eBook

Mission Secure

A Comprehensive Guide to Maritime Cybersecurity

With the digitization of industrial control systems (ICS), vessels and ports are left exposed to new cybersecurity risks. In this guide, we will help you navigate the ins and outs of maritime cybersecurity, address cybersecurity challenges and compliance considerations, and get you geared up to establish your maritime cybersecurity action plan.

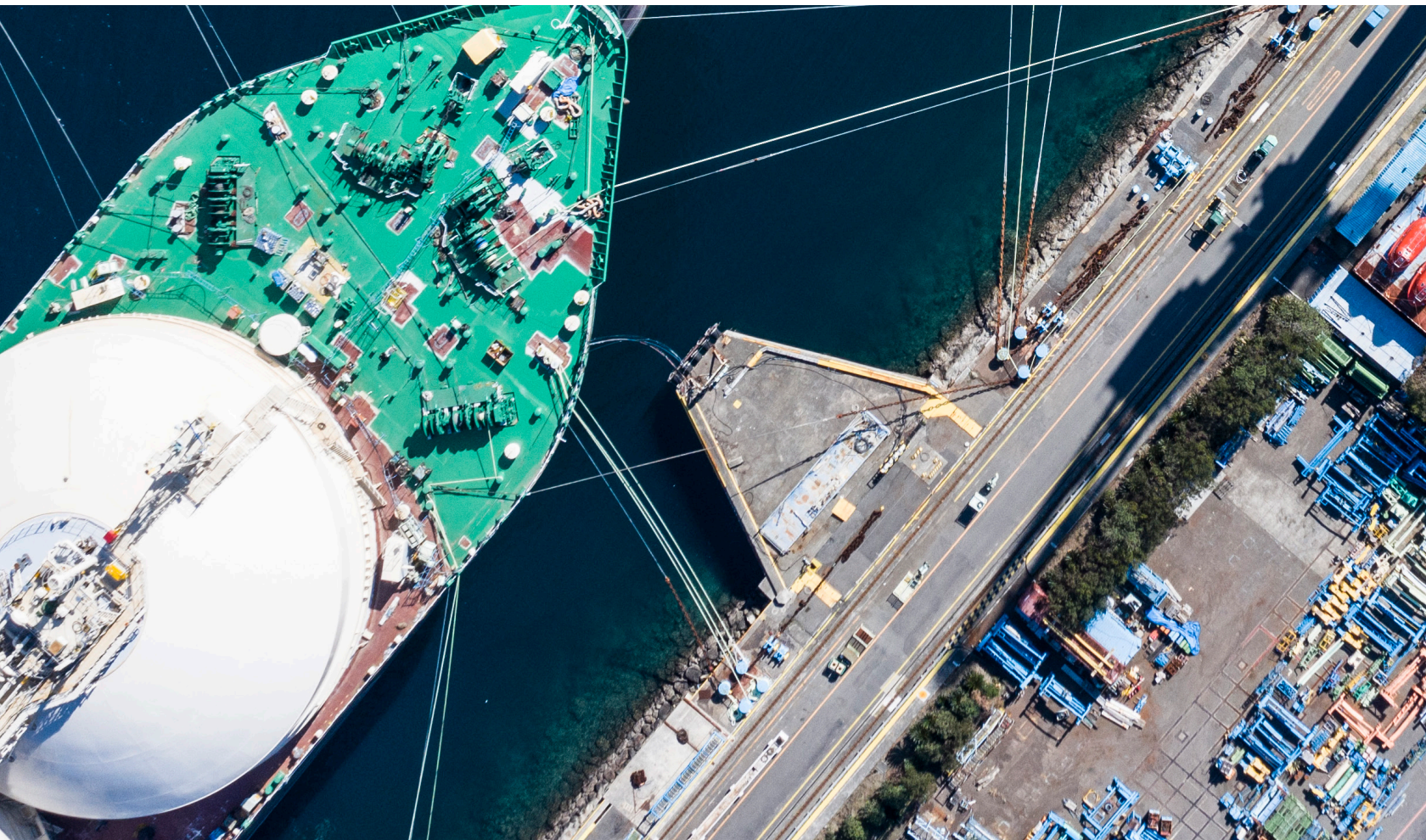


Table of Contents

Mission Secure

Introduction

Maritime is one of the oldest industries and lifeblood of the global economy, accounting for the carriage of 90% of world trade. Ships and other vessels may seem like unusual targets for cyberattacks. But with their growing use of industrial control systems (ICS) and satellite communications, hackers have a new playground that's ripe for attack.

TOP

Maritime History and Definitions

Maritime is one of the oldest industries and lifeblood of the global economy, accounting for the carriage of 90% of world trade. Ships and other vessels may seem like unusual targets for cyberattacks. But with their growing use of industrial control systems (ICS) and satellite communications, hackers have a new playground that's ripe for attack.

In a 2020 Safety at Sea and BIMCO Maritime Cyber Security survey, despite the majority of respondents (77%) viewing cyber-attacks as a high or medium risk to their organizations, few appear to be prepared for the aftermath of such an attack. 64% of respondents said their organization has a business continuity plan in place to follow in the event of a cyber incident, but only 24% claimed it was tested every three months, and only 15% said that it was tested every six to 12 months. Only 42% of respondents said that their organization protects vessels from operational technology (OT) cyber threats, and some respondents went so far as to describe their company policy to OT cyber risk as "careless."

77%

77% view cyber-attacks as high or medium risks

Yet,

42%

only 42% protect vessels from OT cyber threats.

As hackers become even more sophisticated in their tactics, it's inevitable that cyberattacks against OT on ships are becoming the norm rather than the exception. It's time for the maritime industry to take a look at every aspect of their ship operations to ensure they're protected and resilient against these growing threats.

In this guide, we will help you navigate the ins and outs of maritime cybersecurity, address cybersecurity challenges and compliance considerations, and get you geared up to establish your maritime cybersecurity action plan.

Let's get started

Control Systems

From these simple process loops, very complex behavior can be modeled and controlled with nested and/or cascading architectures. Logic can be built to control continuous manufacturing processes, such as those found in a refinery or chemical plant, and batch manufacturing processes, such as is found on an assembly line. Control systems also found their way into distributed applications such as electrical power grids, railways, and pipelines.

Industrial Control Systems (ICS) and Operational Technology (OT)

All of the technologies we have discussed have historically been rolled up under the heading of **industrial control systems (ICS)**. However, the use of the term **operational technology (OT)**, in contradistinction to IT, has become popular in recent years. The analyst firm Gartner defines OT as:

> ***"Hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes and events in asset-centric enterprises, particularly in production and operations."***

This definition makes it clear that the distinction between OT and ICS is not so much in the core functionality of OT but more in the recognition of an evolving definition of "asset-centric" enterprises, with OT now finding application far beyond the traditional "industrial" industries where ICS has found a home for the last 50 years.

Cyber-Physical Systems (CPS)

Another term that is worth remembering is **Cyber-Physical System (CPS)**. Gartner defines CPS as a collection of systems that interact with the physical world through cyber environments. The term is intended to encompass a broader set of applications than traditional OT. Examples include autonomous automobile systems, automatic pilot avionics, and smart grids. Again, all of these terms overlap to some degree and their distinctions in practice can often be found in how they are architected or to whom they are being sold.

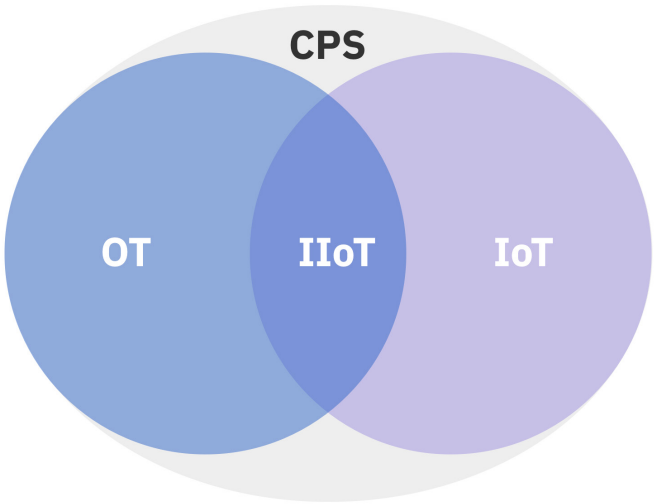


Figure 1: The relationship between CPS, OT, IoT, and IIoT

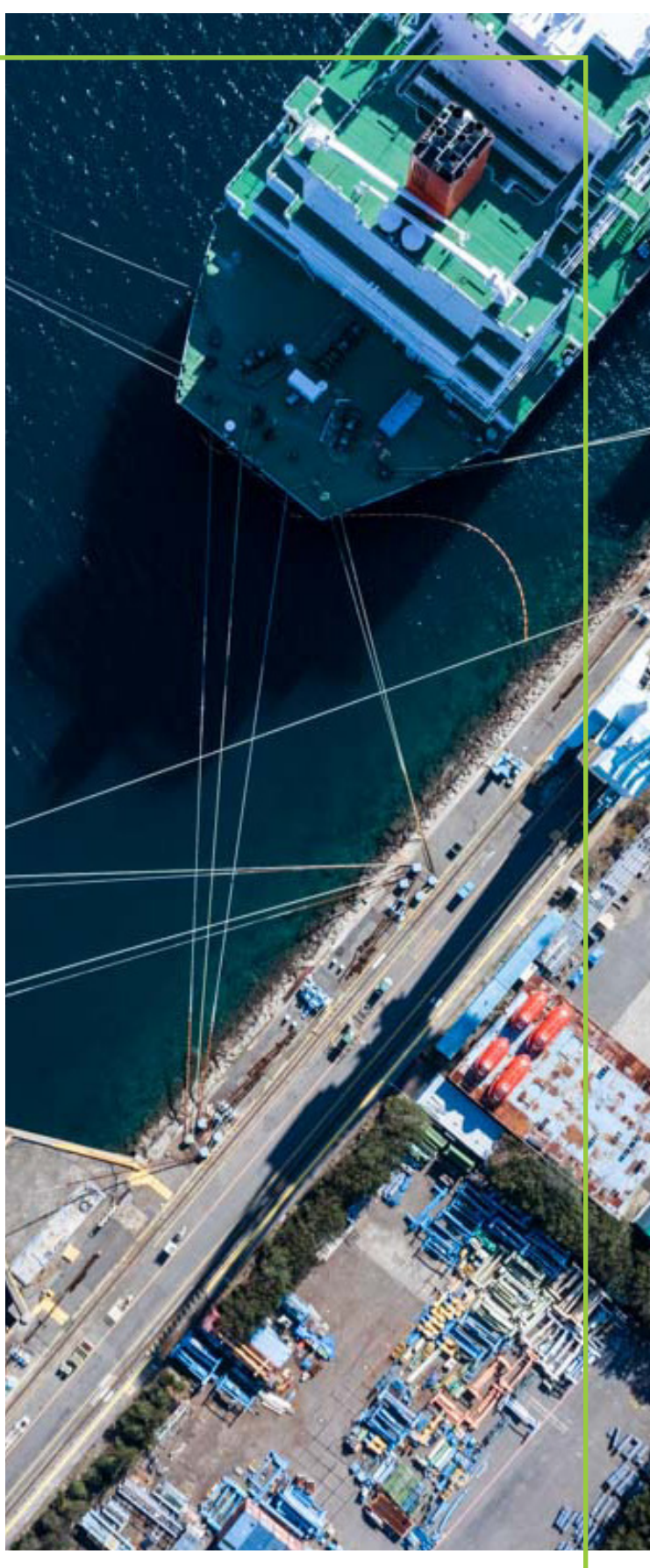
Internet of Things (IoT) and Industrial Internet of Things (IIoT)

Another relatively new term, and one that overlaps considerably with OT, is the **Internet of Things (IoT)**. Like OT, IoT utilizes devices such as actuators and sensors. But IoT architectures are fairly streamlined compared with OT. Typically, an IoT system would consist of endpoint devices connected to an edge gateway, which in turn would connect to cloud services. IoT technologies are often deployed in commercial or even consumer environments, but when applied to industrial applications, they are referred to as the **Industrial Internet of Things (IIoT)**.

Examples of IoT devices include:

- ✓ Electricity/Gas/Water Smart Meters
- ✓ Smart Home
- ✓ Building Automation
- ✓ Vehicle Head Unit
- ✓ Security & Fire Alarms
- ✓ Inventory Management
- ✓ CCTV
- ✓ Healthcare Monitoring
- ✓ Assisted Living Monitoring

IoT leverages several new technologies that have significantly reduced the difficulty and cost of deploying monitoring and control systems, particularly in highly geographically distributed environments. These technologies include real-time analytics, commodity sensors, sophisticated embedded systems, cloud storage and computing, and 5G networks. The sophistication of analytics, the ubiquity of bandwidth—wired and wireless—and the low price of data storage and compact multi-purpose sensors have all converged to make it much cheaper and easier to collect, analyze and act, on massive amounts of data about the world around us.



Mission Secure

What is Maritime Cybersecurity

Maritime cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies used to protect maritime organizations, their vessels, and their cyber environment.

