CENSUS
IT Security Works

CYBERSECURITY IN MARITIME SECTOR

CENSUS can assist both **shipping crew** and **vendors** through its cutting-edge **information technology** (**IT**) and **operational technology** (**OT**) cybersecurity services. CENSUS can improve the security of **IT systems externally** or **internally**, and consequently the safety of the crews and the ships through **social engineering** and **physical security**, as well as through the examination of external and internal **network infrastructure**. Furthermore, CENSUS can assess the **Security of OT Systems** in **new** and **old vessels**, and **test the environment**.

CENSUS offers a set of services to maintain the organization's **cyber resilience by reducing the risk exposure**, as well as by meeting **the highest security standards** on each vessel's internal and external network.

THE CHALLENGES

Maritime, one of the oldest and most competitive industries, requires the integration of new technologies, while increasing **efficiency** and **sustainability**. It also requires the **collaboration of the sector**. Adopting advanced technologies may bring benefits, but also carries risks. Ships are increasingly using systems that rely on digitization, digitalization, integration, and automation. As technology continues to develop, on-board **IT** and **OT** are being networked together – and often connected to the Internet.

Cybersecurity plays a pivotal role in Maritime as the global economy is dependent upon the movement of cargo, such as food, transportation oil and gas as well as passengers. Attacks in Maritime might have disastrous consequences. Moreover, delays in transportation may lead to **financial losses**, **supply chain disruption**, and damage an **organization's reputation**. For example, impersonating maritime authorities or tampering with the messages received could prevent a vessel from reaching a port or force a delay. Furthermore, some attacks could affect more crucial factors, such as the **environment** and **employee safety**. A deliberate accident may lead to the physical malfunction of the vessel, and even lead to the loss of human life.

THE THREATS

A **cyberattack** may occur when the ship's data and systems are part of a **general target** or when the ship is the **intended target**. Generic attacks use techniques that identify and exploit vulnerabilities that may also exist in vessels, compromise a system, and allow attackers to gain access to sensitive data. Any kind of disruptive influence can cause disorder within the systems, leading to significant or even irreparable damage to the vessel.

A vessel's functionality depends on different third-party components, making it vulnerable to **supply chain attacks**. If the system of an IT provider is compromised, then it is possible for the vessel to be hit by cyberattacks under a general target group.

Maritime industry faces numerous threats with different motives:

1. **Nation-States**
   Maritime's critical infrastructure contains sensitive data crucial to economies. Thus, some maritime organizations have been the targets of state-sponsored attacks.
2. **Terrorists**
   Over the years, Maritime has strengthened its physical security against terrorists, but it remains vulnerable to cyber-terrorism which tries to take advantage of critical infrastructure. In addition, pirates also remain a significant threat; they could use cyberattacks as a precursor to a physical attack.
3. **Hacktivists**
   Hacktivists align cyberattacks with activist campaigns promoting a cause of social progress or change. The aim is to cause disruption and damage an organization's reputation, usually through a data breach.
4. **Insider Threats**
   Employees, contractors, partners, and vendors could also be listed as potential cyber threats. Cyberattacks from insider threats may be caused by deliberate or unintentional actions, such as revealing sensitive information or unintentionally changing IT configurations.
5. **Cybercriminals**
   Their motives are financial, and they achieve their goals through manipulating cargo management, logistics systems and sensitive cargo information.

As ships become smarter and more connected due to the increased usage of smart technologies, the threat landscape expands, combining the tools and techniques used in cyber attacks that continue to evolve. Therefore, the maritime industry should **constantly evaluate** its **risk posture**.

MARITIME CYBERSECURITY DIFFERS FROM OTHER INDUSTRY SECTORS

In recent years, Maritime has been incorporating more and more smart technologies. However, the sector's cybersecurity technology penetration is not at the same maturity level as other sectors, such as banking.

