**Cyber incidents database in maritime transportation**

1. **Maritime transportation business disruption and maritime system execution failure**

(1) NotPetya attacked Servers and computers of Maersk Line

Shipping giant and NotPetya victim Maersk were forced to replace tens of thousands of servers and computers in the aftermath of the June 17, 2017, ransomware attack, the company’s chairman said in Davos at the World Economic Forum. It said that Maersk Line was not the direct target, affected by treats to Iranian nuclear centrifuge. 

Source of the website: [www.scmagazine.com/notpetya-attack-totally-destroyed-maersks-computer-network-chairman/article/739730/](http://www.scmagazine.com/notpetya-attack-totally-destroyed-maersks-computer-network-chairman/article/739730/)

<https://www.theregister.co.uk/2018/01/25/after_notpetya_maersk_replaced_everything/>

<https://backend.orbit.dtu.dk/ws/portalfiles/portal/200738854/190401_Analyzing_the_Attack_Surface_of_Ships.pdf>

(2) Hacker attacked the movement controlling and shipping containers locating system in Port of Antwerp

In late 2013, the Port of Antwerp was in the spotlight. Presumably, for two years it had been the victim of an APT attack organized by a drug cartel. In June 2011, hackers had compromised and gained control over the terminal systems.

They released containers to their truckers without knowledge of the port authorities and then removed information about contraband containers from all databases. When police uncovered the case, they also discovered a ton of cocaine, guns, and more than 1.3 million Euros in a suitcase, and those were just the tip of the iceberg. ( <https://www.kaspersky.com/blog/maritime-cyber-security/8796/>)

Source website of this picture: <https://www.globexs.com/es/tags/port-antwerp>

(3) Pirates attacked the content supervisory system of shipping company

According to a recent [RISK Labs report from Verizon](http://www.verizonenterprise.com/resources/reports/rp_data-breach-digest_xg_en.pdf), a security team from the company was tapped to help a global shipping company deal with its pirate problem.

Although the shipping company had dealt with pirates before, something changed in recent months that raised alarm – the pirates began targeting specific ships and even specific containers to find what was most valuable to them.

Rather than hijacking a ship and holding the crew hostage for days, the pirates were in and out in a matter of hours.

It soon became apparent that the pirates knew the contents of every crate being shipped, using bar codes on the shipping containers to identify and steal only certain items, leaving the rest.

As Verizon discovered, the pirates had exploited an unpatched vulnerability in the shipping company’s homegrown content management system (CMS) to create a backdoor, which they used to access records of shipping routes, schedules, and container contents. ( <https://nakedsecurity.sophos.com/2016/03/07/pirates-hacked-shipping-company-to-steal-info-for-efficient-hijackings/>)

(4) Cyber-attacks against the floating oil rig

In 2010, a drilling rig was tilted from its construction site in South Korea towards South America. The vessel’s computers and control systems were riddled with viruses. Identifying the hack and fixing it took 19 days. (<https://www.kaspersky.com/blog/maritime-cyber-security/8796/>)

Mark Gazit, CEO of ThetaRay, an internet security company, said an attacker managed to tilt a floating oil rig to one side off the coast of Africa, forcing it to shut down. It took a week to identify the cause and fix, he said, mainly because there were no cybersecurity professionals aboard. He declined to say more. These attacks showed the vulnerability of floating oil rig systems, and illustrated the cyberattacks against oil infrastructure may cost high economic loss for the energy company. (<https://www.scmp.com/news/world/article/1496193/experts-warn-global-shipping-industry-vulnerable-cyber-attack>). Source website of this picture: <https://www.petro-online.com/news/fuel-for-thought/13/breaking-news/how-do-oil-rigs-floatnbsp-nbsp/35151>

(5) Hackers attacked Port of Barcelona and San Diego Port:

On the morning of September 20, Port of Barcelona was the victim of a cyberattack, as reported by experts in ethical hacking from the International Institute of Cyber Security; fortunately, maritime operations were not affected by the incident, as the Port administration had a plan to respond to these kinds of contingencies.

To date, technical details about the cyberattack have not been publicly disclosed, but it’s known that the attackers hit several servers in the port’s security infrastructure, without interrupting their maritime operations. Likewise, land operations, such as reception and delivery, seem to have suffered no problems due to the attack.