TOP

Cybersecurity Concerns with IT and OT Integration

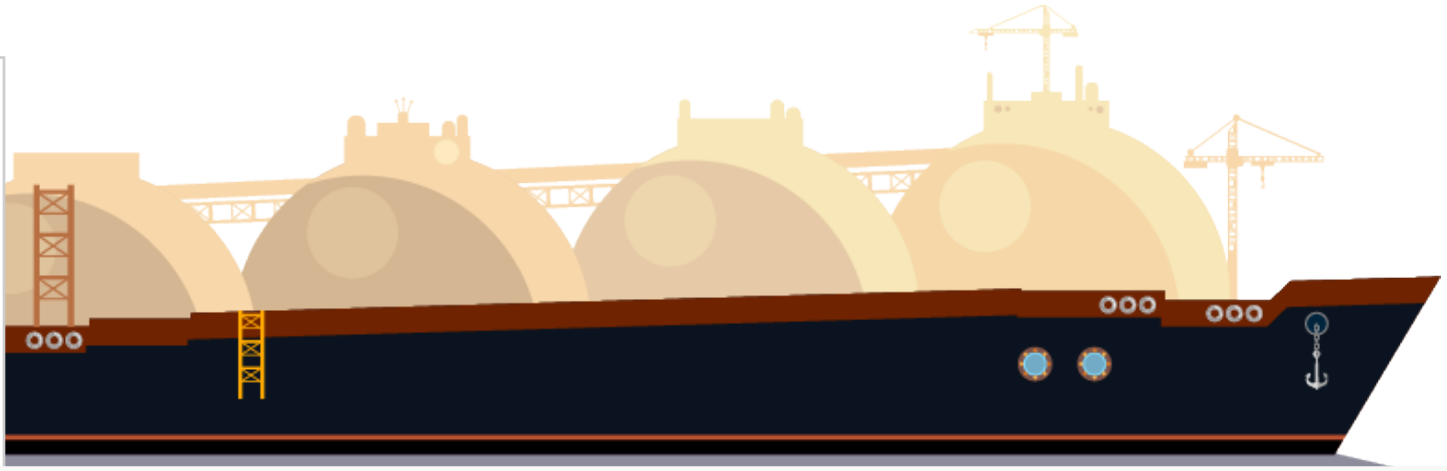
And according to the International Maritime Organization (IMO), maritime cyber risk refers to a measure of the extent to which a technology asset could be threatened by a potential circumstance or event, which may result in shipping-related operational, safety or security failures as a consequence of information or systems being corrupted, lost or compromised.

Many of the globally connected networks and infrastructures at sea still leverage legacy technologies that were not built to be connected to the Internet. These complex networks include a blend of information technology (IT) and operational technology (OT) systems (we'll cover those in the next section) used by internal crew and third-party vendors, extending the potential for a compromise by hackers or insider threats.

> ***...the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies used to protect maritime organizations, their vessels, and their cyber environment.***

Connectivity on A Modern Maritime Vessel

There was a time when connectivity on a vessel was minimal, and ship control engineers addressed security issues with air gapping to physically isolate a secure network from unsecured networks. By definition, an air-gapped system is neither connected to the Internet nor any other system. But now, using something as simple as a USB flash drive or unsecured Wi-Fi connection, a malicious hacker or even an inexperienced insider could infiltrate and infect critical systems. This development is especially concerning given the connectivity of modern maritime vessels:



Bridge Control:
Bridge systems, automatic identification system (AIS), voyage data recorder (VDR), automatic radar plotting aid (ARPA)

Operations Security:
Human-machine interfaces (HMIs), logic controllers (PLCs), digital and analog sensors, electronics

Safety Systems:
Fire and flood control, tracking, shipboard security, CCTV, emergency shutdown

Propulsion & Power:
Engine control, steering, fuel management, onboard machinery monitoring,

Network Security:
Firewalls, segmentation devices, antivirus software, software updates, vendor patches

Communications:
Satellite internet communications, ship-to-shore, ship-to-ship, handheld radios, voice-over-IP (VoIP)

Navigation:
GPS/GNSS, electronic chart display and information system (ECDIS), radar, weather systemsmonitoring,

Physical Security:
Server rooms, access control, bridge, machinery spaces, network infrastructure

Crew Network:
Email, Wi-Fi, wired, bring your own device (BYOD)

Loading & Stability:
Ballast systems, hull stress, stability control, stability decision support systems, cargo management system

Ship Networks:
Email, customs and immigration, personnel administration, maintenance and spares management

Supply Chain:
Remote or on-shore vendor updates, maintenance, and administration

Whether moving dry or liquid bulk, containers or cars, crude oil, products, or chemicals, the maritime industry is a critical backbone of our global economy. Protecting a vessel's critical operations from cyber threats poses unique challenges with operation centers and fleets of numerous classes and vintages spread across the world, increasingly digitalized operations, and a complex environment merging IT with industrial control systems (ICS) and operational technology (OT).

Real-World Lessons Learned from Maritime Cybersecurity Incidents

Current Threats to Maritime Security

If you're in charge of cybersecurity for your maritime vessel networks, the last thing you want to wake up to is your mobile phone blowing up and your organization in the headlines because of a cyberattack. Between vessels being more connected than ever, the flourishing cybercrime economy contributing to over $1 trillion in losses and a global pandemic that has changed how we work, it seems that it's all you can do to keep your vessel networks running.

With a 400% increase in attempted cyberattacks targeting the maritime industry since February 2020, it's not just keeping your networks running that will keep you up at night. The global pandemic has brought on an influx of cybersecurity issues, including but not limited to phishing attempts, ransomware, employees working remotely, and network access adjustments due to travel restrictions. But hopefully, you've deployed your cybersecurity risk management plan and developed an optimal design for your vessel network infrastructure. Even after all of that, your hard work might have just delayed the inevitable – the day your organization ends up in the headlines. The good news is that sometimes, hindsight doesn't have to be 20/20.

In this blog, we will walk through three cybersecurity incidents that made headlines in the maritime industry and detail the lessons learned from each event that can help you stay ahead of potentially catastrophic cyberattacks.

Maritime Cyber Attacks 2017 | Incident #1: Maersk

In June 2017, Danish shipping giant Maersk suffered one of the most high-profile and damaging maritime cybersecurity incidents to date. The largest container ship and supply vessel operator with offices across 130 countries and over 80,000 employees went dark after being hit with NotPetya.

What's interesting about NotPetya is that while it has the general characteristics of ransomware, it is not technically ransomware. It's able to spread on its own without any spam emails or social engineering. It relies on tools like the EternalBlue and EternalRomance exploits developed by the US National Security Agency (NSA). Designed as a wiper, NotPetya encrypts everything in its path and damages the data beyond repair with no way to recover. What was allegedly a state-sponsored Russian cyberattack targeted at Ukrainian companies, NotPetya spread beyond the Ukrainian borders and caused an estimated $10 billion in total damages worldwide.

When NotPetya hit Maersk, it propagated through the network in **seven minutes**. Computer screens faded to black, and employees scrambled to unplug any connected devices throughout the offices to protect against the fast-spreading malware. Except for an undamaged domain controller from the Ghana office that had experienced an unrelated power outage, Maersk lost most of its data, with over 49,000 laptops and 4,000 servers destroyed. Damages were estimated at over $300 million.

"In the event that we see something suspicious going on in the network, we don't just flag it – we stop it."

– Maersk's CISO

Lessons Learned from Maersk

Beyond Protection, Focus on Response Plans: You have to assume that hackers are already in your network, and you need extra intelligence to assess what or who is in your network. Maersk has invested in a separate internal threat team that studies emerging threats and determines how to respond to and mitigate future avenues of attack. Your response plans should be tested and updated frequently to improve processes, identify any shortcomings and determine new mitigation actions against any emerging cyberattacks.

Establish a Data Protection and Recovery Strategy: Yes, you need to ensure your vessel network and critical control systems are protected, but you also need a data protection and recovery plan in place so that if your network is knocked offline, you can still operate. You also need to rethink your backups. Standard online backups are no longer a safe approach. If your backups are attached to your network, they're susceptible to attack. You

need to protect your vessel OT network against data loss and be able to reconstruct your database after data loss, and the addition of offline backups should be considered.

Maritime Cyber Attacks 2018 | Incident #2: COSCO

Just over a year after the Maersk attack, it was time to find out if the maritime industry had taken steps to strengthen their cybersecurity defenses. That test would come in July 2018, when the China Ocean Shipping Company (COSCO) became a victim of the SamSam ransomware. When SamSam hit, it caused a failure across COSCO's networks in the United States, Canada, Panama, Argentina, Brazil, Peru, Chile and Uruguay.

Similar to NotPetya, once SamSam gains access to your network, hackers can gain administrative rights and run executable files without human action or authorization. The group behind SamSam doesn't push their ransomware as a commodity through a SaaS model – they keep development in-house and update it frequently to avoid enterprise security defenses.

The SamSam attack occurred soon after COSCO acquired one of its rivals, Orient Overseas Container Lines. By activating their contingency plans, COSCO's operations were back to normal in five days. Any damages from the cyberattack have not been disclosed.

Lessons Learned from COSCO

Segment Your Maritime Networks: Because COSCO had isolated its internal networks across the globe, they were able to contain the damage. Network segmentation helps you reduce the attack surface and is a very useful architectural concept of a defense-in-depth cybersecurity strategy. Your OT and IT networks need to be segmented to limit the spread of a cyberattack and stop it from spreading laterally toward your critical vessel controls.

Have a Contingency Plan: As with any organization, those in the maritime industry need to have a contingency plan in place that will keep operations running in the interim while they recover from a cyberattack. In COSCO's case, they made sure that they had alternative procedures to communicate with customers and deal with service requests. They also utilized social media to reply directly to service requests and updated a FAQ document every time there was a status change. While the process of communicating with customers via emails and phone calls took up a little more time, they were able to continue cargo handling in the United States and Canada without any

disruptions.

Maritime Cyber Attacks 2019 | Incident #3: Norsk Hydro

In March 2019, a crippling ransomware attack brought Norsk Hydro's worldwide network down to its knees, when they fell victim to the LockerGoga ransomware.

LockerGoga's wrath is especially tumultuous because it disables the computer's network adapter to disconnect it from the network, changes both user and admin passwords and logs the machine off. LockerGoga will sometimes leave the victim without the ability to see the ransom message or even know that they've been hit with the ransomware, further delaying an organization's ability to recover their systems.

Norsk Hydro estimated that the hackers had been in their network two or three weeks before they were discovered. With over 22,000 computers and thousands of servers affected over five continents, LockerGoga

```
Greetings!

There was a significant flaw in the security system of your company.
You should be thankful that the flaw was exploited by serious people and not some rookies.
They would have damaged all of your data by mistake or for fun.

Your files are encrypted with the strongest military algorithms RSA4096 and AES-256.
Without our special decoder it is impossible to restore the data.
Attempts to restore your data with third party software as Photorec, RannohDecryptor etc.
will lead to irreversible destruction of your data.
```

Text file message included on a Norsk Hydro system from the hackers

brought down Norsk Hydro's entire worldwide network, affecting their production and office operations. Damages were estimated at $71 million.

Lessons Learned from Norsk Hydro

Be Transparent: Just like Maersk, Norsk Hydro shared more information than usual with the authorities, giving investigators enough information to warn other organizations to prevent similar attacks. Norsk Hydro took their transparency to the next level to keep everyone informed. They held daily press conferences at their Oslo headquarters, set up a temporary website, provided updates on Facebook and conducted daily webcasts hosted by senior staff who answered audience questions.

Never Let Your Guard Down: It took several months for Norsk Hydro to rebuild its infrastructure and deploy a segmented network to ensure that IT and OT were protected. During their initial investigations, they found

several variants of the virus that hackers had planted just in case they weren't successful the first time. Hackers spend many hours developing, testing and executing their attacks, and you need to take that same approach with your cybersecurity strategy. Keeping your networks secure is a company-wide responsibility. It requires consistent security awareness and education for the organization and ongoing monitoring of your cybersecurity framework to minimize risk across your maritime environment.

"Gradually, new computers and servers are connected to these zones, and more and more employees can now connect to the network. The danger is still not over."

– Norsk Hydro's IT Manager

A Recap of Lessons Learned

While the Norsk Hydro cyberattack isn't maritime-related, it serves as a wake-up call for the industry. Hackers do not discriminate – they are hitting organizations large and small, with or without abundant cybersecurity resources. Protecting your vessel OT environment is no easy task, but with the right security measures and procedures in place to help you maintain the integrity and continuity of your vessel operations, you're off to a good start keeping ahead of malicious hackers.

Let's recap our lessons learned for vessel cybersecurity and effective cyber risk management:
Beyond Protection, Focus on Response Plans: Your response plans need to be tested and updated frequently to identify any shortcomings, improve processes and determine new mitigation actions.

Establish a Data Protection and Recovery Strategy: A data protection and recovery plan will help you keep operations running in the event your network is knocked offline.

Segment Your Maritime Networks: Segmenting your networks will limit the spread of a cyberattack toward your critical vessel controls.
Have a Contingency Plan: A concrete contingency plan will help keep your operations running in the interim while your organization recovers from a cyberattack.

Be Transparent: Be transparent to help the authorities and help others in the maritime industry learn from your experience so that they are better prepared.

Never Let Your Guard Down: Protecting your maritime network requires consistent security awareness and education and ongoing monitoring of your cybersecurity framework.

Mission Secure

How do IT and OT Cybersecurity Differ?

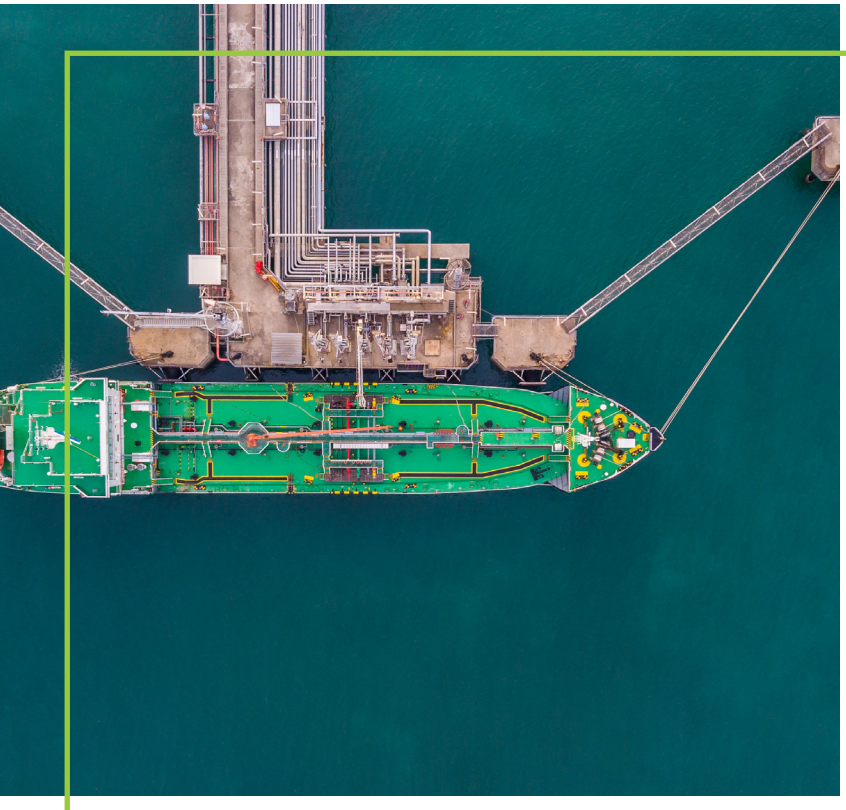
Before we delve into the cybersecurity challenges affecting the maritime industry, let's take a step back and examine some of the differences between IT and OT systems.

