine in this case. CBI is generally triggered when an IT vendor supporting an affected network suffers a loss, making it unlikely that a port authority cyberattack would qualify. The insurance company would also need to differentiate if CBI was caused by the hurricane or the cyberattack and which determination is more advantageous. These complications thus necessitate a close analysis of coverage before an extension of any indemnity.

3.2.2 CRITICAL INFRASTRUCTURE SECTOR

The panelists discussed several concerns and responses they had when faced with this scenario. The first concern was determining the extent of the attack. Panelists wanted to know what functions were down at the affected ports, and whether the ports maintained any tracking, screening, or functional capabilities. It is important that the high-risk cargo continues to be tracked.

Panelists also wanted to determine if the ports were all on the same system. If they are on the same system, the next question worth asking is why some ports were affected and not others. Identifying the attack vector would help to answer these questions and provide insight into the ports that are not yet affected.

Another initial concern of the panelists is whether all victim organizations are in the same network of insurance. Although it is mostly the concern of the insurance companies, it also affects how fast the recovery costs are compensated.

Determining the attackers' motives was also of concern to the panelists. An attack of this size could be conducted by a nation-state, or by proxies for a nation-state. Are there secondary motives for attacking the ports? Panelists speculated that the attack could have been launched in order to distract from cargo being properly screened. When dealing with a nation-state attack, it is important to consider implications larger than just economic damage. Panelists also discussed that based on the incoming hurricane, they needed to begin thinking ahead and preparing for the attack to get worse.

Possible recovery strategies included paying the ransom, despite ethical concerns, restoring from back-ups, and rebuilding the whole system if this was in fact a possible and quicker option. And in case of paying the ransom, the ports should definitely negotiate the rate. Panelists also discussed the possibility of rerouting ships and the ability to receive extra expense coverage for doing so.

Following the first inject and the worsening of the scenario, more focus was placed on the idea of paying the ransom and the problems that it may incur. One problem is the probability that the decryption key to be given by the attackers may not work. Another problem would be that even if the decryption key was functional and ports retrieved their data, there is the issue of being able to trust the data due to a possible breach of the integrity of the data by the attackers to cause further damage to the operations. In this situation, recovery time may be underestimated due to the need to implement a manual process to verify information that is usually done by an automated process.

Some of the ports have started using automated equipment to move containers within ports. The recovery process for ports with automation can further suffer from the attack and might require completely different processes as part of the recovery.

Following the second inject, further questions and concerns arose about paying the ransom. Panelists discussed the many considerations the ports should have taken before paying the ransom. These included verifying if their bitcoin broker was approved by their insurance company and determining if their attacker is on the OFAC sanctions list. Regarding the allegations of attribution to a sanctioned state, paying the ransomware brings up new concerns about whether the victims are allowed to pay the ransom. Taking these steps is important for the port authorities to receive a payout from their insurance firm.

Panelists also discussed the role that the act of war exclusion could play in this incident. A catastrophe at this level may fall outside the scope of the MT-ISAC.

3.2.3 GOVERNMENT (DHS)
The panelists representing DHS questioned who owned and operated the ports, and how that would affect the DHS's role. Assuming the ports were owned and operated by states and localities, often through Port Authorities or similar structures, a major question would be whether and/or how those organizations would view DHS's participation in any response.

Another related question, about the ownership of the facilities, was "Who gets the bill?" – whether these incidents and their consequences are ultimately paid for by public or private sector entities, which some felt could influence what role DHS and other federal resources could play in a response. This question of public and private impacts also came up in the definition of catastrophic, with panel members wondering whether events that result in "business interruption" to private companies meet the threshold for catastrophic. Another threshold question that emerged was whether the ransomware attacks alone would have resulted in a federal response, or whether the subsequent hurricane might have been a key factor in raising the level of salience.

3.3 INFORMATION SHARING, COMMUNICATION, & COLLABORATION OF STAKEHOLDERS

3.3.1 INSURERS
Initially, the insurance company would conduct some form of breach coaching and IT Forensics to gain insight into how the ransomware was triggered and to develop response options. Ideally, the insurance company would lead investigations for all affected port authorities and hire one common breach coaching and IT Forensics vendor to best coordinate the response. However, the company would need to investigate the policies of each authority to

determine if any of the policyholders had negotiated the ability to hire their own vendors. Difficulties could also arise should there be disagreement amongst the authorities in terms of their preferred event responses. For instance, while one port authority may prefer to pay the ransom, another may prefer to focus on rebuilding impacted systems.