This is not the first time that a maritime operations organization suffers a similar attack. Sensitive information from the firm was subtracted and the attackers demanded payment for its return. ( <https://www.securitynewspaper.com/2018/09/26/hacking-attack-in-port-of-barcelona/>)

Source website of the picture: <https://www.viator.com/en-IN/tours/Barcelona/Barcelona-Transfer-Central-Barcelona-to-Cruise-Port/d562-2140BCNHTLPRT>



The Port of San Diego has experienced a serious cybersecurity incident that has disrupted the agency’s information technology systems, the port said in a statement.

The port’s investigation has so far determined that ransomware was involved in this attack. The ransom note requested payment in bitcoin, although the amount that was requested was not disclosed.

“It is important to note that this is mainly an administrative issue and normal port operations are continuing as usual. The port remains open, public safety operations are ongoing, and ships and boats continue to access the Bay without impacts from the cybersecurity incident,” said Port of San Diego CEO Randa Coniglio.

“While some of the port’s information technology systems were compromised by the attack, port staff also proactively shut down other systems out of an abundance of caution.”(<https://worldmaritimenews.com/archives/261525/port-of-san-diego-hit-by-cyber-attack/>)

Source website of the picture: <https://www.bigstockphoto.com/zh/image-80874998/stock-photo-ms-cap-san-diego-in-the-port-of-hamburg>

(6) Hacker Disabled Offshore Oil Platforms' Leak-Detection System

In 2009, a Los Angeles federal grand jury indicted a disgruntled tech employee Tuesday on allegations of temporarily disabling a computer system detecting pipeline leaks for three oil derricks off the Southern California coast. Mario Azar, 28, faces a maximum 10-year term after being accused of purposely impairing a computer system that monitored for leaks on three Pacific Energy Resources platforms offshore of Huntington Beach.

Federal authorities expressed alarm over the incident. Most malicious hacks, especially those by aggrieved employees, often wreak havoc on a company's internal computer operations to disrupt business activity. But in this case, the Southern California coastline was exposed to an environmental disaster.

"It was offline. The leak-detection system was rendered inoperable for some time," said Thom Mrozek, a spokesman for Los Angeles federal prosecutors. (<https://www.wired.com/2009/03/feds-hacker-dis/>)

(7) COSCO Shipping Lines Falls Victim to Cyber Attack

COSCO Shipping Lines confirmed that it has been hit by a cyberattack impacting its internet connection within its offices in America.

As such, local email and network telephone were not working properly and the company decided to shut down the connections with other regions for further investigation.

Based on the information released so far, the incident that took place on Tuesday, July 24, was described as a ransomware attack.

The Chinese shipping and logistics company said that its vessels were not impacted and that its main business operation systems were performing stably. However, COSCO’s terminal at the Port of Long Beach was affected. (<https://worldmaritimenews.com/archives/257665/cosco-shipping-lines-falls-victim-to-cyber-attack/>)

(8) A large ship heading to New York City falls victim to cyber attacks

 A commercial vessel suffered a significant malware attack in February, prompting the US Coast Guard to issues an advisory to all shipping companies: Here be malware.

In February 2019, a large ship bound for New York City radioed the US Coast Guard warning that the vessel was "experiencing a significant cyber incident impacting their shipboard network."

The Coast Guard led an incident-response team to investigate the issue and found that malware had infected the systems of the ship and significantly degraded functionality. Fortunately, essential systems for the control of the vessel were unimpeded. ( <https://www.darkreading.com/vulnerabilities---threats/coast-guard-warns-shipping-firms-of-maritime-cyberattacks/d/d-id/1335198>)

Source website of the picture: <https://spectrum.ieee.org/transportation/marine/the-struggle-to-make-dieselguzzling-cargo-ships-greener>

(9) Steamship Authority hit by ransomware attack



Jun 2, 2021. (WWLP & SHNS) – Passengers going to Nantucket and Martha’s Vineyard via the Steamship Authority may have to deal with possible delays Wednesday, due to a ransomware attack.

The ferry service posted on their official Twitter account Wednesday that the attack is affecting their operations, and that a team of IT professionals is currently working to assess the impact of the attack. More information is expected to be released once that initial assessment is completed.