TOP

What is Operational Technology (OT)

Operational technology (OT) is hardware and software that detects or causes a change through the direct monitoring and control of industrial equipment, assets, processes, and events. In contrast, information technology covers the entire spectrum of technologies for information processing, including software, hardware, communications technologies, and related services.

> ***An attack on IT could lead to data theft, while an attack on OT could lead to injury or loss of life, asset damage, or environmental impact.***



Differences in System Requirements

Before we delve into the cybersecurity challenges affecting the maritime industry, let's take a step back and examine some of the differences between IT and OT systems. Some of the differences in system requirements include:

- **Performance**
- **Availability/Reliability**
- **Risk Management**
- **System Operation**
- **Resource Constraints**
- **Communications**
- **Component Lifetime**
- **Component Location**

Performance

IT System Requirements

- ✓ Non-real-time
- ✓ Response must be consistent
- ✓ Less critical emergency interaction
- ✓ Tightly restricted access control can be implemented to the degree necessary for security

OT System Requirements

- ✓ Real-time
- ✓ Response is time-critical
- ✓ Response to human and other emergency interaction is critical
- ✓ Access should be strictly controlled, but should not hamper or interfere with human-machine interaction

Availability/Reliability

IT System Requirements

- ✓ Responses such as rebooting are acceptable
- ✓ Availability deficiencies can often be tolerated, depending on the system's operational requirements

OT System Requirements

- ✓ Responses such as rebooting may not be acceptable because of operational requirements
- ✓ Availability requirements may necessitate redundant systems

Risk Management

IT System Requirements

- ✓ Manage data
- ✓ Data confidentiality and integrity is paramount
- ✓ Fault tolerance is less critical – momentary downtime is not a major risk
- ✓ Significant risk impacts may lead to delays in ship clearance, loading/unloading, business operations

OT System Requirements

- ✓ Control physical world
- ✓ Human safety is paramount, followed by protection of the process
- ✓ Fault tolerance is essential; even momentary downtime may not be acceptable
- ✓ Major risk impacts are regulatory non-compliance, environmental impacts, harm to the crew onboard, equipment and/or cargo

System Operation

IT System Requirements

- ✓ Systems are designed for use with typical operating systems
- ✓ Upgrades are straightforward with the availability of automated deployment tools

OT System Requirements

- ✓ Differing and possibly proprietary operating systems, often without security capabilities built-in
- ✓ Software changes must be carefully made, usually by software vendors, because of the specialized control algorithms and modified hardware and software involved

Resource Constraints

IT System Requirements

- ✓ Systems are specified with enough resources to support the addition of third-party applications such as security solutions

OT System Requirements

- ✓ Systems are designed to support the intended industrial process and may not have enough memory and computing resources to support the addition of security capabilities

Communications

IT System Requirements

- ✓ Standard communications protocols
- ✓ Primarily wired networks with some localized wireless capabilities
- ✓ Typical IT networking practices Manage data

OT System Requirements

- ✓ Many proprietary and standard communication protocols
- ✓ Several types of communications media used, including radio, satellite Internet, ship to shore, ship to ship, VoIP
- ✓ Networks are complex and sometimes require the expertise of control engineers

Component Lifetime

IT System Requirements

- ✓ 3 to 5 years

OT System Requirements

- ✓ 10 to 15 years

Component Location

IT System Requirements

- ✓ Components are usually local and easy to access

OT System Requirements

- ✓ Components can be isolated, remote, and might require extensive physical effort to gain access to them

*Table modified from NIST Special Publication 800-82, Revision 2 (Table 2-1)

From a cybersecurity perspective, OT and IT are different in several ways. On staffing, there is a cybersecurity specialization on the IT side. Professionals have been specifically trained and certified in application security, network security, or other security disciplines. In OT, those tasked with security are usually operational technology people. As part of their day job, they have to also deal with security—it's an add-on, not a specialization.

OT and IT are different, especially in attack outcomes. An attack on IT could lead to data theft, while an attack on OT could lead to injury or loss of life, asset damage, or environmental impact. Traditional cybersecurity measures fail to protect vessels from cyber-attacks and leave the OT network exposed, falling short on providing the visibility and protection required for cyber-physical processes underlying in the maritime industry. And with the convergence of IT and OT, organizations must balance the use of traditional IT security tools at the network and endpoint layer with specialized security tools designed for OT requirements.

CIA vs. CAIC

One of the best ways to distinguish the difference between IT security and OT security is the CIA triad. The CIA triad is a model designed to guide policies for information security within an organization. Ranked in order of priority, CIA stands for confidentiality, integrity, and availability.

Figure 4: Comparing the IT CIA Model to the OT CAIC Model of Priorities

IT Priorities vs. OT Priorities

By contrast, the OT benchmark is CAIC, which stands for control, availability, integrity, and confidentiality. Although OT cares about the same security properties, they're ranked in a different order, with safety forever being the top priority.

In the CAIC model, availability is more important than confidentiality because of the nature of processes and the impact that shutting down and restarting systems can have on productivity. Control refers to the ability to control a process and change a state when needed in a safe and secure manner. Since it can impact people, safety, and assets, it will have the highest priority when considering the attack surface of any system.

Maritime Security Challenges: The Physical Impact of Maritime Cyber Threats

An attack on an OT network (or maritime vessel network) can have disastrous consequences and lead to injury, loss of life, asset damage or environmental impact.

When we see a dangerous security vulnerability or debilitating cyberattack appear in the (almost) daily headlines, the story is usually the same: a hacker compromises an enterprise network and steals personnel data, credit card numbers, product roadmaps, confidential emails and more. And just for fun (and money), a hacker will hold the data for a sizeable ransom and threaten to publish the information if the payment isn't received.

But there is a whole other world of cyberattacks, where hackers target operational technology (OT) environments that support infrastructures in manufacturing, transportation, defense, utilities and others.

An attack on an OT network (or maritime vessel network) can have disastrous consequences and lead to injury, loss of life, asset damage or environmental impact.

In this post, we'll dive into how a hacker can attempt to compromise the on-vessel OT network, look at a couple of real-world examples and help you eliminate the physical impact of cyber threats in your maritime environment.

Let's Get Physical: A Hacker's Approach

In IIoT deployments, data is not constrained by traditional Purdue hierarchies, and in fact, data no longer lives entirely within the enterprise.

The allure of hacking industrial systems and programmable logic controllers (PLCs) on maritime vessels stems from their lack of built-in security. Also, maritime vessel networks have historically been flat and isolated, with air-gapping as the "security solution" of choice. Because of this, security had not been top of mind. But as these networks become more connected, the attack surface on a vessel increases. With inadequate or no segmentation at all between the IT and vessel networks, the threat of malware making its way into the vessel networks and spreading laterally toward critical controls is real.

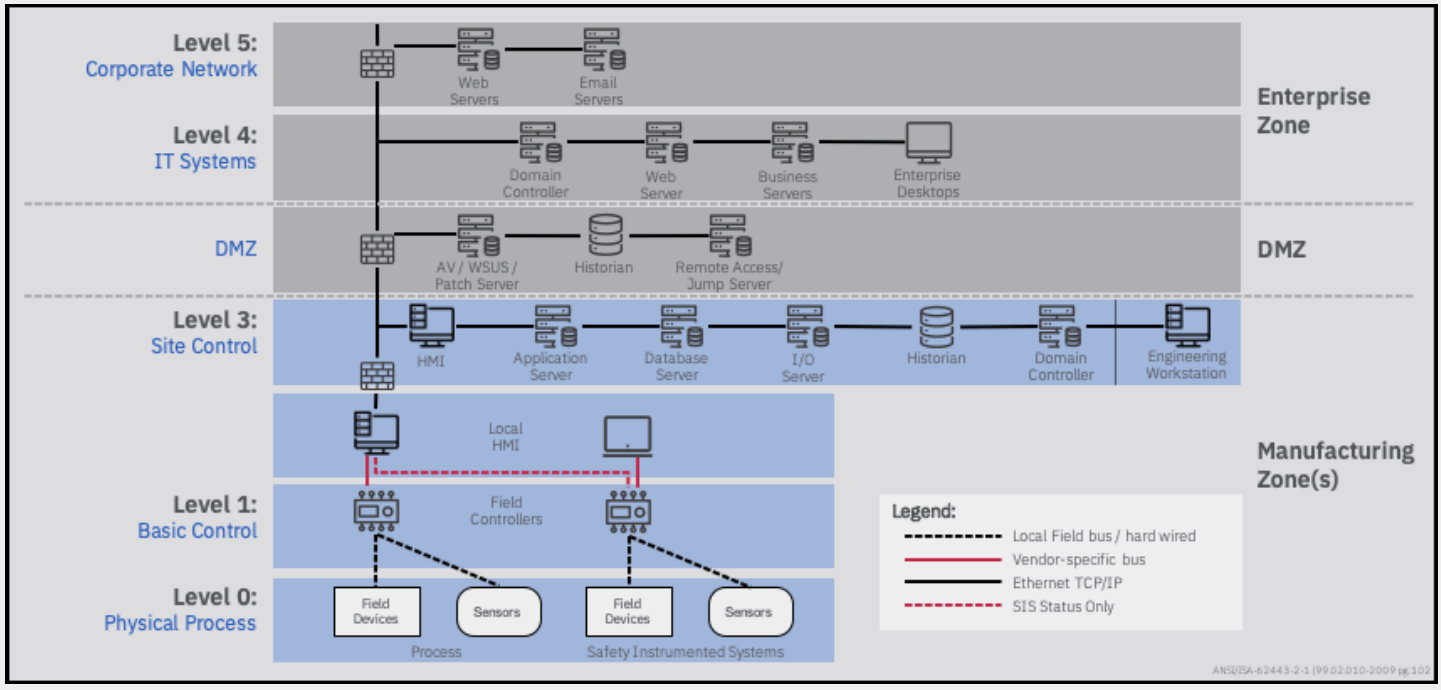


Figure 1: Purdue Enterprise Reference Architecture

As maritime organizations review and adjust their security architectures, one of the recommended frameworks for them to adopt is the Purdue model.

Maritime Security Challenges: The Physical Impact of Maritime Cyber Threats

If we look at a typical attack sequence, a hacker will probably attempt to infiltrate the vessel's OT network through various methods. They will look for vulnerable entry points through satellite communications terminals, open or unprotected Wi-Fi networks, endpoints in the IT/corporate network and maritime-specific systems. Some common attack vectors include spear phishing, compromised or misconfigured endpoints, and stolen credentials. If the hacker is onboard, they can infiltrate systems directly with infected USB thumb drives.

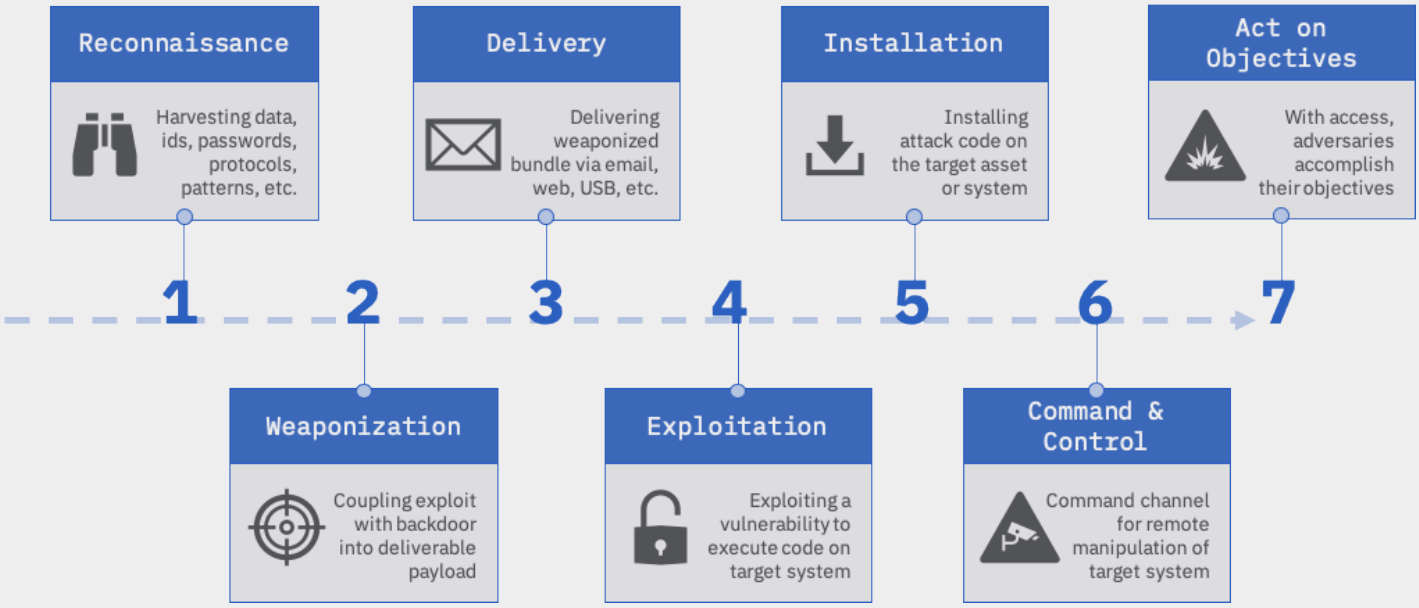


Figure 2: Hacker Attack Sequence

Once they get in, they'll hide through various obfuscation methods and eventually assume control of critical control systems and devices. The hacker can now compromise things like navigation and communications systems, open or close critical valves, and take over propulsion and rudder controls – and the consequences can be disastrous.

Maritime Security Incidents: Physical Cyber Threats in the Real-World

There have been a growing number of cyberthreats targeting OT networks, but more often than not, those incidents are not reported. According to the SANS 2019 State of OT/ICS Cybersecurity Survey, despite the growing demand to publicly acknowledge incidents, 43% of respondents admit being restricted by internal policy from sharing such information outside of official organizational channels, as opposed to 25% in 2017. In fact, the United States Coast Guard's 2018 warning on the Emotet malware came after a merchant vessel was infected with it due to an almost total lack of cybersecurity safeguards. The ship was not named to encourage others to report cybersecurity incidents. And since the Coast Guard's 2018 warning, there have been additional warnings issued, and they have shared cybersecurity best practices for commercial vessels.