With the size of the event, the insurance company would want to coordinate breach response with government authorities such as the Federal Bureau of Investigation (FBI) or DHS could be involved in this investigatory stage as well. Given OFAC guidelines, communication with such authorities is necessary to determine the legality of paying the ransom.

The insurance company will reach out to their respective reinsurance companies on their panel to notify them of potential losses as well. Assuming that the company exists within an insurance tower, these losses will also be communicated with other associated carriers and the broker who assembled the tower. If the insurance company was the primary carrier, they would lead investigations, and if not, they would defer to the primary carrier.

One of the immediate concerns would be communicating with any other ports in the insurance company's portfolio about the event and providing instructions for mitigation. Though the panelists expressed this after the first inject, it was noted that this should have been done immediately after learning about the attacks. Communication with the ports would also center around developing a plan to maintain business continuity, drawing from existing BCP and DRP if applicable.

Likewise, from an insurance perspective, it would be important for the ports to run collaborative workshops, where information sharing and coordinated response are of top priority. The insurance company will also communicate potential damages caused by the cyber event and hurricane to their policyholders. However, if cyber insurance and property insurance are handled by different companies, they may face challenges in laying claims or in collaborating on a response.

Following attribution in inject two, there would likely be back-channeled communication between federal regulators and the insurance company to determine how the ransom will be handled. The economic consequences may prompt federal government authorities and the insurance company to reach an understanding that payment of the ransom, regardless of war exclusions, is the best way to mitigate the loss. It is unlikely that the company would go through with paying the ransom without such communication.

The panelists suggested that following such an incident, there may be communication about setting up a cybersecurity backstop to address systemic cyber risk similar to the Terrorism Risk Insurance Act (TRIA) following 9/11. The insurance company's role in setting up such a backstop would be part of an industry-wide response largely focused on lobbying efforts and testimony before Congress. In developing such a policy, it is necessary to maintain some sort of incentivization structure to avoid the promulgation of moral hazards. Without such a structure, it is possible that the importance of cyber hygiene could be minimized or implemented sloppily going forward.

3.3.2 CRITICAL INFRASTRUCTURE SECTOR

The panelists discussed the importance of information sharing, communication, and collaboration with stakeholders, including their lawyers and counsel, the federal government, and their insurance carrier. There was also discussion on bringing in outside experts to help with the incident response and recovery.

Panelists emphasized the importance of speaking with their private counsel before speaking to law enforcement or sharing any information with other ports in order to establish an attorney-client privilege. Though panelists recognized the need to share information and intelligence with other ports, they stressed the need to gain privilege in order to be protected from liability. This, unfortunately, would delay information sharing with the other affected ports until they had met with their lawyers. But after an attack at this scale, the federal government would be

involved right away. Agencies such as CISA and FBI would interfere to scope the attack, prevent its spread, and help victim organizations in any relevant means.

Maersk had been a victim of ransomware in the past.[25] Being a shipping company rather than a port authority, they had a different experience, but it is absolutely relevant. According to the panelists, it certainly would be valuable to have their input regarding the incident response and recovery.

Following the first inject, which informed the panelists of the loss of operation of another port due to a hurricane, there was discussion about the heavy involvement of the federal government during this national catastrophe. Panelists agreed that FEMA would be mobilized to respond to the hurricane and that a White House incident response team would have been created for the ports under attack. It would be important to coordinate with both of these groups throughout the duration of both the cyberattack and the weather event. There was also the question of monetary support from the federal government during the recovery from the cyberattack.

Following the second inject, which informed the panelists of ports paying the ransom, the panelists discussed the need to bring in a lot of experts to get help due to the high chance that anything gets worse with wrong reactions. It includes communicating with the attackers, paying the ransom, and recovering. For example, experts who speak the language of the attackers may be needed for negotiations. Regarding the concerns of possible war exclusion, paying money to a sanctioned country, and even selecting the bitcoin broker to pay the ransom, the victims need to get consent from their insurance companies to become eligible to be reimbursed for the losses. Regarding the OFAC check, the insurance carriers usually depend on the third-party incident response firms rather than internal teams of the victim organizations to investigate whether the attacker is considered a sanctioned entity. The panelists believed that how to bring in all these experts is something that should have been discussed in tabletop exercises by the organizations before they become victims of attacks.