The Steamship Authority’s website remained inaccessible around midday. As a result, passengers cannot book or reschedule vehicle reservations online or by phone. The Authority posted its ferry schedules to Martha’s Vineyard and Nantucket on [social media](https://nam11.safelinks.protection.outlook.com/?url=https%3A%2F%2Ftwitter.com%2FSteamshipMA&data=04%7C01%7CAmy.Phillips%40wwlp.com%7C54cdbddd5c9c49a2c10008d925fc269d%7C9e5488e2e83844f6886cc7608242767e%7C0%7C0%7C637582587196283479%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000&sdata=v7m60NuyQF%2BnpBZLhHhHUFKtUDl6FhT966twSajbVZQ%3D&reserved=0) to help those who cannot load the website.

Any existing reservations will be honored, and all rescheduling and cancellation fees will be waived, the organization said. “If traveling with the Authority today, cash is preferred for all transactions. The availability of credit card systems to process vehicle and passenger tickets, as well as parking lot fees, is limited,” officials said in their statement. “Additional information will be provided as it becomes available.”(<https://www.wwlp.com/news/massachusetts/steamship-authority-hit-by-ransomware-attack/>)

(10) Cyber-attack disrupts major South African port operations

****JOHANNESBURG, July 22, 2021 (Reuters) - A cyber-attack has disrupted container operations at the South African port of Cape Town, an email seen by Reuters on Thursday said. The latest disruption has delayed containers and auto parts, but commodities were mostly unaffected as they were in a different part of the port, one of the sources said.

It will also create backlogs that could take time to clear.

Transnet said its container terminals were disrupted while its freight rail, pipeline, engineering and property divisions reported normal activity.

**(**<https://www.reuters.com/world/africa/exclusive-south-africas-transnet-hit-by-cyber-attack-sources-2021-07-22/>**)**

1. **Maritime data breach**

(11) Defense shipbuilder Austal hit by cybersecurity breach and extortion attempt

Western Australia-based Defence shipbuilder Austal has been the subject of a cybersecurity breach and extortion attempt.

The company announced to the stock exchange last night that its Australian data management system had been targeted by an "unknown offender".

Some staff email addresses and mobile phone numbers were accessed, according to the statement which acknowledged that a "small number" of customers had been affected.

A hacker tried to sell some of the stolen Austal information online and extort the company after a cyber breach.

Austal says there is "no evidence" that information affecting national security was stolen. The Federal Police and Australian Cyber Security Centre are now investigating.

(<https://www.newscientist.com/article/2143499-ships-fooled-in-gps-spoofing-attack-suggest-russian-cyberweapon/>)

Source website of the picture: <https://www.abc.net.au/news/2018-11-01/cape-class-patrol-boa/10458088>

(12) Hacked Brit shipping giant Clarksons

 British shipping company Clarkson has 'fessed up to a data breach, saying a miscreant has accessed its systems and the public should expect some of it to be made public.

According to the announcement, "unauthorized access" to "computer systems" was "gained via a single and isolated user account which has now been disabled".

Cryptically, the announcement noted "the person or persons behind the incident may release some data" and "the data at issue is confidential and lawyers are on standby wherever needed to take all necessary steps to preserve the confidentiality in the information".(<https://www.theregister.co.uk/2017/11/29/clarksons_got_some_data_stolen/>)

Source website of the picture: <https://www.teiss.co.uk/clarksons-data-breach-ransom/>

1. **Theft or manipulation or loss of maritime information**

(13) Hackers attacked the Australian Customs and Border Protection Service Cargo Management Systems

In 2012 hackers, working for a criminal syndicate, compromised the cargo system controlled by the [Australian Customs and Border Protection Service agency](http://en.wikipedia.org/wiki/Australian_Customs_and_Border_Protection_Service). Cybercriminals wanted to know which shipping containers were suspected by the police or customs authorities. With this data, they’d know if they needed to abandon particular containers with contraband cargo.