On July 5, 2020, X-FAB Group, a leading analog/mixed-signal and micro-electro-mechanical systems foundry group manufacturing silicon wafers for automotive, industrial, consumer, medical and other applications, became the latest victim of Maze ransomware. The attack resulted in a total shutdown of X-FAB Group's IT systems and production at all six manufacturing sites, as well as the postponement of the company's publication of second-quarter results. Also, the group behind the attack has publicly released some of the data stolen from the company in the form of zip files. As of July 13, 2020, production has resumed at one of X-FAB Group's manufacturing sites, with the others back in production as of August 27, 2020.

In 2015, a steel mill in Germany was struck by hackers in what was, at the time, only the second confirmed case of a cyberattack causing physical damage (Stuxnet being the first). Hackers gained access to the steel mill through the enterprise network via a spear-phishing attack and were then able to work their way into production networks to access systems that controlled plant equipment. Showing expertise in their knowledge of industrial control systems, the hackers were able to compromise individual control components and even entire systems. The plant was unable to shut down a blast furnace, resulting in massive damage to the system.

In the maritime cybersecurity world, Danish shipping giant Maersk (A.P. Møller-Maersk) fell victim to NotPetya in June 2017. While Maersk lost most of its data, applications, over 49,000 laptops and almost half of their servers, the computers on their actual ships were spared. However, the terminals' software designed to receive the Electronic Data Interchange files from those ships had been wiped entirely.

Where ships' systems were affected occurred in June 2017, when a GPS spoofing attack involving over 20 ships in the Black Sea made them "disappear." Instead of showing actual positions, ships were being shown 25 to 30 miles away at Gelendzhik airport. When one ship operator radioed the other vessels, it was confirmed that there was an issue with everyone's GPS. GPS spoofing can deliver potentially catastrophic consequences: ships could be directed off course and criminals could take advantage to steal precious cargo.

Maritime Security Today: How Can You Eliminate the Physical Impact of Maritime Cyberthreats?

Before you can eliminate the physical impact of maritime cyberthreats, you need to have a baseline understanding of what is in your IT/OT network environment so that you can classify and manage them appropriately. Then you can analyze communication flows, identify any security gaps and take the appropriate actions to:

Protect: Restrict unauthorized access and block abnormal or malicious activity from reaching important controllers and Level 1 devices.

Monitor: Continuously monitor network IP levels, alongside digital and analog signals with a secure, multi-layered system.

Detect: Conduct analysis in real-time with automated incident detection.

Inform: Keep trusted operators and cybersecurity professionals informed through dedicated communications systems.

Collect: Gather system data from digital and analog sensors, actuators, controllers, and the OT network for forensic purposes.

Correct: Execute automated or operator-guided responses, system restorations, and reset functions to safe operating states.

Mission Secure

What are the Cybersecurity Challenges Affecting the Maritime Industry?

When we see a dangerous security vulnerability or debilitating cyberattack appear in the (almost) daily headlines, the story is usually the same: a hacker compromises an enterprise network and steals personnel data, credit card numbers, product roadmaps, confidential emails and more. And just for fun (and money), a hacker will hold the data for a sizeable ransom and threaten to publish the information if the payment isn't received.

But there is a whole other world of cyberattacks, where hackers target operational technology (OT) environments that support infrastructures in manufacturing, transportation, defense, utilities and others.

TOP

Comparing the IT CIA Model with the OT CAIC Model of Priorities

Many of the common cybersecurity challenges that affect the maritime industry mirror those in other industries that deal with IT networks:

- ✓ No clear understanding of all systems and devices on the OT network across a fleet or operation
- ✓ Lack of visibility into each vessel's OT networks
- ✓ Lack of real-time monitoring or segmentation of the OT network
- ✓ Inadvertently connected IT and OT networks
- ✓ Use of unsecured wireless networks
- ✓ 24/7 remote access granted to third-party OEMs
- ✓ Lack of visibility into third-party OEM networks (black box)
- ✓ Poor physical security controls
- ✓ Lack of cybersecurity awareness among the crew, employees, and contractors

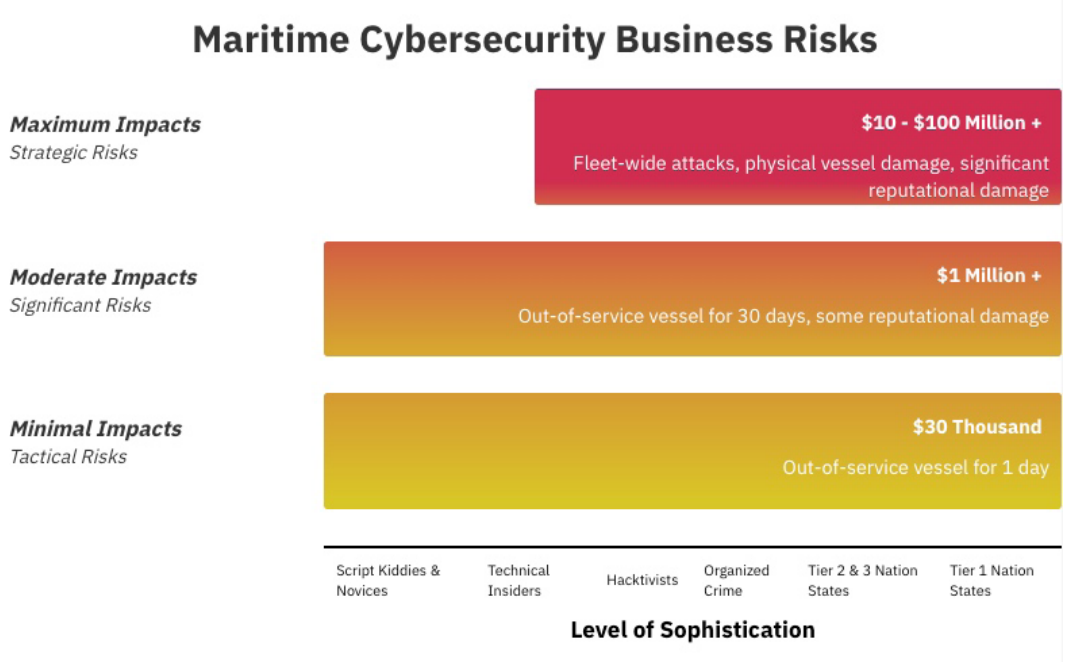
> ***Maintaining control of all physical assets to ensure their safe operation at all times is the primary objective of OT cybersecurity and overrides all other concerns.***

Potential Maritime Cybersecurity Attacks

Cybersecurity is not just about preventing hackers from gaining access to systems and information. It is also about protecting digital assets and data, ensuring business continuity, and ensuring that the maritime industry is resilient to external and internal threats. It is crucial to keep ship systems safe from physical attacks and to ensure the integrity of supporting systems.

The complexities associated with vessels and tankers make them vulnerable to high-impact attacks. Cyber incidents can last for hours, days, or weeks. When one ship is impacted, it can often spread malware to sister vessels via the corporate network. Some of the potential attacks that can cripple a vessel's operations include:

- ✓ An attack on an OEM network or third-party supplier that spreads to their client's on-vessel OT network
- ✓ An attack on a satellite provider that gains access to a vessel's IT/OT network
- ✓ Exploited cyber vulnerabilities that grant access to a vessel's OT network and provide various attack options, including:
    - ✓ GPS/navigation system attack
    - ✓ Open/close critical valves
    - ✓ Propulsion and rudder control
    - ✓ Ballast control
    - ✓ Ransomware/Malware
    - ✓ Gain full administrative privileges



A compromised ship system could initiate physical harm to the IT and OT systems, personnel, and cargo, potentially endangering lives or causing the loss of the ship and the loss of sensitive information, including commercially-sensitive or personal data.

Recent Maritime Cybersecurity Attacks

Cybersecurity attacks are not new in the maritime industry, but many incidents go unreported. There is an ongoing reluctance to share critical information with law enforcement agencies and collaborate with other peers to share threat information to thwart future attacks and build cybersecurity best practices. And with the rate of maritime cyberattacks increasing by 900% since 2017, the number of reported incidents is set to reach a record by the end of 2020. A

sampling of cyberattacks affecting the maritime industry in 2020 alone shows that all organizations can be susceptible to attack, regardless of size or location:

APRIL 2020

Mediterranean Shipping Company (MSC)

Geneva, Switzerland

Incident Type: Malware
Malware: Unknown

APRIL 2020

DESMI

Denmark

Incident Type: Ransomware
Malware: Unknown

MAY 2020

Shahid Rajaee Port Terminal

Iran

Incident Type: Unidentified Hacker(s)
Malware: Unknown

MAY 2020

Toll

Australia

Incident Type: Ransomware
Malware: Nefilim

MAY 2020

Anglo-Eastern

Hong Kong

Incident Type: Ransomware
Malware: Unknown

JUNE 2020

Vard

International

Incident Type: Ransomware
Malware: Unknown

AUGUST 2020

Carnival Corporation

International

Incident Type: Ransomware
Malware: Unknown

SEPTEMBER 2020

CMA CGM SA

Asia-Pacific

Incident Type: Ransomware
Malware: Ragnar Locker

SEPTEMBER 2020

US Tugboat

Louisiana, United States

Incident Type: Phishing Email
Malware: Unknown

OCTOBER 2020

The International Maritime Organization (IMO)

International

Incident Type: Malware
Malware: Unknown

OCTOBER 2020

Iran Port Authority

Iran

Incident Type: Unidentified Hacker(s)
Malware: Unknown

OCTOBER 2020

Red Funnel

United Kingdom

Incident Type: Unidentified Hacker(s)
Malware: Unknown

NOVEMBER 2020

Port of Kennewick

Washington, United States

Incident Type: Ransomware

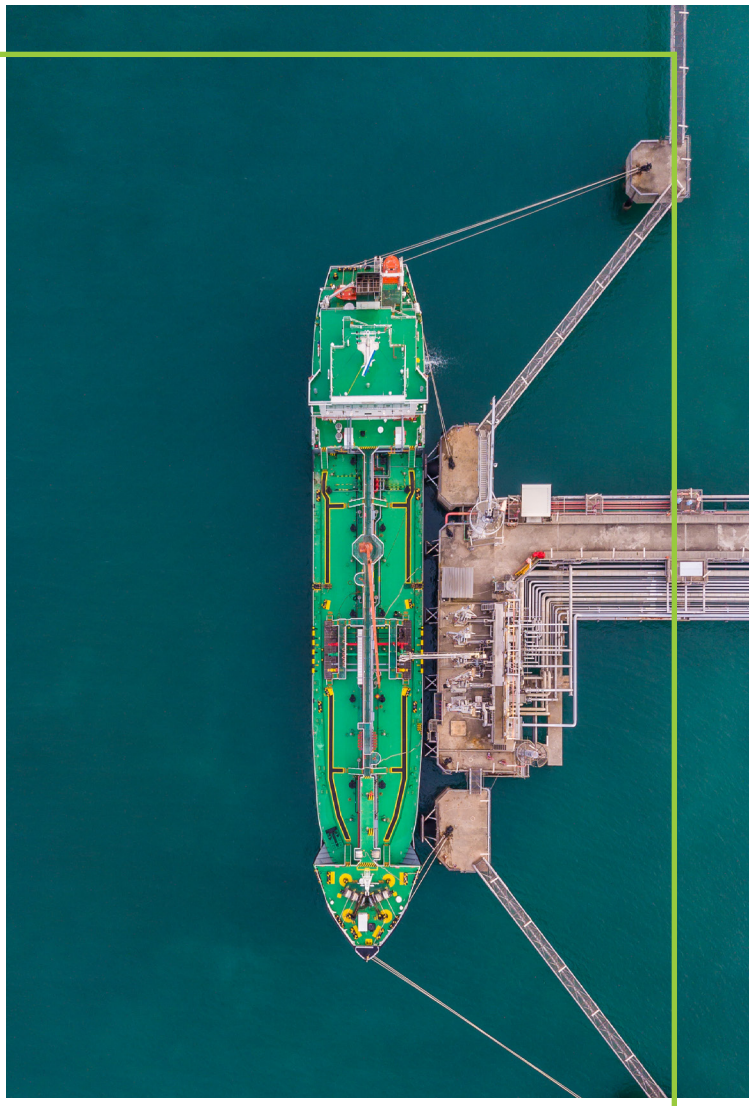
Malware: Unknown

Maritime Security Incidents: NotPetya

One of the most significant and most devastating cyberattacks to date is NotPetya, which caused more than $10 billion in total damages in June 2017. Primarily targeted at Ukrainian companies, NotPetya's reach went far beyond Ukraine and hit many large organizations, including pharmaceutical company Merck, delivery company FedEx and Danish shipping giant Maersk (A.P. Møller-Maersk), which handles one out of seven containers shipped globally.

Maersk was hit particularly hard, to the tune of $300 million and lost most of its data:

- ✓ All end-user devices, including 49,000 laptops and print capability, were destroyed
- ✓ All of their 1,200 applications were inaccessible, and approximately 1,000 were destroyed
- ✓ Data was preserved on back-ups, but the applications themselves couldn't be restored as they would be reinfected
- ✓ 3,500 of their 6,200 servers were destroyed and couldn't be reinstalled
- ✓ All fixed-line phones were inoperable due to the network damage, and because they'd been synchronized with Outlook, all contacts had been wiped from mobiles, severely hampering any coordinated response



Maritime Security Incidents: COVID-19 Pandemic

More recently, with the onset of the COVID-19 pandemic, the number of shipping cyberattacks has jumped 400% since February.

Travel restrictions, social distancing, and the economic recession are having an impact on the maritime industry and its ability to protect itself. OEMs, technicians, and vendors are forced to connect standalone systems to the Internet to service them. Ship and offshore staff are connecting their OT systems to onshore networks for brief periods to carry out diagnostics and upload software updates, leaving endpoints, critical systems, and components susceptible to attack since they are no longer segmented. Also, stress levels of short-staffed crews can leave vessels vulnerable to scams, misconfigurations, and human error.

Maritime Security Incidents: Disruptive Cyber-attack Cripples Port Facility

Geopolitical tensions are one of many maritime security challenges. It's critical to have strong security measures in place across your vessel OT networks and between your interactions with port terminals.