3.3.3 GOVERNMENT (DHS)

The discussion in the DHS group shared that there was likely some kind of disconnect between authorities and capabilities in the realm of cyber response. Panel members largely agreed that the Department of Defense had more capabilities in cyber forensics and incident response than DHS components did, but that there were serious challenges to using those capabilities in such domestic scenarios. Discussions of Defense Support to Civil Authorities (DSCA), whether and how DoD and DHS might coordinate or compete in such an event, and the role of resources like National Guard cyber teams and FEMA's capabilities in responding to the hurricane component of the event all included questions of authorities and capabilities and how those might be leveraged in response.

One area that there was some consensus about, in terms of DHS's role, was that they would likely be central to planning and coordinating efforts for recovery (rather than response per se). This would include coordinating with public and private sector partners to help manage the logistical problems stemming from port closures and delays, manage "Public Relations (PR)" and public sentiment associated with the event, as well as doing things like coordinating with neighbors Mexico and Canada to help manage cross border land transportation as ports in the United States slowly work their way out of the snarls and tangles resulting from these port interruptions.

---

[25] Greenberg, A. (2018, August 22). The Untold Story of NotPetya, the Most Devastating Cyberattack in History. *Wired*. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Section 4: Acknowledgements

The authors' deepest gratitude goes to those without whose efforts this project could not have come to fruition: the volunteers who generously shared their wisdom, insights, advice, guidance, and arm's-length review of this study prior to publication. Any opinions expressed may not reflect their opinions nor those of their employers. Any errors belong to the authors alone.

Expert Panel Participants:

Seth Baum, Global Catastrophic Risk Institute

Michael Bean, Canadian Institute of Actuaries

Nicole Becher, Google

Kenneth Crowther, Xylem

Gregory Falco, Johns Hopkins University

Ben Goodman, 4A Security and Compliance

Tyler Moore, University of Tulsa

Norman Niami, American Academy of Actuaries

Reid Putnam, Gregory & Appel Insurance

Sasha Romanosky, RAND Corporation

Marc Schein, Marsh McLennan

Scott Stransky, Marsh McLennan

Jeremy Straub, North Dakota State University

Maochao Xu, Illinois State University

At the Society of Actuaries Research Institute:

Rob Montgomery, ASA, MAAA, FLMI, Consultant -Research Project Manager

Facilitators at the University at Albany:

Unal Tatar, PhD, Assistant Professor

Brian Nussbaum, PhD, Associate Professor

Omer F. Keskin, PhD, Assistant Professor

Doug Clifford, Program Manager of CART

Elisabeth Dubois, MBA, PMP

Dominick Foti, MBA

Brianna Bace

Rian Davis

Appendix A: Core Scenario Read Ahead

Red Teaming for Insurance and Critical Infrastructure Sector

Scenario Read Ahead

Cyber Attacks Hit 4 Major Ports

Monday, September 18th, 2023, 12pm

On Monday, September 18th, 2023, at 10.30 am EDT, a cyber-attack simultaneously hit four of the ten largest ports in the United States. A ransomware attack has targeted the Port of Los Angeles, Port of Long Beach, Port of Savannah, and Port of Charleston, causing a complete shutdown of operations at all four ports. The cybercriminal group responsible for the attack, #CyberPirates, has encrypted the data and files of the port systems. Without the data essential for cargo management and tracking systems, it is impossible for port workers to track the contents, location, or destination of any of the containers at the ports. Containers and manifests must be visually inspected and hand scanned. The ransomware attack has brought the operations of the ports to a complete halt, causing chaos and confusion. Incoming vessels are anchored offshore, and trucks are backed up for miles as they wait to enter the ports. The port authorities are attempting to regain control of the situation and find a solution to the ransomware attack.

Immediate Impacts

The immediate impacts of the incident include:

- Supply Chain Disruption: Delayed delivery of goods to downstream receivers, including the retail sector, manufacturing sector, and intermodal transportation sector. Backed-up unloading causes storage problems at the upstream partners.
- Economic Losses: includes losses to the ports themselves and the other businesses that depend on the operation of the ports. The manufacturing industry depends on the raw materials and parts; the automotive industry depends on the cars being delivered; the retail industry depends on the products being delivered, the energy sector depends on the imported and exported oil and LNG, and many agricultural goods imported from abroad are spoiling or rotting.
- Reputational Damage: Affected ports and businesses directly (e.g., shipping and cargo companies) and indirectly (e.g., retailers, manufacturers) affected by the incident have their reputations harmed and lose customer confidence due to disruption to their services.