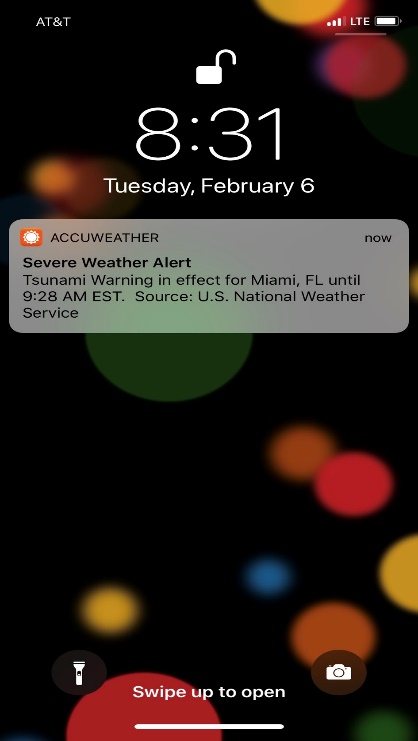
Source of Website: <https://www.kaspersky.com/blog/maritime-cyber-security/8796/>

(14) Ships fooled in GPS spoofing attack suggest Russian cyberweapon

On 22 June, the US Maritime Administration filed a seemingly bland incident report. The master of a ship off the Russian port of Novorossiysk had discovered his GPS put him in the wrong spot – more than 32 kilometers inland, at Gelendzhik Airport. After checking the navigation equipment was working properly, the captain contacted other nearby ships. Their AIS traces signals from the automatic identification system used to track vessels placed them all at the same airport. [At least 20 ships were affected](http://maritime-executive.com/editorials/mass-gps-spoofing-attack-in-black-sea). This is probably for defensive reasons; many NATO guided bombs, missiles, and drones rely on GPS navigation, and successful spoofing would make it impossible for them to hit their targets. If the hardware and software are becoming more accessible, nation-states soon won’t be the only ones using the technology. This is within the scope of any competent hacker. There have not yet been any authenticated reports of criminal spoofing, but it should not be difficult for criminals to use it to divert a driverless vehicle or drone delivery or to hijack an autonomous ship. Spoofing will give everyone affected the same location, so a hijacker would just need a short-ranged system to affect one vehicle.

But Humphreys believes that spoofing by a state operator is the more serious threat. “It affects safety-of-life operations over a large area,” he says. “In congested waters with poor weather, such as the English Channel, it would likely cause great confusion, and probably collisions.”(<https://www.newscientist.com/article/2143499-ships-fooled-in-gps-spoofing-attack-suggest-russian-cyberweapon/#ixzz6EORvpyep>)

(15) Buoys data under cyber manipulation enable falsely impending tsunami announcement



The Tsunami Warnings system consists of an ocean-floor sensor and an acoustic cable linking it to a buoy. The sensor measures any tsunami, and the buoy quickly transmits data to a monitoring station by satellite.

Spousta and Chan asserted buoys data under cyber manipulation enable falsely impending tsunami announcement and even breach electric power system through contextualizing the connection between buoy data, transmission network, warning system, and infrastructure resilience. Image Source come from: <https://www.npr.org/sections/thetwo-way/2018/02/06/583634420/false-tsunami-warning-issued-across-the-east-coast-and-caribbean>

1. **Theft or loss of funds from maritime sectors**

(16) Hackers attacked two shipping companies

In 2013, a failed attempt at digital piracy occurred when a Dutch drug ring used a group of Belgian hackers to reroute two tons of cocaine and heroin into their waiting arms. These hackers were able to gain remote access to the computers of two different shipping companies. Here, they then rerouted the containers into the port of Antwerp, Belgium, for a convenient pick-up. Instead of the usual transportation company, the drug runners showed up, ready to haul away their prize – worth more than $1.7m. But police caught them before they could carry out their devious plan. (https://eandt.theiet.org/content/articles/2019/04/cyber-pirates-terrorising-the-high-seas/)

Source website of the picture <https://www.dreamstime.com/editorial-photography-top-biggest-container-shipping-companies-logos-vector-collection-icons-services-white-tablet-rusty-wooden-image65618577>

(17)Hackers steal $644,000 from a Cyprus shipping company

Hackers posing as a bunker supplier have stolen $644,000 from an unnamed shipping company based in Limassol, Cyprus.

The shipping company had received a legitimate invoice from its bunker supplier in Africa for marine fuel supplied to its fleet, police investigators told the Cyprus News Agency.

Unknown cyber-criminals, thought to be based in Poland, later emailed the shipping company posing as the bunker supplier, asking that the payment be remitted to another bank account.