On May 9, 2020, all shipping traffic at the Shahid Rajaee port terminal in Iran came to an abrupt halt. According to The Washington Post, an unknown foreign hacker briefly knocked the port's computers offline, which led to massive backups on waterways and roads leading to the terminal.

Maritime networks have become an attractive playground for hackers, with cyber-attacks on vessel OT networks and systems increasing by 900% over the past three years. Attacks on vessel OT networks can be catastrophic, leading to injury, loss of life, asset damage or environmental impact.

In this post, we'll walk through what happened at the Shahid Rajaee port terminal, why it happened, the aftermath, and how you can ensure your vessel OT networks are protected against debilitating cyberattacks.

What Happened?

The Shahid Rajaee port facility is the newest of two major shipping terminals in the Iranian coastal city of Bandar Abbas, on the Strait of Hormuz. Computers that regulate the flow of vessels, trucks and goods at the port were knocked offline simultaneously on May 9, 2020, disrupting operations and causing road and waterway congestion that lasted several days.

Maritime Security Incidents: Disruptive Cyber-attack Cripples Port Facility

According to an official, the damage was more severe than initially described by Iranian officials. Photos shown to The Washington Post dated May 9, 2020 exposed miles-long traffic jams on highways leading to the Shahid Rajaee port terminal. A photograph dated May 12, 2020 also showed dozens of loaded container ships in a waiting area off the coast.

The attack on the port's computers was confirmed a day later by Mohammad Rastad, managing director of the Ports and Maritime Organization (PMO), who stated, "A recent cyberattack failed to penetrate the PMO's systems and was only able to infiltrate and damage a number of private operating systems at the ports."

Why Did This Happen?

There has been some ongoing tension between Israel and Iran in the form of an alleged back and forth of attempted and successful cyberattacks against physical infrastructures. On April 24, 2020, an attempted cyberattack on Israeli water facilities (which Iran has denied any involvement) caused some temporary disruptions in some local water systems. The attempted attack, which targeted programmable logic controllers (PLCs) that operate valves for water distribution networks, was routed through computer servers in Europe and the United States. While PLCs tend to be attractive targets for hackers due to their lack of security, the incident was quickly detected and thwarted before it could cause significant damage.

Water facility cyber-attack: While the April attack on Israel's water facilities was downplayed, Western intelligence sources believe that the hackers attempted to alter water chlorine levels before being detected and stopped. If the attack hadn't been stopped and water chlorine levels had been adjusted, attackers could have caused mild poisoning of the local population served by the affected treatment facility.

> ***Water facility cyber-attack:*** *While the April attack on Israel's water facilities was downplayed, Western intelligence sources believe that the hackers attempted to alter water chlorine levels before being detected and stopped. If the attack hadn't been stopped and water chlorine levels had been adjusted, attackers could have caused mild poisoning of the local population served by the affected treatment facility.*

There is speculation that the attack on Shahid Rajaee was retaliation by Israel and intended to send a warning to Iran without inflicting any significant physical harm or casualties. And while details are scarce on the actual execution of the cyberattack against the Shahid Rajaee port terminal, it is more than likely that the Terminal Operating System (TOS) that controls and manages the entire port was targeted through the various companies that have an interface to the TOS, given that only a number of private operating systems were damaged during the attack.

Maritime Security Incidents: Disruptive Cyber-attack Cripples Port Facility

What's the Aftermath?

There have been additional incidents that may be indicative of continued cyber warfare between the two nations:

Following the April 2020 attack, two more attacks hit Israel's water management facilities in June 2020. One hit agricultural water pumps in upper Galilee, and the other hit water pumps in the central province of Mateh Yehuda. In a Water Authority statement, the affected facilities were specific, small drainage installations that were immediately repaired without any harm done.

There have also been several accidents and explosions at various facilities in Iran. On July 2, 2020, a fire that broke out at Iran's Natanz Nuclear Facility is believed to be the result of a cyberattack, according to three Iranian officials. A spokesman for Iran's Atomic Energy Organization stated that while the incident caused significant damage and could slow down the development and production of advanced centrifuges in the medium term, there were no casualties.

UPDATE: On October 16, 2020, it was reported that Iran's Port Authority had been hit in a cyberattack, a day after Iranian officials vaguely confirmed that two governmental departments had been attacked. The attack targeted the Port Authority's infrastructure to disrupt the flow of goods in and out of the country but failed to affect the process.

UPDATE: On December 1, 2020, a group of Iranian hackers accessed an unprotected industrial control system at an Israeli water facility. The hackers were able to access a human-machine interface (HMI) system directly connected to the internet without any cyber protection for a reclaimed water reservoir. The owner made changes to prevent access to the HMI system without authentication after the hackers posted a video about their exploit.

While neither nation is officially claiming responsibility for any of these incidents, there might be additional incidents as both countries have stated they will respond accordingly if a cyberattack is used against them. We will keep updating this page as more unfolds.

Maritime Security Incidents: Disruptive Cyber-attack Cripples Port Facility

Economic Impacts: Ports & Shipping

Shipping and ports go hand-in-hand. Disruption to one creates a ripple effect for the other — this is a fact we've already seen first-hand with the current global pandemic and oil crash.

With the historically low oil prices, many companies and ports began to struggle with storage. Bloomberg writes, "From California to Gibraltar, tankers have piled up as suppliers deal with the largest glut the world has ever seen and ports have become congested." The lack of storage prolonged voyages with tankers having no place to go — and at port, they clogged up a well-worn system, causing knock-on consequences. While there are many factors at play, the interdependencies between ports and shipping are stark — as European oil tankers voyage around South Africa's Cape of Good Hope solely to prolong their journeys.

From another perspective, Lloyd's of London looked at the estimated damage of a coordinated cyber-attack against ports. In their worst-case scenario, a coordinated cyber-attack on 15 Asian ports would cost $110 billion. Additionally, 92% of the estimated costs from the cyber-attack are uninsured.

The report also projected the interrelated costs with countries linked to each port. Asian countries would lose $26 billion, followed by Europe at $623 million, and North America at $266 million. Related industries would also take a hit, with aerospace losing $28.2 billion, manufacturing at a $23.6 billion loss, and retail losing $18.5 billion. (The report and estimates are pre-COVID 19 figures.)

OT cybersecurity isn't just a must-have for ships and vessels. Onshore operations, ports, and terminals must also secure and protect their operations.

Keep Cyberattacks at Bay from Your Vessel OT Network

Geopolitical tensions are one of many maritime security challenges. It's critical to have strong security measures in place across your vessel OT networks and between your interactions with port terminals. With a global pandemic that continues to impact the global economy and expand the attack surface, port, ship and offshore staff must adapt their cybersecurity operations accordingly to ensure their endpoints, critical systems and components are updated and protected. Start your path to protection with our Comprehensive Guide to Maritime Cybersecurity.

Mission Secure

What are the Maritime Cybersecurity Compliance Measures You Need to Consider?

Many industries and organizations address environment, health, and safety (EHS/HSE) and cyber risk management separately, often managed by entirely different departments. Conversely, IMO Resolution MSC.428(98) essentially merges the two seemingly separate 'disciplines' under on framework - operational risk management - encouraging maritime organizations "to ensure that cyber risks are appropriately addressed in safety management systems." There are considerable similarities between safety and cyber risk management practices, and the two clearly impact each other in today's digitally connected world. So, what does this look like?

TOP

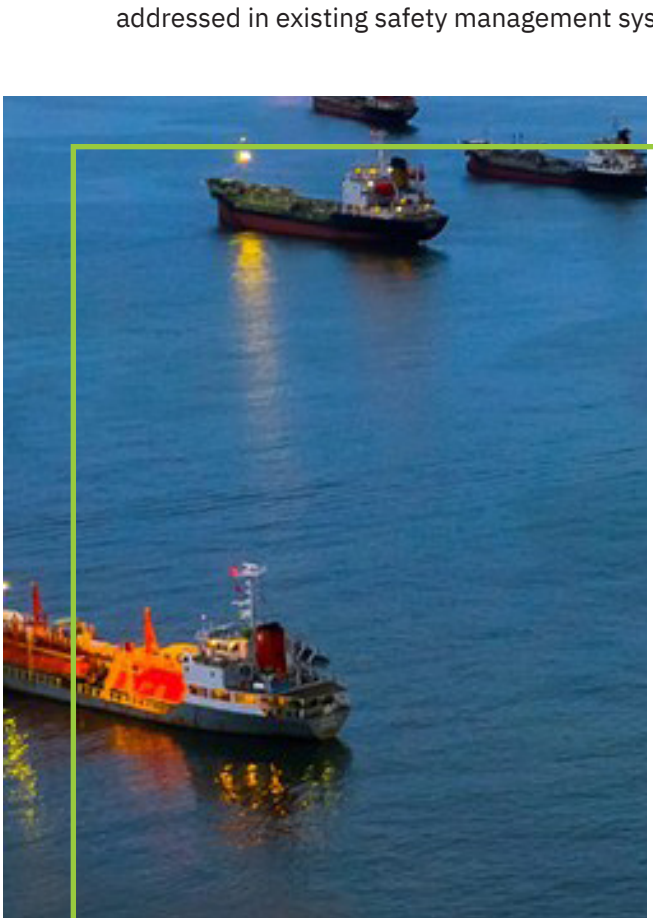
What are the Maritime Cybersecurity Compliance Measures You Need to Consider?

Some of the maritime cybersecurity compliance measures you need to consider include IMO Resolution MSC. 428(98), ISA/IEC 62443, ISO/IEC 27001, and TMSA. There are also other industry and regulatory standards that you need to adhere to based on your country of operation and nature of your vessels' operations.

As connectivity and reliance on the Internet are now the norms with many technologies essential to the operation and management of vessels, the security, safety, and reliability of these systems is paramount. To that end, the maritime industry is recognizing the need for cybersecurity oversight to ensure the effective management and mitigation of evolving cyber threats. Let's take a look at a few of the compliance measures in depth:

IMO Resolution MSC.428(98)

A significant cybersecurity compliance deadline facing the maritime industry is the International Maritime Organization's (IMO) Resolution MSC.428(98), which encourages administrations to ensure that cyber risks are appropriately addressed in existing safety management systems (as defined in the ISM Code) no later than the first annual verification



of the company's Document of Compliance after January 1, 2021. These are based on the NIST 800-53 R4 cybersecurity framework and tailored for the Maritime industry to provide a standardized approach for applying and evaluating security controls within an OT environment.

These guidelines provide recommendations and include functional elements that support effective cyber risk management:

Identify: Define personnel roles and responsibilities for cyber risk management and identify the systems, assets, data, and capabilities that, when disrupted, pose risks to ship operations.

Protect: Implement risk control processes and measures, and contingency planning to protect against a cyber-event and ensure continuity of shipping operations.

Detect: Develop and implement activities necessary to detect a cyber-event in a timely manner.

Respond: Develop and implement activities and plans to provide resilience and to restore systems necessary for shipping operations or services impaired due to a cyber event.

Recover: Identify measures to back-up and restore cyber systems necessary for shipping operations impacted by a cyber-event.

ISA/IEC 62443

The ISA/IEC 62443 series of standards have been developed jointly by the ISA99 committee and IEC Technical Committee 65 Working Group 10 customized to address the need to design cybersecurity robustness and resilience into industrial automation control systems (IACS). An IACS is defined as a collection of personnel, hardware, software, and policies involved in the operation of the industrial process, and that can affect or influence its safe, secure, and reliable operation. The ISA/IEC 62443 Series Standards and Technical Reports are arranged in four groups:

ISA/IEC 62443 Family of Standards

General

ISA-62443-1-1	**Terminology, concepts, and models**
ISA-62443-1-2	**Master glossary of terms and abbreviations**
ISA-62443-1-3	**System security conformance metrics**
ISA-62443-1-4	**IACS security lifecycle and use-cases**

Policies & Procedures

ISA-62443-2-1	**Establishing an IACS security program**
ISA-62443-2-2	**IACS security program ratings**
ISA-62443-2-3	**Patch management in the IACS environment**
ISA-62443-2-4	**Security program requirements for IACS service providers**
ISA-62443-2-5	**Implementation guide for IACS asset owners**

System

ISA-62443-3-1	**Security technologies for IACS**
ISA-62443-3-2	**Security risk assessment for system design**
ISA-62443-3-3	**System security requirements and security levels**

Components

ISA-62443-4-1	**Product security development lifecycle requirements**
ISA-62443-4-2	**Technical security requirements for IACS components**

General—This group includes documents that address topics that are common to the entire series:

- Part 1-1: Terminology, concepts, and models introduce the concepts and models used throughout the series.
- Part 1-2: Master glossary of terms and definitions is a list of terms and abbreviations used throughout the series.
- Part 1-3: System security conformance metrics describe a methodology to develop quantitative metrics derived from the process and technical requirements in the standards.
- Part 1-4: IACS security lifecycle and use cases provide a more detailed description of the underlying lifecycle for IACS security, as well as several use cases that illustrate various applications.

General

This group includes documents that address topics that are common to the entire series:

- Part 1-1: Terminology, concepts, and models introduce the concepts and models used throughout the series.
- Part 1-2: Master glossary of terms and definitions is a list of terms and abbreviations used throughout the series.
- Part 1-3: System security conformance metrics describe a methodology to develop quantitative metrics derived from the process and technical requirements in the standards.
- Part 1-4: IACS security lifecycle and use cases provide a more detailed description of the underlying lifecycle for IACS security, as well as several use cases that illustrate various applications.

Policies and Procedures

Documents in this group focus on the policies and procedures associated with IACS security:

- Part 2-1: Establishing an IACS security program describes what is required to define and implement an effective IACS cybersecurity management system.
- Part 2-2: IACS security program ratings provide a methodology for evaluating the level of protection provided by an operational IACS against the requirements in the ISA/IEC 62443 Series of standards.
- Part 2-3: Patch management in the IACS environment provides guidance on patch management for ACS.
- Part 2-4: Security program requirements for IACS service providers specify requirements for IACS service providers such as system integrators or maintenance providers.
- Part 2-5: Implementation guidance for IACS asset owners provides guidance on what is required to operate an effective IACS cybersecurity program.