1

Ransomware Screenshot

Figure 1: Ransomware Screenshot with the Ransom Amount

Sorry!
All your data have been encrypted!

What happened to My Computer?

Your files were encrypted and can only be recovered using the decryption key we have. You need to pay in 72 hours to be able to get the encryption key. Otherwise, you will never be able to recover your files.

Can I recover my files?

Yes, but only using the encryption key. We guarantee that you will be able to decrypt all your files. Attention!

Do not rename encrypted files.

How Do I pay?

You need to send us 2360 Bitcoin (40 million U.S. Dollars in Bitcoins), evenly distributed to the four addresses given below. After the payment is submitted, email us at: cyberpirates@protonmail.com with your I.D. in the title of your message: SACHM392759. Then, you will get your decryption key.

c0411b4faa415aa5636f39215f224dc882c7d5821414b436fcb6d34cfa07b4f6

159a024da13dae13908a2389aeb8a781345ab4d655b3a69938089dfeaa3e7811

f547ee5f4ad3757dff6d4e0bfbb9aac579e13f1f2a6d5cf1d097501caec692cc

bdeb4703d25ca23129d463d100403832b92df3888ad12b32c6c92592bf102d41

2

Top 10 Busiest Ports in the U.S.

Table 1: Top 10 ports of the U.S. are given in the table along with their capacity.

Top 10 Busiest Ports	Annual TEUs (million)	Status Operational?	Primary Dependent Sectors
Port of Los Angeles	10.7	Down -Ransomware	Transportation, Retail, Manufacturing
Port of Long Beach	9.4	Down-Ransomware	Transportation, Retail, Manufacturing
Port of N.Y. and NJ	8.9	Operational	Transportation, Retail
Port of Savannah	5.6	Down-Ransomware	Transportation, Manufacturing, Retail
Port of Seattle	3.7	Operational	Transportation, Retail
Port of Houston	3.7	Operational	Energy, Transportation, Retail
Port of Virginia	3.5	Operational	Transportation, Energy, Defense
Port of Charleston	2.8	Down-Ransomware	Transportation, Retail
Port of Oakland	2.4	Operational	Transportation, Retail, Manufacturing
Port of Miami	1.3	Operational	Transportation, Retail
Total (10 ports)	52		

TEU is used to measure capacity and stands for the twenty-foot equivalent unit, referring to the total number of containers a port loads/unloads in a year.

Primary dependent sectors are the sectors whose operations depend on each port the most. The transportation sector is directly affected by a nonoperational port since all related marine, rail, ground, and air transportation is halted or delayed. The retail sector heavily depends on the products waiting in containers for just-in-time deliveries and logistics. The manufacturing sector depends on the raw materials and parts waiting in the containers. The energy sector depends on the transportation of oil and liquefied natural gas via ports.

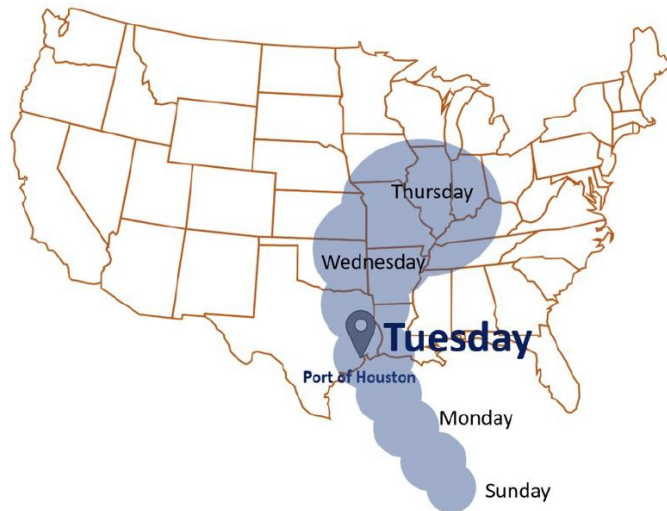**Figure 2:** Top 10 Busiest Ports in the U.S. (the Nonoperational Ports are in red as of Monday)

3

Hurricane in the Gulf of Mexico

A category 3 hurricane, Hurricane Ophelia, in the Gulf of Mexico is being watched. It could possibly make landfall in southern Texas within 24 hours.