The shipping company made two separate transfers on July 28 and 29 to the bank account in question and the money disappeared.

The theft was discovered when the legitimate fuel supplier in Africa sent an email to the shipping company, requesting payment.

Police investigations are ongoing in Cyprus with the cooperation of Interpol. (<https://splash247.com/hackers-steal-644000-from-a-cyprus-shipping-company/>)

(18) Nigerian hackers target shipping companies globally

 A criminal gang in Nigeria targeting the global maritime industry has been running multiple “business email compromise” scams for hundreds of thousands of dollars. The group calling themselves “Gold Galleon” has been sending messages to infiltrate payments within shipping companies over the last year.

As informed, the Gold Galleon uses similar tools, tactics, and procedures (TTPs) to other Business Email Compromise groups, typically using publicly available malware like inexpensive remote access trojans (RATs), crypters and email lures. The group often targets smaller maritime companies, such as those who may provide ship management services, port services, and ‘cash to master’ facilities.

Gold Galleon appeared to identify target emails from looking at publicly available websites, and it also appeared to be using commercially available marketing tools to scrape email addresses – such as Email Extractor and BoxxerMail – as well as purchasing email address lists. Once they gained access to a target’s inbox, they extracted all the target’s contacts – plus every email address that the target ever had an exchange with, using a free tool called EmailPicky.

A South-Korean shipping company was among the victims: The group was able to steal credentials for eight accounts belonging to the company, including the accountant’s and they then targeted all of the clients. The attackers monitored the business transaction of the South Korean company and a cash-to-master service for a ship arriving in America and inserted themselves into the transaction with a fake Outlook email account. They submitted a fraudulent email asking the South Korean company to deposit the payment into a “subsidiary bank account” – a mule operated by the criminals.

A separate attack saw Gold Galleon targeting another of this South Korean company’s clients for $325,585, a large Japanese company that provides marine transportation of petroleum and chemicals with clients worldwide. The Japanese company, ultimately, had flagged the transaction as suspicious.

A third attempt against a separate multinational Japanese conglomerate for $243,838 was also derailed, with SecureWorks able to notify both parties and South Korean CERT – the incident response team in the country.

(<https://safety4sea.com/nigerian-hackers-target-shipping-companies-globally/>)

(19)Washington’s Port of Kennewick hit by cyberattack

November 20, 2020, the Port of Kennewick has learned it was victimized by a digital ransomware attack, whereby cybercriminals circumvented its systems, placed a sophisticated encryption lock on the port’s servers, and demanded $200,000 in ransom to restore access to the port’s servers and files. This was a differentiated cyberattack with sophisticated, military-grade encryption focused on locking the port’s servers and holding those servers hostage to leverage a ransom. The port’s technology contractor reported that it is confident no individual data has been compromised as the virus focused on locking the port servers instead of accessing data or information located within those servers.

Port of Kennewick staff has reported the ransom threat to the Federal Bureau of Investigation and have been in contact with both their Richland and Seattle offices, and staff reached out to the Washington State Office of Cyber Security as well. According to these agencies, this variant of ransomware virus has no known decoder. (https://www.professionalmariner.com/washingtons-port-of-kennewick-hit-by-cyberattack/)

1. **Theft or loss of cargoes**

(20) GPS Jammers: Cargo Theft Groups employ it to Mask GPS Tracking Devices

In 2015, Auto thieves shipping vehicles to China used GPS jammers placed in shipping containers in an attempt to thwart tracking of the containers, according to July 2014 information from the National Insurance Crime Bureau. In 46 reported incidents, the thieves placed one or more GPS jammers in cargo containers with stolen automobiles. The devices were made in China and could be bought for approximately $14.00 over the internet. The use of the GPS jammers was an apparent attempt by thieves to thwart the tracking of the shipping containers. (<https://publicintelligence.net/fbi-cargo-thieves-gps-jammers/>). The original website of this picture: <https://www.ilinesinternational.com/vehicle-shipping/>

(21) Cyber-fraud occurred in Word Fuel Service

October 2013 when WFS received an enquiry from an individual identifying himself as James Battell who said he was employed by the Defense Logistics Agency (DLA), an agency that supplies the U.S. Government with fuel and one it was noted, is also a regular customer of WFS.