System Requirements

The documents in the third group address requirements at the system level:

- Part 3-1: Security technologies for IACS describes the application of various security technologies to an IACS environment.
- Part 3-2: Security risk assessment for system design addresses cybersecurity risk assessment and system design for IACS.
- Part 3-3: System security requirements and security levels describe the requirements for an IACS system based on the security level.

Component Requirements

The fourth and final group includes documents that provide information about the more specific and detailed requirements associated with the development of IACS products:

- Part 4-1: Product security development life cycle requirements describe the requirements for a product developer's security development lifecycle.
- Part 4-2: Technical security requirement for IACS components describes the requirements for IACS Components based on the security level. Components include Embedded Devices, Host Devices, Network Devices, and Software Applications.

ISO/IEC 27001

ISO 27001 is a technology-neutral, vendor-neutral information security management standard that offers a prescription of the features of an effective information security management system (ISMS). The mandatory requirements for ISO 27001 are defined in its clauses 4 through 10 – to receive certification or to pass an audit, your ISMS must conform to these requirements.

CLAUSE 4:

Context of the Organization

defines requirements for understanding external and internal issues, interested parties and their requirements, and defining the ISMS scope.

CLAUSE 5:

Leadership
defines top management responsibilities, setting the roles and responsibilities, and contents of the top-level Information Security Policy.

CLAUSE 6:

Planning
defines requirements for risk assessment, risk treatment, Statement of Applicability, risk treatment plan, and setting the information security objectives.

CLAUSE 7:

Support
defines requirements for the availability of resources, competencies, awareness, communication, and control of documents and records.

CLAUSE 8:

Operation
defines the implementation of risk assessment and treatment, as well as controls and other processes needed to achieve information security objectives..

CLAUSE 9:

Performance Evaluations
defines requirements for monitoring, measurement, analysis, evaluation, internal audit, and management review.

CLAUSE 10:

Improvement
defines requirements for nonconformities, corrections, corrective actions, and continual improvement.

TMSA

In 2004, the Oil Companies International Marine Forum (OCIMF) introduced the Tanker Management and Self Assessment (TMSA) program to help vessel operators assess, measure, and improve their safety management systems. It complements industry quality codes and is intended to encourage self-regulation and promote continuous improvement among tanker operators.

The TMSA framework is based on 12 elements of management practice. Each element includes a clear objective and a set of supporting KPIs:

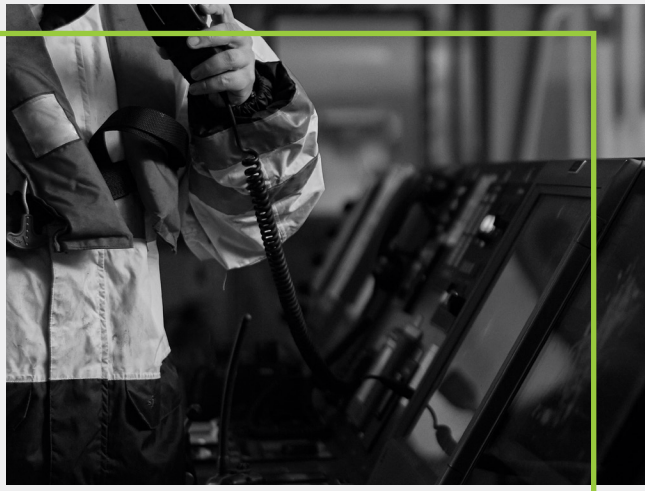
1. Management, leadership, and accountability
2. Recruitment and management of shore-based personnel
3. Recruitment and management of vessel personnel
4. Reliability and maintenance standards
5. Navigational safety
6. Cargo, ballast and mooring operations
7. Management of change

8. Incident investigation analysis
9. Safety management
10. Environmental management
11. Emergency preparedness and contingency planning
12. Measurement, analysis, and improvement

Guidelines on activities, grouped into four stages, are provided to help you meet these objectives. You should work through the 12 elements to produce as accurate and substantive an assessment as possible. You can use the assessment to conduct a gap analysis to identify which elements and stages have yet to be attained and how best to develop a performance improvement program.

> *Maritime organizations now need to follow the guidance and recommendations outlined by the IMO to ensure their vessel operations are protected from potentially catastrophic cyberattacks."*

IMO 2021: Three Steps to Ensure IMO/ ISM Cybersecurity Compliance



IMO Guidelines on Maritime Cyber Risk Management

New Year's Day 2021 will not just be the start of a new year – it will also be a date of significance for those in the maritime industry. The International Maritime Organization (IMO) will be enforcing Resolution MSC. 428(98) that "encourages administrations to ensure that cyber risks are appropriately addressed in existing safety management systems (as defined in the International Safety Management (ISM) Code) no later than the first annual verification of the company's Document of Compliance (DOC) after January 1, 2021."

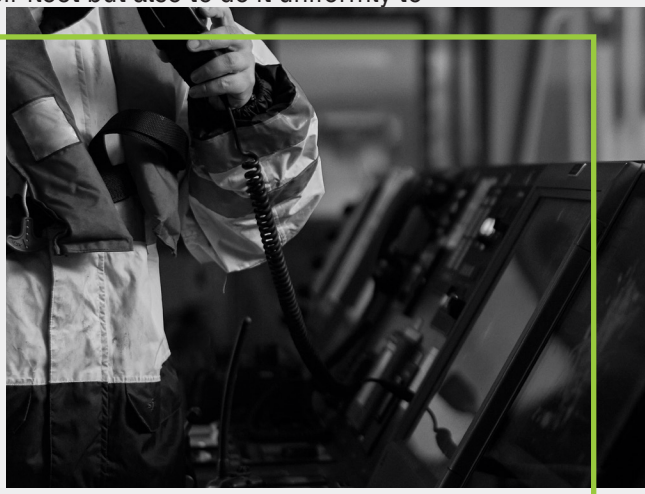
> ***Maritime organizations now need to follow the guidance and recommendations outlined by the IMO to ensure their vessel operations are protected from potentially catastrophic cyberattacks.***

Maritime cybersecurity is no longer on the back-burner. Vessel systems are more connected than ever, and despite a global pandemic, hackers have ramped up their efforts to compromise critical vessel OT systems. Maritime organizations now need to follow the guidance and recommendations outlined by the IMO to ensure their vessel operations are protected from potentially catastrophic cyberattacks.

In this post, we'll walk you through the three recommended steps to ensure IMO cybersecurity compliance to get you ahead of the upcoming January 2021 deadline.

Why is IMO Cybersecurity Compliance Important?

With sophisticated cyber threats now taking full aim at the maritime industry, there must be protections in place to safeguard the carriage of 90% of world trade. There is an immediate need for companies to not only develop and implement a safety management system (SMS) for vessels within their fleet but also to do it uniformly to reduce inconsistencies across the entire industry.



The IMO Resolution is designed to standardize and document processes that will reduce the number of cybersecurity incidents on vessels and addresses people, process and technology from a cybersecurity perspective within the safety management system. Within the IMO Resolution is MSC-FAL.1/Circ.3, which provides recommendatory guidelines on maritime cyber risk management. It includes information on additional guidance and standards that those in the maritime industry should take into consideration in addition to any other international and industry standards and best practices. Among the recommended standards is ISO/IEC 27001, a technology-neutral, vendor-neutral information security management standard that offers a prescription of the features of an effective information security management system (ISMS).

Another standard recommended is The Guidelines on Cyber Security Onboard Ships, which is supported by BIMCO, CLIA, the International Chamber of Shipping (ICS), INTERCARGO, INTERMANAGER, INTERTANKO, the International Union of Marine Insurance (IUMI), OCIMF and the World Shipping Council. This extensive document offers guidance to shipowners and operators on procedures and actions to maintain the security of cyber systems in their organization and onboard their vessels and also includes direction based on another IMO-recommended standard: National Institute of Standards and Technology (NIST) Cybersecurity Framework.

The NIST Cybersecurity Framework is a living document based on international standards and guided by academia and the public and private sectors. It applies to any type of risk management, defines the entire breadth of cybersecurity and includes the functional elements that support effective cyber risk management:

IMO 2021: Three Steps to Ensure IMO/ISM Cybersecurity Compliance

The NIST Cybersecurity Framework is a living document based on international standards and guided by academia and the public and private sectors. It applies to any type of risk management, defines the entire breadth of cybersecurity and includes the functional elements that support effective cyber risk management:

Identify: Define personnel roles and responsibilities for cyber risk management and identify the systems, assets, data and capabilities that, when disrupted, pose risks to ship operations.
Protect: Implement risk control processes and measures, and contingency planning to protect against a cyber-event and ensure continuity of shipping operations.
Detect: Develop and implement activities necessary to detect a cyber-event in a timely manner.
Respond: Develop and implement activities and plans to provide resilience and restore systems essential for shipping operations or services impaired due to a cyber event.
Recover: Identify measures to backup and restore cyber systems necessary for shipping operations impacted by a cyber-event.

As we walk through the three steps to ensure IMO Cybersecurity Compliance, keep in mind that they cover people, process and technology across the functional elements of the NIST Cybersecurity Framework:

Ensure IMO Cybersecurity Compliance with These Three Recommended Steps

These three recommended steps represent an overall approach that will help you address maritime cybersecurity and comply with the IMO Resolution and ISM Code. Before you can begin your approach to complying with IMO's compliance requirements, you need to evaluate the cyber risks in your vessel OT environment. And to have a clear understanding of your entire maritime environment, you need comprehensive visibility so that you can make real-time, continuous assessments of your environment.

1. Assess Maritime Cybersecurity Risks

Your vessel IT and OT network consists of many interconnected systems, and all of them can be vulnerable to cyberattacks, including: propulsion and machinery management and power control systems; communication systems; bridge systems; access control systems; cargo handling and management systems; public-facing networks; passenger servicing and management systems; and administrative and crew welfare systems. Information and data are exchanged within these systems and they must be evaluated for any cyber risks as any sudden failure due to a cyberattack can result in potentially catastrophic conditions.

It would be best if you also looked at your vessel's processes to ensure they are sound against cyber threats from benign, malicious, intentional, unintentional, current or emerging sources. You need to evaluate design, operation, integration or maintenance inadequacies that can potentially impact safety and cybersecurity and review any potential inappropriate or procedural lapses by the crew or any third parties that need to interact with vessel systems.

And last but not least, you need to include your people as part of your cybersecurity risk assessment. Cybersecurity awareness and the training of your crew is crucial to the cybersecurity of your vessels. You need to ensure that your people maintain a level of cyber discipline and hygiene so that there are no lapses in your cybersecurity risk management.

And speaking of cybersecurity risk management, once you have a proper assessment of any potential maritime cybersecurity risks across your people, processes and technologies, you need to incorporate your cybersecurity policy across all levels of your maritime organization, onboard and ashore, and develop a continuous process of reviews, inspections, internal cybersecurity audits and feedback mechanisms.

2. Design a Secure Maritime Cyber Architecture

Per the guidelines in the ISM Code and IMO Guide, maritime organizations are encouraged to design, establish or incorporate cyber risk management into their safety management system. Organizations in the maritime industry will have different needs and levels of maturity when it comes to the breadth of their vessel OT networks and cyber-related systems, so approaches to securing their maritime cyber architectures will vary.

There are a couple of ways that maritime organizations can design a secure maritime cyber architecture.

> One approach that is accepted by the IMO is to compare a current comprehensive cyber risk assessment to an organization's desired cyber risk management posture. Any identified gaps can be addressed to achieve risk management objectives and can enable you to apply your resources most effectively.
>
> Or you can develop your cybersecurity policy or cyber risk management approach encompassing the elements of the NIST Cybersecurity Framework that will help you ensure the cybersecurity practices in your vessel's operations and environment. Your policy should incorporate a comprehensive assessment of all identified cyber risks as they relate to your ships, personnel and environment, as well as continuous improvement of cyber risk management.

The IMO also suggests updates to your safety management system (SMS) to account for your maritime cyber risk management framework and the inclusion of cyber risk documentation that details critical assets that can adversely affect ship operations if compromised; roles and responsibilities for crucial cybersecurity personnel; how objectives will be met; procedures for corrective actions and recurrence prevention; incident response plans; creation and maintenance of backups; and procedures for cyber non-conformity, accidents or incident reporting.

3. Protect Vessels and Maritime Operations

Ultimately, the goal of the IMO Resolution is to protect vessels and maritime operations. The functional elements of the NIST Cybersecurity Framework need to be a consistent part of your maritime cybersecurity policy so that you can execute the following:

Identify:

- Critical cyber systems through asset discovery and inventory tracking
- Network traffic flows across IT and OT vessel networks

Protect:

- Critical devices through network segmentation, continuous monitoring and validation
- Network traffic against unauthorized or unknown traffic
- Network access through green-lighting, blocking or restricting rights
- Assets and systems with robust encryption mechanisms

Detect:

- Critical devices, assets or data through real-time monitoring
- Unauthorized or unknown network traffic and/or devices
- Abnormal events
- Data validation using analog and digital signals
- Potential cyberattacks with real-time notifications or alerts

Respond and Recover:

- Critical devices, assets or data through real-time monitoring
- Real-time notifications or alerts to key personnel
- Automated and/or operator-guided corrective actions

Navigate Your Way to IMO Cybersecurity Compliance

Now is the time to review your operations and management of your vessels to ensure their security, safety and reliability from the onslaught of emerging cyberattacks. With a thorough and effective cybersecurity risk management approach, you'll be able to ensure that you have the resources needed to protect your onshore and offshore operations. And with real-time visualization of your data and protection of critical assets and continuous monitoring across your vessels and maritime operations, you will be on your way to achieving IMO cybersecurity compliance.

Mission Secure

How Do You Start Designing Your On-Vessel Maritime Cybersecurity Action Plan?

Cyber risk assessments can help jumpstart your efforts to create a cybersecurity strategy and establish an initial baseline of cybersecurity requirements and internal standards for your vessel networks. But be prepared; these assessments can expose issues of which you may or may not be aware. We've conducted lots of onboard maritime vessel cyber risk assessments, both point-in-time walkthroughs with pen testing and others that are continuous in nature.

TOP

Your maritime cybersecurity action plan will take some time to pull together, you can do several things in the short-term to jumpstart your efforts and establish an initial baseline of cybersecurity for your vessels:

Your On-Vessel Maritime Cybersecurity Action Plan

- ✓ **Update the admin password on critical systems and devices on your OT network**
  Make sure you change the admin password on your critical systems and devices from the manufacturer default. Hackers can quickly identify and access internet-connected systems that use shared default passwords. It is imperative to change default manufacturer passwords and restrict network access to critical vessel systems.