Figure 3: The projected path of the Hurricane Ophelia

4

Insurance Industry Loss Estimates - Overview

Table 1: Insurance Industry loss estimates overview group by claimants
(Adapted from Lloyd's of London et al., 2019)

Class of Insurance	Type of Insurance	Cyber Policy Type	Insurance Ind. Loss ($ mil.)
Port Operators			
Cyber	Business Interruption	Cyber Affirmative	288
Commercial Property	Business Interruption	All Risks	241
Liability	Directors and Officers	All Risks	41
Cyber	Incident Response Costs	Cyber Affirmative	39
Cyber	Regulatory and Defense Coverage	Cyber Affirmative	68
Cyber	Reputational Risk	Cyber Affirmative	30
Cyber	Data and Software Loss	Cyber Affirmative	28
Cargo Content Owners			
Marine	Cargo	Cyber Affirmative	2
Ship Owners			
Marine	Freight, Demurrage, and Defense	All Risks	15
Port Management System Software			
Liability	Directors and Officers	All Risks	58
Liability	Technology Errors and Omissions	All Risks	34
Logistics and Cargo Handling Companies			
Liability	Directors and Officers	All Risks	78
Cyber	Business Interruption	Cyber Affirmative	23
Commercial Property	Business Interruption	All Risks	93
Cyber	Data and Software Loss	Cyber Affirmative	69
Ship Management Company			
Liability	Technology Errors and Omissions	All Risks	96
Liability	Directors and Officers	All Risks	5
Cyber	Data and Software Loss	Cyber Affirmative	15
Supply Chain Companies			
Commercial Property	Contingent Business Interruption	All Risks	421
Cyber	Contingent Business Interruption	Cyber Affirmative	50
Total Insured Losses			**1694**

The loss estimates are broken down for each claimant type and aggregated for all actors within each category. Policies that explicitly include cyber and specifically for cyber are categorized as Cyber Affirmative. Most claims after such a loss would be made for Business Interruption, Reputation Loss, Incident Response Costs, Regulatory Fees, and Liability risks.

Appendix B: Inject 1 – MT ISAC Bulletin

⚓ **Marine Transportation ISAC** Home Services Maritime Cybersecurity Summit More... **Contact Us**

All Posts Thought Leadership Blogs News 🔍

September 19, 2023

Marine Transportation ISAC Bulletin

This is an emergency bulletin from MT-ISAC about the ongoing disruptions in U.S. ports.

Catastrophic Disruptions in the U.S. Ports

11 AM EDT UPDATE -- On Monday, September 18th, 2023, a ransomware attack targeted the Port of Los Angeles, Port of Long Beach, Port of Savannah, and Port of Charleston. The attack encrypted the cargo management and tracking systems at these ports, causing a complete shutdown of operations. As of Tuesday, these four ports are still in the process of recovering from the attack and attempting to access backup or alternative information technology systems.

Two more Ports were Attacked

As of Tuesday, September 19th, 2023, 9 am EDT, it has been reported that two other ports, the Port of Virginia and the Port of Miami, have also fallen victim to a ransomware attack – apparently by the same threat actor. These two ports are also experiencing a complete shutdown of operations as a result of the attack.

Hurricane Makes Landfall at the Port of Houston

In addition to the ransomware attacks, a Category 4 hurricane, Hurricane Ophelia, made landfall on the Texas coast, impacting the Port of Houston. It caused disruptions to the port, surrounding transportation and petrochemical infrastructure, and exacerbated the impacts of the ransomware attacks on the national supply chain.

After the initial cyber-attack at four ports, some marine traffic had been diverted to other ports; however, with the loss of operation in the additional three ports, the impact has increased.

The widespread impact of these incidents is potentially catastrophic, as the affected ports handle a significant amount of containerized and other types of cargo. The disruption to the supply chain could result in delays and shortages of goods and materials, as well as increased costs for businesses that rely on the affected ports for shipping.

Figure 1: Top 10 Busiest Ports of the U.S. (Updated to indicate Nonoperational or Severely Impacted Ports in red as of Wednesday)

Technical Details – Zero-Day Vulnerability

The initial forensics analysis of the malware revealed that the attackers exploited a zero-day vulnerability that exists in a widely utilized cargo management and tracking system. The vulnerable systems are also commonly used by the other ports, and they might be at risk unless such systems are patched as soon as possible. Unfortunately, no patch is available yet - it is expected to be released in 24-48 hours by the software vendor, PoCaMaS, for the use of other ports that still have vulnerable systems in operation. Those ports are in the process of making the backups of the most critical systems to store in air-gapped systems.