A significant lack of regulations related to IT infrastructure in Maritime contributes to the sector's low cybersecurity maturity level. The most important regulation was released as recently as 2017 *[IMO Resolution MSC. 428(98)]*, recognizing the urgent need to raise awareness of cyber threats and vulnerabilities to support safe and secure shipping, which is operationally resilient to cyber risks. Despite the fact that there are other regulations for industrial automation control systems (IACS) e.g., *ISA/IEC 62443*, or more general ISMS systems e.g. *ISO/IEC 27001*, these are not specific to the industry's characteristics.

Furthermore, **the lack of cybersecurity specialists** and **untrained crew** on board makes vessels vulnerable to unintentional actions, such as the disclosure of sensitive information through phishing, installation of malicious programs, or reconfiguring IT/OT protocols and processes.

EACH VESSEL NEEDS TO BUILD A DIFFERENT "STRONGHOLD"

Each vessel needs to build a **different stronghold**, as there are a wide variety of vessels with different requirements. There is **different equipment**, **network segmentations** and **needs in each vessel**. Consequently, common industry best practices cannot be directly applied. For example, it is not possible to remotely update an old critical device, considering that transferring data to a vessel in, for example, the Pacific, is a problem on its own.

Moreover, each vessel may need to conduct **its own arrangements** with untrusted third parties, such as

ports, authorities, and supply managers. The attack surface increases due to a lack of control on third parties, making the vessels easy targets for adversaries. Furthermore, cybersecurity in Maritime becomes more complicated as many vessels are **connected directly** to the organization's **internal infrastructure**, using different technology that requires different assessments.

CENSUS can cover every different demand of a vessel's operation, facilitating the **cybersecurity maturity journey**.

VESSEL'S OT ENVIRONMENTS NEED A PRE-EMPTIVE CYBERSECURITY APPROACH

Since new technologies are constantly emerging in the maritime sector, cybersecurity has never been more critical. The **Operational Technology** (OT) systems that physically control the ship are integrated with **Information Technology** (IT) systems and **Internet of Things** (IoT). As vessels update their systems to more electronically advanced components, it is necessary to increase their **cybersecurity vigilance**. IT and IoT systems can be compromised and controlled by adversaries, tampering with the OT technology.

Adversaries may also choose to directly target the OT technology of the ship. Spoofing attacks against the vessel's adjacent communication services (e.g., radio frequencies, AIS system) are not uncommon. In cases of AIS spoofing attack, crafted messages could fake the location of an existing vessel, or even create a nonexistent vessel in a virtual location. The main targets are communication systems and machinery, and propulsion controls. The adversaries can cause delays by affecting the satellite or the radio communication system or directly affecting the capabilities of a targeted vessel to sail or load cargo.

OT hardware and software are critical as they control physical devices in a **real-time environment**. For OT systems, **common approaches** like rebooting a device **are not applicable** due to operational requirements. Furthermore, the opportunities to 'patch' embedded operational technologies safely are not frequent, thus recovering from backups and software changes might not always be impossible.

The **new digital solutions** are created and integrated into new and older vessels, creating **new attack paths**.

SERVICES PROVIDED BY CENSUS

To secure the organization's infrastructure, CENSUS provides a variety of services including **Penetration Testing, Threat Modelling & Security Risk Assessment, Red Teaming, Tiger Team, Security Training & Consulting, Vulnerability Research,** and **Social Engineering Attacks**.

Penetration Testing

Penetration testing is the process of testing an IT infrastructure for security vulnerabilities in a controlled manner on each vessel's external & internal network. The testing is conducted against specific organization assets or infrastructure components. The process varies according to the degree of knowledge provided by the client (Black-Box, White-Box, Grey-Box testing, etc.); a mixture of these degrees of knowledge can also be applied to evaluate the effects of both insider and outsider attacks. Penetration testing evaluates the organization's controls deployed as part of an in-depth security model, aiming to uncover previously unknown attack paths that could be used to affect the confidentiality, integrity, and availability of the targeted assets. Penetration Testing can be performed both remotely and on a sample of vessels.