Unaware the Battell was, an imposter, WFS agreed to sell him 17,000 metric tonnes (mt) of MGO valued at some $ 17 million on net 30-day payment terms.

WFS then contracted with physical supplier Monjasa, who between December 7 and 9, 2013, supplied Battell’s nominated vessel, Ocean Pearl, with the bunkers via two ship-to-ship transfers off the coast of Lome, Togo.

WFS invoiced Battell on December 20, 2013, for $17910, 833.28, and on January 6, 2014, settled its invoice of $ 17, 061, 968.73 with Monjasa.

Also in January, over two weeks to weeks to weeks, WFS followed up with legitimate DLA personnel regarding the status of its invoice and was eventually told by an FBI agent that Battell was not a DLA employee and that WFS had been defrauded.

“This was the first time World Fuel Learned that Battell was an imposter. To date, the World Fuel invoice to Battell has not been paid; none of the MGO has been recovered; the locations of the MGO remain unknown,” Engelmayer wrote. ( <https://shipandbunker.com/news/world/340232-court-backs-world-fuel-services-following-17-million-bunker-theft>)

Source website of the picture: https://50skyshades.com/news/business-aviation/world-fuel-services-expands-business-and-general-aviation-global-fuel-portfolio

**Table A.1 Descriptive statistics of maritime cyberattacks.**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **No.** | **Categories** | **Year** | **Targets** | **Purpose** | **Retrieved website** |
| 1 | Business disruption, system and execution failure: the ransomware virus (NotPetya) | 2017 | Servers and computers of Maersk Line | Not the direct target, affected by treats to Iranian nuclear centrifuge | www.scmagazine.  com/notpetya-attack-totally-destroyed-maersks-computer-network-chairman/  article/739730/ |
| 2 | Business disruption, system and execution failure: hackers | 2011-2013 | the movement controlling and shipping containers locating system in Port of Antwerp | Producing fake bills of cargo containers and allowing criminals to remove them before the real [proprietor](javascript:;) reached; Reroute the containers | <https://www.kaspersky.com/blog/maritime-cyber-security/8796/>  <https://eandt.theiet.org/content/articles/2019/04/cyber-pirates-terrorising-the-high-seas/> |
| 3 | Business disruption, system and execution failure: hackers | 2016 | The content supervisory system of shipping company | Letting pirates recognize particular containers on appointed vessels, and then get on and off the vessel within several hours | <https://nakedsecurity.sophos.com/2016/03/07/pirates-hacked-shipping-company-to-steal-info-for-efficient-hijackings/> |
| 4 | Business disruption, system and execution failure: hackers | 2014 | A floating oil rig | Hackers tilted one floating oil rig and force it to shut down 19 days | https://www.reuters.com/article/us-cybersecurity-shipping/all-at-sea-global-shipping-fleet-exposed-to-hacking-threat-idUSBREA3M20820140423 |
| 5 | Business disruption, system and execution failure: ransomware | 2018 | Port of Barcelona and San Diego Port: | Hacker infiltrated some information system to request ransom payment that led to disrupting internal administrative functions but port operations were continuing as normal. | <https://www.securitynewspaper.com/2018/09/26/hacking-attack-in-port-of-barcelona/>  https://worldmaritimenews.com/archives/261525/port-of-san-diego-hit-by-cyber-attack/ |
| 6 | Business disruption, system and execution failure: hackers | 2009 | A computer system detecting pipeline leaks for three oil derricks off the Southern California coast | Disabled Offshore Oil Platforms’ Leak-Detection System. | <https://www.wired.com/2009/03/feds-hacker-dis/> |
| 7 | Business disruption, system and execution failure: Virus | 2018 | the Port of Long Beach: the customer service system at COSCO’s terminal | Network shut down resulting in unavailable of electronic communication and affecting Cosco’s daily operation | <https://worldmaritimenews.com/archives/257916/cosco-shipping-lines-back-to-normal-after-cyber-attack/> |
| 8 | Business disruption, system and execution failure: malware | 2019 | A large ship heading to New York City | Infected shipboard network and expressively lower down functionality | https://www.darkreading.com/vulnerabilities---threats/coast-guard-warns-shipping-firms-of-maritime-cyberattacks/d/d-id/1335198 |