Ransomware Recovery

Authorities and cybersecurity vendors are working to contain the ransomware attacks and bring the affected ports back online as soon as possible. It is not yet known when the affected ports will be able to resume normal operations. Some of the factors that could affect the speed of recovery include:

- The extent of the damage caused by the ransomware attack
- The availability of backups
- The complexity of the systems
- The lack of expertise deployable to numerous impacted facilities
- The extent of the disruption and size of the port

It is likely to take a port longer to recover from a ransomware attack if they do not have regular backups and are unable to pay the ransom. In such cases, the port may need to rebuild systems and data from scratch, which could take a significant amount of time and resources. Only the Port of Virginia have air-gapped backup systems; therefore, they will try to restore from the backups and have the potential for a quicker and fuller recovery.

The backups of the rest of the ports were either infected, inaccessible, or unusable. The port authorities are in the process of negotiating to pay the ransom. Even if the ransom is paid, it might take one week to ten days to gain 95% of the operability capacity from the impact of the ransomware due to the number of available I.T. personnel and the systems in each port.

Figure 2: Cumulative recovery distributions for the ports
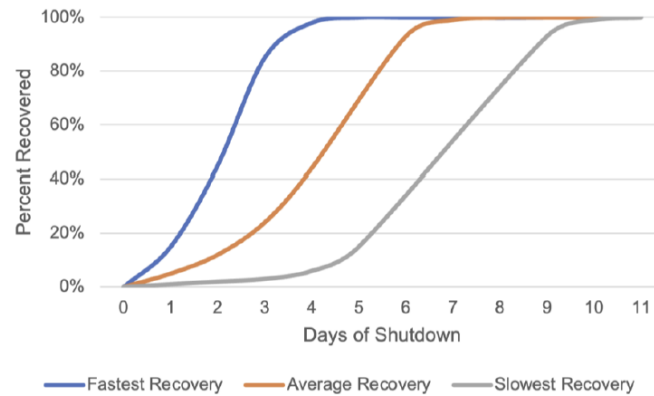

Table 1: Top 10 ports of the U.S., along with the affected capacity, status, and recovery durations. Affected TEUs indicate the throughput based on the estimated recovery duration for each affected port.

Ports	Affected TEUs (Thousands)	Status Operational?	Estimated Recovery Durations
Port of Los Angeles	205.2	Down-Ransomware	7 days
Port of Long Beach	180.2	Down-Ransomware	7 days
Port of Savannah	122.7	Down-Ransomware	8 days
Port of Houston	81.1	Down-Hurricane	10 days
Port of Virginia	38.4	Down-Ransomware	4 days
Port of Charleston	53.7	Down-Ransomware	7 days
Port of Miami	32.1	Down-Ransomware	9 days
Port of N.Y. and NJ	N/A	Operational	N/A
Port of Seattle	N/A	Operational	N/A
Port of Oakland	N/A	Operational	N/A
Total (7 ports)	713.4		

Insurance Industry Loss Overview

Table 2: Insurance Industry loss overview group by claimants, $millions
(Adapted from Lloyd's of London et al., 2019)

Stage 1: 4 Nonoperational Ports on 9/18/2023

Stage 2: 7 Nonoperational Ports on 9/19/2023

Class of Insurance	Type of Insurance	Cyber Policy Type	Insurance Industry Loss in $ Millions	
			Stage 1	Stage 2
Port Operators				
Cyber	Business Interruption	Cyber Affirmative	288	890
Commercial Property	Business Interruption	All Risks	241	563
Liability	Directors and Officers	All Risks	41	127
Cyber	Incident Response Costs	Cyber Affirmative	39	235
Cyber	Regulatory and Defense Coverage	Cyber Affirmative	68	189
Cyber	Reputational Risk	Cyber Affirmative	30	89
Cyber	Data and Software Loss	Cyber Affirmative	28	33
Cargo Content Owners				
Marine	Cargo	Cyber Affirmative	2	103
Ship Owners				
Marine	Freight, Demurrage, and Defense	All Risks	15	45
Port Management System Software				
Liability	Directors and Officers	All Risks	58	139
Liability	Technology Errors and Omissions	All Risks	34	97
Logistics and Cargo Handling Companies				
Liability	Directors and Officers	All Risks	78	193
Cyber	Business Interruption	Cyber Affirmative	23	68
Commercial Property	Business Interruption	All Risks	93	217
Cyber	Data and Software Loss	Cyber Affirmative	69	185
Ship Management Company				
Liability	Technology Errors and Omissions	All Risks	96	253
Liability	Directors and Officers	All Risks	5	32
Cyber	Data and Software Loss	Cyber Affirmative	15	74
Supply Chain Companies				
Commercial Property	Contingent Business Interruption	All Risks	421	1302
Cyber	Contingent Business Interruption	Cyber Affirmative	50	135
Total Insured Losses			**1694**	**2154**