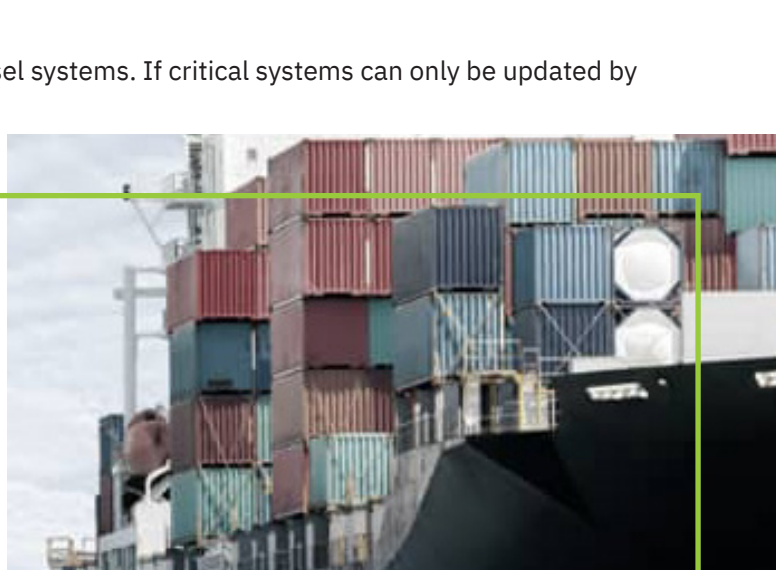
- ✓ **Update your passwords regularly and use multi-factor authentication, where possible**
  If you do not have one in place already, deploy a password management system for your critical computers and devices on your OT network. This includes adding multi factor authentication, where possible, and changing passwords (including any that are shared) on a regular basis.

- ✓ **Make sure your critical systems and devices are not accessible via the Internet**
  Most providers offer a private IP address space to keep hackers from reaching your systems over the Internet. You can determine if your vessel terminals are public by entering the IP address in a browser to see if you can route to the terminal web interface.

- ✓ **Update the software on critical systems and devices**
  Most updates include fixes for security flaws, so make sure your systems are running the latest software versions and ensure they are updated every time the manufacturer publishes an update.

- ✓ **Secure USB ports on all ship systems**
  Lock down USB access to prevent malware from entering vessel systems. If critical systems can only be updated by USB, keep dedicated USB keys in a secure location.

- ✓ **Lock up your IT and OT equipment on the ship**
  This seems like an obvious security control, but many times, for many reasons, cabinets and rooms are left wide open for an adversary to use as an access point both on board vessels and in operations centers. With the transient nature of crews on board maritime vessels, an adversary could simply pay a crew member to put a device on an open network or USB port, bypassing other security in place, and gain access to the most critical parts of the OT system. Keep the critical devices locked up and develop a key management strategy.



- **Check all onboard Wi-Fi networks**
  Just like you need to make sure you change default admin passwords on your satcom system and other devices, the same applies to your Wi-Fi routers. Also, you need to make sure you have strong encryption and passwords for all of your Wi-Fi networks. Make sure that your crew Wi-Fi network does not connect to anything other than the Internet and streaming services for personal use. Any of your vessel systems that use Wi-Fi for comms and navigation (e.g., tablets) must have strong security levels and strong user authentication (e.g., multi-factor authentication).

- **Segment your bridge, engine room, crew, Wi-Fi and business networks on board**
  If a device on your vessel is compromised, segmented networks will ensure critical systems are not susceptible to an attacker. Ensure that the crew's personal devices and laptops do not have access to navigation systems and other critical areas of the ship's network.

- **Eliminate unsecured wireless devices and services on your networks**
  Devices such as wireless printers, wireless keyboards, and mice offer easy targets for a moderately sophisticated cyber adversary

- **Educate your crew about cybersecurity**
  Establish a cybersecurity training program for your crew. You can also take advantage of complimentary resources like ESET's online cybersecurity awareness training and the Be Cyber Aware At Sea campaign to raise cybersecurity awareness and help train your crew to avoid opening the vessel to compromise. Security starts with your people.

Maritime Security: Getting Started with Your Action Plan

There is so much to consider when developing a maritime security plan. Your plan must include a significant cybersecurity component to ensure the safety of your vessels and offshore operations from the growing number of maritime cyber threats. As ships become more sophisticated in the digital era, at the same time, crews are shrinking and dedicated resources to cybersecurity may be scarce. But cybersecurity cannot be an afterthought – it needs to be elevated as a board-level priority issue.

We've touched on some of the security frameworks and compliance considerations that you can leverage in your planning efforts. Establishing your cybersecurity plan will not happen overnight. The burden and responsibility of cybersecurity fall on everyone – process and cultural changes will need to happen for an effective cybersecurity plan.

As you begin your in-depth cybersecurity planning efforts, the cyber risk management approach * from "The Guidelines on Cyber Security Onboard Ships," produced and supported by BIMCO, Cruise Lines International Association (CLIA), International Chamber of Shipping (ICS), International Association of Dry Cargo Shipowners (INTERCARGO), InterManager, INTERTANKO, International Union of Marine Insurance (IUMI), Oil Companies International Marine Forum (OCIMF), and World Shipping Council (WSC) guides shipowners and operators on procedures and actions to maintain the security of cyber systems in their organization and onboard their vessels.

Cyber Risk Management Approach

The Guidelines on Cyber Security Onboard Ships

1. Identify Threats

- Understand the external cybersecurity threats to the ship.
- Understand the internal cybersecurity threat posed by inappropriate use and lack of awareness.

2. Identify Vulnerabilities

- Develop inventories of onboard systems with direct and indirect communication links.
- Understand the consequences of a cybersecurity threat on these systems.
- Understand the capabilities and limitations of existing protection measures.

3. Assess Risk Exposure

- Determine the likelihood of vulnerabilities being exploited by external threats.
- Determine the likelihood of vulnerabilities being exposed by inappropriate use.
- Determine the security and safety impact of any individual or combination of vulnerabilities being exploited.

4. Develop protection & detection measures

- Reduce the likelihood of vulnerabilities being exploited through protection measures.
- Reduce the potential impact of a vulnerability being exploited.

5. Establish contingency plans

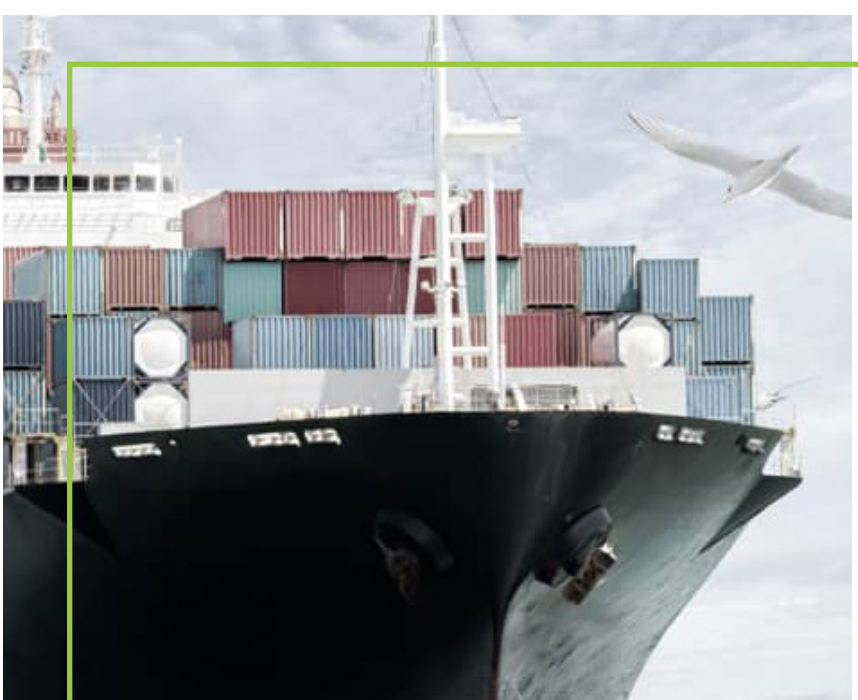
- Develop a prioritized contingency plan to mitigate any potential identified cyber risk.

6. Respond & Recover

- Respond to and recover from cybersecurity incidents using the contingency plan.
- Assess the impact of the effectiveness of the response plan and re-assess threats and vulnerabilities.

Identify Threats

The cyber risk is specific to the company, ship, operation, and/or trade. When assessing the risk, organizations should consider any specific aspects of their operations that might increase their vulnerability to cyber incidents.



There are motives for organizations and individuals to exploit cyber vulnerabilities. There is the possibility that company personnel, onboard and ashore, could compromise cyber systems and data. In general, the organization should realize that this may be unintentional and caused by human error when operating and managing IT and OT systems or failure to respect technical and procedural protection measures. There is, however, the possibility that actions may be malicious and are a deliberate attempt by a disgruntled employee to damage the company and the ship.

Identify Vulnerabilities

It is recommended that a shipping company performs an assessment of the potential threats that may be faced. This should be followed by an assessment of the systems and onboard procedures to map their robustness to handle the current level of threats. The result should be a strategy centered around the key risks.

Standalone systems will be less vulnerable to external cyberattacks compared to those attached to uncontrolled networks or directly to the Internet. Care should be taken to understand how critical onboard systems might be connected to uncontrolled networks.

Assess Risk Exposure

Cyber risk assessment should start at the senior management level of a company, instead of immediately delegated to the ship security officer or the head of the IT department:

- Initiatives to heighten cybersecurity and safety may also affect standard business procedures and operations, rendering them more time consuming and costly. This usually becomes a senior management level decision to evaluate and decide on risk mitigation.
- Some initiatives, which would improve cyber risk management, are related to business processes, training, the safety of the vessel, and the environment – not to IT systems, and should be anchored organizationally outside the IT department.
- Initiatives which heighten cyber awareness may change how the company interacts with customers, suppliers, and authorities, and impose new requirements on the co-operation between the parties. It is a senior management level decision whether and how to drive these changes in relationships.

Develop Protection and Detection Measures

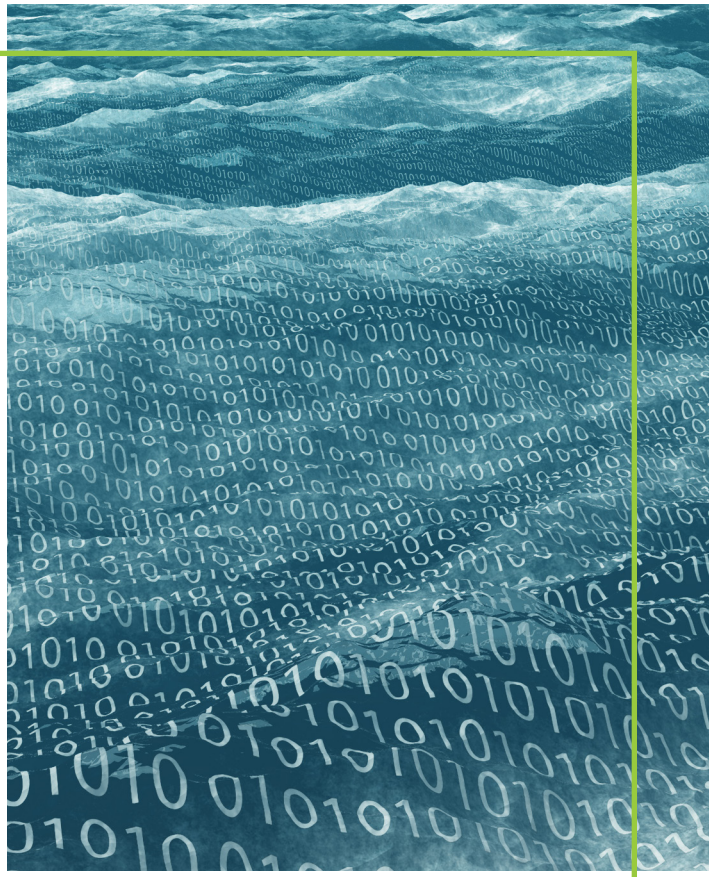
The outcome of the company's risk assessment and subsequent cybersecurity strategy should be a reduction in risk to be as low as reasonably practicable. At a technical level, this would include the necessary actions to be implemented to establish and maintain an agreed level of cybersecurity. It is crucial to identify how to manage cybersecurity onboard and delegate responsibilities to the master, responsible officers, and, when appropriate, the company security officer.

Establish Contingency/ Incident Response (IR) Plans

When developing contingency plans for implementation onboard ships, it is important to understand the significance of any cyber incident and prioritize response actions accordingly.

Any cyber incident should be assessed to estimate the impact on operations, assets, etc. In most cases, and with the exception of load planning and management systems, a loss of IT systems onboard, including a data breach of confidential information, will be a business continuity issue and should not have any impact on the safe operation of the vessel.