Furthermore, CENSUS performs OT Penetration Testing providing passive assessments that can be carried out anytime, as well as active assessments during maintenance periods.

Threat Modelling

CENSUS focuses on identifying threats and threat actors. Threats are actions that can affect the system, while threat actors include individuals or groups intending to use those threats to inflict harm or bring financial gain. Differentiating these elements allows prioritization of risks when it comes to remediation. Moreover, CENSUS can assist in identifying those system parts that require the highest attention or those components where a cybersecurity investment would yield the most favorable results.

Red Teaming

CENSUS consultants adopt an adversary mindset and simulate different threat agents of the organiza-

tion. The team identifies vulnerabilities in the utilised technology, the corporate processes, and the human element, exploits gaps in the organization's security model and attacks the in-scope assets. All aspects of an organization's attack surface (deployed software solutions, specialized hardware as part of the organization's products, external network perimeter, internal network segmentation, cloud infrastructure, on-premises physical controls, corporate employees) may be targeted according to the project scope.

Tiger Team

Tiger Team testing is the ultimate way to execute an asymmetric attack against an organization, a black box-only engagement that does not have a specific project plan or scope. The Tiger Team targets the core business, testing all layers of the organization's security architecture, making every effort to remain undetected and sharing information about the attack only with upper management.

Security Training & Consulting

CENSUS provides security training and consulting to improve the organization's security awareness, helping the personnel and allowing the management to identify and mitigate security issues in an effective manner.

Social Engineering Attacks

Social Engineering evaluates the cybersecurity awareness of the vessels' staff and the effectiveness of security tools in corporate network perimeters and security processes. Social Engineering attacks are performed through remote channels and local means. This module extends the infrastructure testing to the human factor, exploiting the personnel's knowledge, privileges, and habits.

CENSUS also offers:

- **Pre-emptive Security** for Design & Architecture reviews on new digital solutions,
- **IoT & OT Device Testing** providing specialised **cybersecurity assessments** on individual devices, and
- **Specialized IT Security solutions** to uncover unknown vulnerabilities in a vessel's infrastructure, using CENSUS **in-house Vulnerability Research**.

KEY TAKEAWAYS

Information Security is based on: (i) **the people**, (ii) **the technology**, and (iii) **the procedures**. Since security is everyone's responsibility, it is important to involve all parties, provide education and awareness programs, and regularly evaluate the company's security **awareness level**.

Additionally, cyber risk management through **enumeration** and **depiction** of the current IT and IoT network architecture, OT systems, equipment, and applications is of increasingly significant importance. It is necessary to know the company's **digital transformation strategy** in order to prioritize your upcoming security projects, bearing in mind the legal and regulatory framework requirements that offer protection against a cyber incident, and ensure **continuity of shipping operations**. Furthermore, it is crucial to **identify the responsibilities of users**, personnel, and ashore/on-board management, and develop and **implement detection mechanisms** against potential threats.

Moreover, the company's procedures should include **risk assessment**, **implementation of security policies**, and periodic **security testing on every component**. The importance of using simple language to raise IT information awareness should never be overlooked. It is necessary to understand the organization's risk posture; in this way the cybersecurity strategy will be more well-structured and better explained to the crew in non-technical terms so they may fully grasp what is at stake.

Finally, every company should employ **security experts** to address the maritime security **threat landscape** in an efficient and structured manner. **CENSUS** provides detailed deliverables that empower clients to make informed **strategic decisions** towards new technologies and to choose the **most secure solution** that meets their requirements.

CENSUS
IT Security Works

www.census-labs.com

USA
607 Boylston Street,
Suite 165L, Boston, MA 02116
T. +1 617-448-5050
E. usa@census-labs.com

EUROPE
128, Leoforos Andrea Syggrou,
11745, Athens, Greece
T. +30 210 220 8989-90
E. eu@census-labs.com

UK
4th floor, The Pinnacle,
Station Way, Crawley RH10 1JH
T. +44 (0) 1293 763 336
E. uk@census-labs.com