The losses are broken down for each claimant type and aggregated for all actors within each category. Policies that explicitly include cyber and specifically for cyber are categorized as Cyber Affirmative. Most claims after such a loss would be made for Business Interruption, Reputation Loss, Incident Response Costs, Regulatory Fees, and Liability risks.

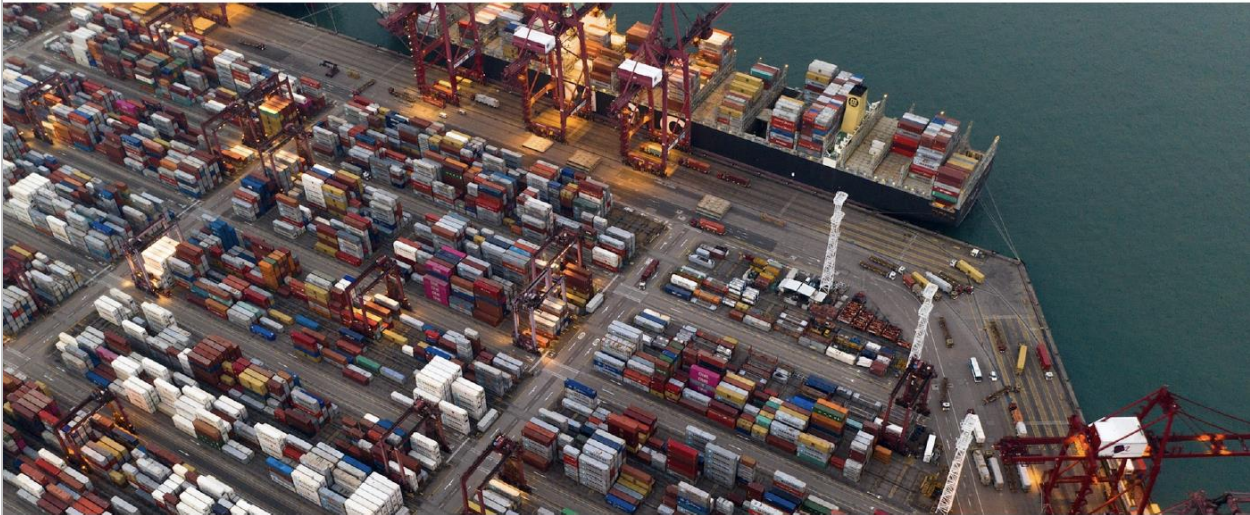## Appendix C: Inject 2 – Albany Herald Post Article

Albany Herald Post

A Nation-State Backed Attack against U.S.

It has been two days since a ransomware attack brought the operations of two additional ports to a standstill, with six major U.S. ports now ground to an almost complete halt.

Give this article

Container Port |Photo Gallery

Sept. 20, 2023

The Port of Los Angeles, Port of Long Beach, Port of Savannah, Port of Charleston, Port of Norfolk, and Port of Miami were all targeted in the cyber-attack, which encrypted the cargo management and tracking systems at these ports. As a result, the ports have been unable to track the contents, location, or destination of any of the containers at the ports, causing widespread disruption to the supply chain.

Port Authorities **paid the ransom** except for the Port of Virginia. The initial ransom amount for each port was reported to be $40 million worth of Bitcoins, but at the time this article was published, we could not confirm the paid ransom amount.

In the time that elapsed since the attack, authorities and cybersecurity experts have been working around the clock to contain the ransomware and bring the affected ports back online. While some progress has been made, the recovery process is expected to take several more days, if not weeks. In the meantime, the affected ports are experiencing significant delays and backlogs, with incoming vessels anchored offshore and trucks backed up for miles.

Just as the affected ports were beginning to make progress in their recovery efforts, the Port of Houston was hit by a major storm, Hurricane Ophelia, causing further disruptions to the shipping industry. The storm damaged infrastructure at the port and disrupted operations, adding to the already significant challenges faced by the U.S. shipping industry and consequently manufacturing and retail sectors. Delays in the delivery of petroleum products, and impacted refineries, have led to an increase in gas prices that has hit almost one dollar in some regions of the country.