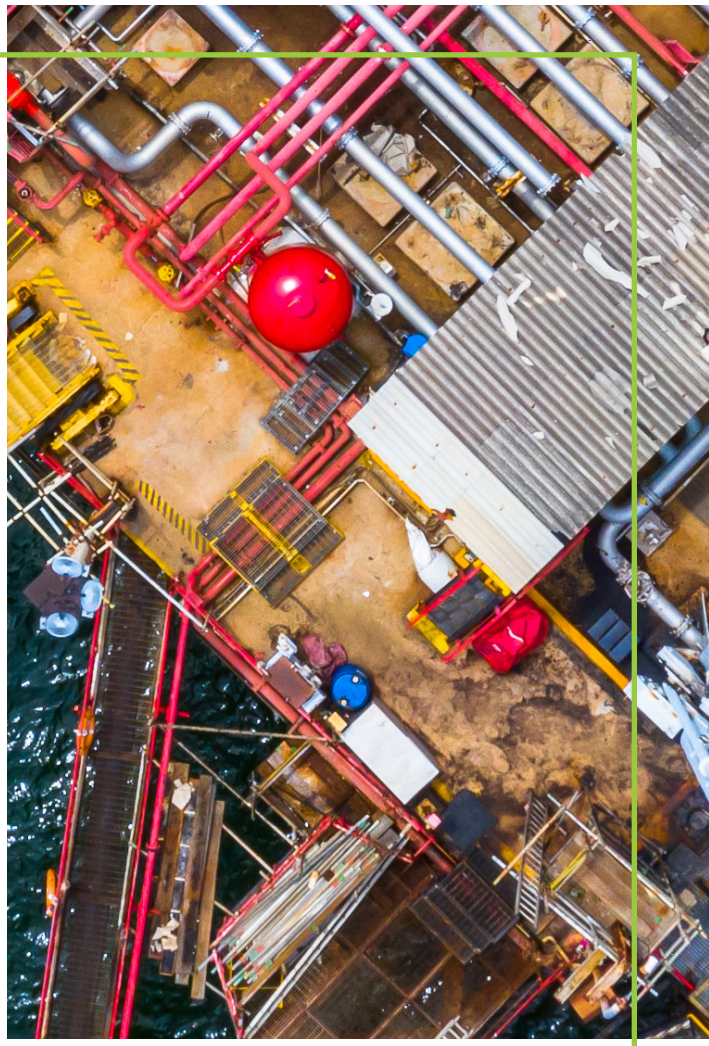
The loss of OT systems may have a significant and immediate impact on the safe operation of the vessel. Should a cyber incident result in the loss or malfunctioning of OT systems, it will be essential that effective actions are taken to help ensure the immediate safety of the crew, ship, cargo, and protection of the marine environment. Your crews should be trained regularly on the response plans. These plans should be regularly practiced by vessel crews, officers, and IT support management and staff – similar to the safety response exercises that are routinely done today. Third-party system providers on board the vessels should be included and required to be part of these IR exercises and planning.



Respond to and Recover from Cyber Security Incidents

It is important to understand that cyber incidents may not disappear by themselves. If, for example, the emergency chart display and information system (ECDIS) has been infected with malware, starting up the back-up ECDIS may cause another cyber incident. Therefore, it is recommended to plan how to carry out the cleaning and restoration of infected systems.

Disaster recovery (DR) plans need to be an integral part of any maritime cybersecurity plan. This includes the preservation of cyber data for forensic purposes in addition to the restoration and protection of your OT processes and ship controls. These plans should also be exercised regularly and updated as necessary both at sea and on shore. Any third-party system providers you partner with should be included and required to be part of the planning and execution of these DR exercises. Any knowledge you obtain about previously identified cyber incidents should be used to improve the response plans of all ships in your company's fleet, and you should consider an information strategy for such incidents.



We've touched on some of the security frameworks and compliance considerations that you can leverage in your planning efforts. Establishing your cybersecurity plan will not happen overnight. The burden and responsibility of cybersecurity fall on everyone – process and cultural changes will need to happen to ensure your success in developing an effective cybersecurity plan.

Your Vessel Exposed: 10 Potential Surprises to Expect from Your Maritime Cyber Risk Management Assessment

Cyber-related risk and threats to your vessel network are mounting, and so are the maritime industry cybersecurity compliance requirements. Between the upcoming International Maritime Organization's (IMO) Resolution MSC.428(98) and other programs like the Tanker Management and Self Assessment (TMSA), you'll need to get a handle on your vessel OT network before you can even commence.

Getting Started with Effective Maritime Cyber Risk Management

Cyber risk assessments can help jumpstart your efforts to create a cybersecurity strategy and establish an initial baseline of cybersecurity requirements and internal standards for your vessel networks. But be prepared; these assessments can expose issues of which you may or may not be aware. We've conducted lots of onboard maritime vessel cyber risk assessments, both point-in-time walkthroughs with pen testing and others that are continuous in nature.

In this blog, we'll discuss why a cyber risk assessment for your vessel network might be right for you, provide you examples of the types of surprises we typically find that might come out of your assessment, and give you guidance on how to avoid these surprises in the future.

Your Vessel Exposed: 10 Potential Surprises to Expect from Your Maritime Cyber Risk Management Assessment

Why is a Cyber Risk Assessment Important?

With the growing number of cyber threats to maritime vessel networks and industrial control systems in recent months, you have to assume that your organization is susceptible to attack. The dangers facing connected vessels are so significant that in July 2020, the United States National Security Agency (NSA) and Cybersecurity and Infrastructure Security Agency (CISA) issued an alert recommending that immediate actions be taken to reduce exposure across operational technologies and control systems.

The dangers facing connected vessels are so significant that in July 2020, the United States National Security Agency (NSA) and Cybersecurity and Infrastructure Security Agency (CISA) issued an alert recommending that immediate actions be taken to reduce exposure across operational technologies and control systems.

The NSA/CISA alert recommends creating an accurate OT network map to detail "as-operated" assets so that you can understand the cyber risk of those assets and protect your network by removing any unwanted assets and eliminating unnecessary or unauthorized connectivity. The alert also recommends establishing an OT resilience plan, an incident response plan, and implementing a continuous and vigilant system monitoring program.

But before you can even start to work on those recommendations, you need the information on what is in your vessel OT network. Performing a cybersecurity risk assessment will help you gather the information you need to properly evaluate your vessel's network cybersecurity framework and security controls, and help you develop your overall cybersecurity risk strategy.

Need help getting your maritime cyber risk assessment started?

Mission Secure can provide an onsite cybersecurity assessment and design service, along with remote red teaming / penetration testing, onsite red teaming, and industrial standards benchmarking (IMO 2021) and scoring. Click here to get started.

10 Potential Surprises to Expect from Your Cyber Risk Assessment

Every vessel OT network is different, and the findings from cyber risk assessments will vary. Here are 10 of those potential findings that might pop up:

1. Outdated or Unused Equipment Connected to Your Vessel OT Networks
Industrial Cyber Security: Managed Services

Any outdated or unused equipment connected to your vessel OT network can be an attractive entry point for hackers, especially if they haven't been updated with the latest security updates. Hackers who make it into your network through these unnecessary systems can take advantage to target your critical equipment and communication systems.

Validate network equipment to ensure all devices are in use and required for your vessel operations. Any outdated or unused equipment should have any previous configuration information removed, disconnected from the network, and physically removed from the vessel if possible.

2. Poor or Non-Existent IT/OT Network Segmentation

> ***The dangers facing connected vessels are so significant that in July 2020, the United States National Security Agency (NSA) and Cybersecurity and Infrastructure Security Agency (CISA) issued an alert recommending that immediate actions be taken to reduce exposure across operational technologies and control systems.***

Gone are the days when you could completely air gap your vessel systems. With networks more connected than ever and more digitalized maritime operations, the ability to protect your vessel network can pose some unique challenges. But with proper network segmentation between your IT and OT networks and within your OT network, you can significantly reduce a hacker's access to the rest of your critical vessel controls should they gain access.

You need to make sure your network is segmented and that your crew's personal laptops and devices do not have access to your critical network systems. If a device on your vessel is compromised, a segmented network will reduce the chances of any malware or other malicious traffic traveling laterally to other critical systems.

3. Unauthorized Network Access

The issue of unauthorized network access isn't limited to just users. Systems on your vessel network can attempt to connect to other devices, and if they're not authorized to do so, they can potentially access malicious servers and systems. The impact of unauthorized access has widespread implications and can lead to data loss and potential compromise of critical communication and navigation systems.

Your network needs to have the appropriate network access controls and protections in place so that only authorized crew members, devices, and third parties have access. You should conduct continuous network monitoring of your vessel systems to determine if unauthorized devices are detected. Any managed switches should be configured with MAC address filtering to keep rogue devices from gaining network access.

4. Insecure Third-Party Connections

Your vessel networks will more than likely have third-party vendors connecting to them to service systems and provide services. The maintenance that your third-party vendors provide can pose issues if you are not able to control their access and track all of the changes and updates being made. Without proper access controls, detailed standards, and control of these connections, you could be subjecting your vessel network to potential compromise.

You need to be able to control access to your vessel network from outside traffic. You can protect your vessel network with a protective layer between your third-party vendor connections using a firewall or whitelisting. Your third-party vendors also need to provide you documentation showing that the systems they provide for you are secure with the latest updates.

5. Vulnerable Peripherals and Wireless Access Points

They seem to be dismissed as unlikely entry points for hackers, but devices such as printers, wireless keyboards, and mice can be easy targets for a moderately sophisticated hacker. Access via peripherals can also be used to penetrate your wireless access points. And if your wireless access points aren't configured correctly or do not have the right level of encryption, hackers will be able to penetrate your vessel network easily and affect critical systems.

You should confirm that if your printer's wireless capabilities are needed on board. If wireless is required, you should use strong passwords, and limits should be imposed on the number of concurrent connections and incorrect password attempts before lockout. For any of your other peripherals and access points, make sure they are running the latest software versions and that passwords are being updated regularly.

6. Outdated Operating Systems

High costs and a lack of resources are some of the reasons why organizations drag their feet when it comes to upgrading their operating systems. Failing to update your operating systems can lead to significant problems if malware penetrates your vessel network. Many malware families tend to exploit known vulnerabilities found in outdated operating systems and software (e.g., NotPetya leveraged EternalBlue, which uses a vulnerability in a Windows protocol). Vessel systems using older versions of operating systems (e.g., Microsoft Windows 7) that are no longer supported are more susceptible to compromise.

Your operating systems should be updated to supported versions and make sure that you establish a patch management process to stay on top of any potential vulnerabilities. If these systems cannot be upgraded promptly, you should apply any emergency patches that might be available from the vendor and segment the systems from the vessel OT network as a compensating control to isolate potential vulnerabilities.

7. Unpatched Systems and/or Programs

You may have supported versions of operating systems and applications, but if you do not apply any patches on a regular basis, your vessel network will be susceptible to attack. Continuous vulnerability management is one of the Center for Internet Security (CIS) Controls that outlines the need to continuously acquire, assess, and take action on new information to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers. Maritime organizations need an effective patch management strategy and process to protect all of their systems and programs against known vulnerabilities.

Your patch management strategy and process should include all system hardware and applications so that you do not have to be burdened with ad hoc quick fixes. You will need to consider the schedule of your maintenance cycles and address any potential impact on vessel operations. If you are unable to deploy critical patches, you will need to explore alternative compensating controls that will let you implement a “virtual patch” to protect and segment the vulnerable systems and applications until you can patch appropriately.

8. Lack of Encryption and Two-Factor Authentication

As the number of wireless access points on your vessel grows, it’s easy to lose track of how they are connected and what is connecting to them. There are times when they are set up incorrectly, potentially transmitting network and email traffic unencrypted and leaving them vulnerable to interception and unauthorized monitoring.

Access to your wireless access points should be limited to authorized devices and secured with strong encryption. If possible, switch to certificate-based authentication and isolate your guest or crew networks from critical vessel networks. Enable two-factor authentication for critical applications (e.g., Microsoft Remote Desktop), protect your data with disk encryption, and make sure encryption is enabled across your communication systems.

9. Poor Password Practices

Organizations, just like individuals, struggle with a high number of passwords and keeping them straight. According to a February 2020 Ponemon Institute research report, 54% of individuals reuse passwords across their personal accounts and 51% share passwords with colleagues to access business accounts. The lack of password management in the maritime industry is exasperated by the fact that many vessel systems are utilized by multiple crew members who share passwords.

You can alleviate your password issues by deploying a password management system for your critical computers and devices on your OT network. You can require changing default passwords to strong ones, limit the number of incorrect password attempts before lockout, add multi-factor authentication, where possible, and change passwords (including any that are shared) on a regular basis.

10. Lack of Content Filtering

The Internet is inherently not a safe place. Without a solution that filters malware-infected web sites or blocks malicious traffic, your vessel network might be vulnerable to malware and phishing scams that can lead to network compromise and loss of critical data, as well as injury or loss of life, asset damage, or environmental impact.

A content filtering solution can help keep your crew from accessing sites that host inappropriate content and help prevent them from accessing insecure web sites that may contain malware and those that hinder productivity (e.g., Facebook, etc.) and consume considerable network bandwidth. You can blacklist banned web sites and malicious Internet traffic or whitelist allowed traffic and block everything else by default.

Avoid Surprises from Your Cyber Risk Assessment

Mission Secure can help you navigate your vessel OT network with a comprehensive cyber risk assessment. We can use your live OT network traffic to detect and analyze issues and threat vectors, evaluate your “as-is” architecture to identify security gaps, develop a unified IT/OT network drawing for your vessels and provide a cyber risk scorecard for each asset. Every cyber risk assessment will be unique, but once you know what cybersecurity issues you need to address on your vessel network, you’ll be better prepared to mitigate any outstanding items that can lead to a cyberattack.

Mission Secure

Maritime Cybersecurity Resources

Need help getting started on your cybersecurity action plan or just want to learn more about maritime security? Here are some resources dedicated to maritime cybersecurity that can get you on the right track:

- **NIST Cybersecurity Framework:** This framework helps organizations focus on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of their risk management processes.

- **NIST Guide to Industrial Control Systems (ICS) Security:** This document provides an overview of ICS and typical system topologies, identifies typical threats and vulnerabilities to these systems, and provides recommended security countermeasures to mitigate the associated risks.

- **International Maritime Organization (IMO) Guidelines on Maritime Cyber Risk Management:** These guidelines provide high-level recommendations on maritime cyber risk management to safeguard shipping from current and emerging cyber threats and vulnerabilities.

- **ISA/IEC 62443:** The 62443 series of standards was developed jointly by the ISA99 committee and IEC Technical Committee 65 Working Group 10 to address the need to design cybersecurity robustness and resilience into industrial automation control systems

- **ISO/IEC 27001:** ISO/IEC 27001 provides requirements for an information security management system.

- **Tanker Management and Self Assessment (TMSA):** The TMSA program provides companies with the means to improve and measure their own safety management systems.

- **The Guidelines on Cyber Security Onboard Ships:** This document offers guidance to shipowners and operators on procedures and actions to maintain the security of cyber systems in their organization and onboard their vessels.

Mission Secure

Mission Secure

Stop OT Cyber Threats Head-On

Mission Secure is setting a new standard in OT cyber-protection stopping OT cyber threats head-on. The Mission Secure Platform backed by 24/7 Managed Services is the first to seamlessly integrate OT visibility, segmentation, protection, threat hunting, and incident response, delivering military strength, industrial grade OT protection. With Mission Secure, defense, critical infrastructure, and process industry customers keep critical operations up and running and safe from harm.