| 9 | Business disruption, system and execution failure: ransomware attack | 2021 | Steamship Authority | Passengers going to Nantucket and Martha’s Vineyard via the Steamship Authority may have to deal with possible delays | <https://www.wwlp.com/news/massachusetts/steamship-authority-hit-by-ransomware-attack/> |
| 10 | Business disruption, system and execution failure: hackers | 2021 | Major South African port operations | The latest disruption has delayed containers and auto parts. | <https://www.reuters.com/world/africa/exclusive-south-africas-transnet-hit-by-cyber-attack-sources-2021-07-22/> |
| 11 | Data Breach: hackers | 2018 | Western Australia-based Defense shipbuilder Austal | Data breach: stole information and sell online and attempted to extortion. Fortunately, sensitive information and technology were not compromised. | <https://www.abc.net.au/news/2018-11-01/defence-shipbuilder-austal-subject-of-a-cyber-security-breach/10458042> |
| 12 | Data Breach: hackers | 2017 | Hacked Brit shipping giant Clarksons | Data breach: stole and released confidential data and attempted extortion. These cybercriminals was connected with unauthorized access to the computer system through an isolated and disable user account | https://www.theregister.co.uk/2017/11/29/clarksons\_got\_some\_data\_stolen/ |
| 13 | Theft or loss or manipulation of information: hackers | 2012 | Australian Customs and Border Protection Service Cargo Management Systems | Tracking illegal cargo and detecting whether the specific containers were labeled as suspicious and then providing alter information to criminals | <https://www.kaspersky.com/blog/maritime-cyber-security/8796/> |
| 14 | Theft or loss or manipulation of information: GPS spoofing | 2018 | ship departure the Novorossiysk port in Russian | Successful spoofing can act as a defensive way to make bombs, missiles and drones cannot hit their targets. Also, criminals can employ them to divert deliveries of unmanned ships. Finally, it may cause confusion and possible collision, especially in congested water with poor sight. | <https://www.newscientist.com/article/2143499-ships-fooled-in-gps-spoofing-attack-suggest-russian-cyberweapon/> |
| 15 | Theft or loss or manipulation of information: buoy data manipulation | 2018 | Buoy Array network | It can enable falsely impending tsunami announcement and even breach electric power system through contextualizing the connection between buoy data, transmission network, warning system, and infrastructure resilience | <https://www.npr.org/sections/thetwo-way/2018/02/06/583634420/false-tsunami-warning-issued-across-the-east-coast-and-caribbean> |
| 16 | Theft or loss of funds: hackers breached the computer platform | 2013 | Two different shipping companies | Rerouted cocaine and heroin into Antwerp port to facilitate picking up by Dutch Drug ring | https://eandt.theiet.org/content/articles/2019/04/cyber-pirates-terrorising-the-high-seas/ |
| 17 | Theft or loss of funds: hackers | 2015 | One shipping corporate in Cyprus | Criminals using the fake bill for the legal order and misguide the capital to their bank account | <https://splash247.com/hackers-steal-644000-from-a-cyprus-shipping-company/> |
| 18 | Theft or loss of funds: numerous “business email compromise” scams run by Nigerian hackers “Gold Galleon” | 2018 | the global maritime industry such as A South-Korean shipping company and large petroleum and chemicals maritime transportation Japanese company | They used a fake Outlook email account inserted themselves into the legitimate transaction and requested payment by submitting fraudulent invoices. | https://safety4sea.com/nigerian-hackers-target-shipping-companies-globally/ |
| 19 | Theft or loss of funds: ransomware attack | 2020 | The server of Kennewick Sport | Kennewick Sport in the United States was hit with a ransomware attack in 2020, disrupting its operations. Hackers accessed the port’s server and demanded a ransom of $200,000 to restore access to data, which the port refused to pay. | https://www.professionalmariner.com/washingtons-port-of-kennewick-hit-by-cyberattack/ |
| 20 | Theft or loss of cargoes: GPS jammer | 2015 | Mask GPS Tracking Devices | Thwart tracking of the containers with stolen automobiles. | <https://publicintelligence.net/fbi-cargo-thieves-gps-jammers/> |
| 21 | Theft or loss of cargoes: hackers | 2013 | Word Fuel Service | Spurious fuel order to defraud money | https://shipandbunker.com/news/  world/340232-court-backs-world-fuel-services-following-17-million-bunkertheft |