The logistics impacts of the ransomware attack and the storm have been widespread; the businesses relying on the ports experience delays and shortages of goods and materials.

Who is behind this Attack?

According to U.S. intelligence sources who wanted to stay anonymous, shell companies tied to sanctioned North Korean companies appear to have shorted U.S. logistics and retail stocks on international exchanges prior to the attack. An investigation into the flow of the cryptocurrency used in the ransoms is ongoing.

Impact of Attribution on Economic Recovery

The possible involvement of a state actor immediately brings one aspect to the attention of insurance providers: war exclusion, or with its legal term, force majeure. If the attack is considered an act of war, most insurance policies have an exception to avoid having to cover such losses.

Another aspect that is not yet certain is the possible involvement of the federal government in backstopping such losses in future cases or perhaps even covering some of these losses using funding tied to a disaster declaration. The catastrophic impact of the recent cyber-attack and hurricane

landfall has led to unusual steps, like the U.S. Chamber of Commerce suggesting that government disaster funding could help ease recovery across several sectors impacted by delays and supply chain interruptions. However, there is no public announcement of a government backstop or funding channel yet. Last year, with the suggestion of the Government Accountability Office, the Department of Treasury sought input from the public, including the insurance industry, on how the federal government should address such catastrophic incidents. Although such developments indicate ongoing discussions in both the Executive and Legislative branches of the United States government, no promises of forthcoming funds have been made.

Albany Herald Post

Go to Home Page »

NEWS

OPINION

ARTS

LIVING

LISTINGS & MORE

Appendix D: Formulas used in Loss Estimate

The following equations are used to calculate the relevant items in the loss estimate tables (Tables 1 and 2 in the simulated content) by adapting from Lloyd's of London et al.[26].

$Incident\ Response\ Costs = (Annual\ TEU\ turnover \div 365\ days) \times \$500\ per\ day$

$Regualtory\ and\ Defense\ Coverage = (Annual\ TEU\ turnover \times \$1\ per\ TEU) + \$10,000,000$

$Cyber\ Data\ and\ Software\ Loss = (Annual\ TEU\ turnover \div 365\ days) \times of\ Days\ Port\ is\ Closed \times \$50\ per\ TEU$

$Perishable\ Cargo = ((Annual\ insured\ TEU\ turnover \div 365\ days) \times Proportion\ of\ Portfolio\ which\ is\ Perishable\ (\%)) \times 75\% \times \#\ of\ Days\ Port\ is\ Closed \times Average\ cost\ per\ TEU\ (\$)$

---

[26] Lloyd's of London, Cambridge Centre for Risk Studies, & Nanyang Technological University. (2019). *Shen attack Cyber risk in Asia Pacific ports* (CyRiM Report 2019).

About The Society of Actuaries Research Institute

Serving as the research arm of the Society of Actuaries (SOA), the SOA Research Institute provides objective, data-driven research bringing together tried and true practices and future-focused approaches to address societal challenges and your business needs. The Institute provides trusted knowledge, extensive experience and new technologies to help effectively identify, predict and manage risks.

Representing the thousands of actuaries who help conduct critical research, the SOA Research Institute provides clarity and solutions on risks and societal challenges. The Institute connects actuaries, academics, employers, the insurance industry, regulators, research partners, foundations and research institutions, sponsors and non-governmental organizations, building an effective network which provides support, knowledge and expertise regarding the management of risk to benefit the industry and the public.

Managed by experienced actuaries and research experts from a broad range of industries, the SOA Research Institute creates, funds, develops and distributes research to elevate actuaries as leaders in measuring and managing risk. These efforts include studies, essay collections, webcasts, research papers, survey reports, and original research on topics impacting society.

Harnessing its peer-reviewed research, leading-edge technologies, new data tools and innovative practices, the Institute seeks to understand the underlying causes of risk and the possible outcomes. The Institute develops objective research spanning a variety of topics with its strategic research programs: aging and retirement; actuarial innovation and technology; mortality and longevity; diversity, equity and inclusion; health care cost trends; and catastrophe and climate risk. The Institute has a large volume of topical research available, including an expanding collection of international and market-specific research, experience studies, models and timely research.

<div align="center">

Society of Actuaries Research Institute

475 N. Martingale Road, Suite 600

Schaumburg, Illinois 60173

www.SOA.org

</div>