How the maritime industry can sail towards stronger cybersecurity

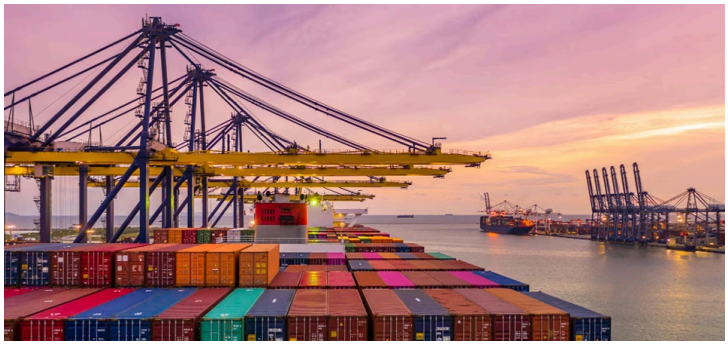
BY ANNA HAMMOND · DECEMBER 3, 2021 · LAST UPDATED ON APRIL 3, 2025

The maritime industry is a driving force in the world's economy. The sector carries over 90% of global merchandise trade, totalling around 11 billion tons of cargo per year, according to the World Bank and the International Association of Ports and Harbors (IAPH). Political events, such as Brexit, and the COVID-19 pandemic demonstrated how shipping and its associated logistical chains play a pivotal role in delivering essential supplies to organisations and homes — but it also laid bare the industry's vulnerability to disruption.

Never has it been more important for maritime transport to increase its robustness and reliability. To ensure continuity, resilience is the industry's top priority, which has led digital transformation to become an increasingly important topic. However, with this comes new cyber threats, meaning cybersecurity must be considered with every steer.

PortXchange is an organisation that provides innovative digital solutions to support shipping and port communities worldwide to become more efficient and sustainable. This year, the organisation is taking a strong focus on further improving its cybersecurity through security testing. In this article, the Information Security Officer of PortXchange, Vlad Gust, explains why the maritime industry must get on board with consistent and continuous cybersecurity testing.

Intigriti: Hi Vlad! Tell us, what cybersecurity challenges are the maritime industry facing today?



Maritime cybersecurity has never been more important than now.

Vlad: Thanks for having me! According to BlueVoyant, shipping and logistics firms experienced three times as many ransomware attacks in 2020 than in 2019. In fact, a spike in malware, ransomware, and phishing emails caused a 400% increase in cyberattack attempts during the first few months of the year.

In 2020, ransomware was a particular pain point for the maritime industry. The Mediterranean Shipping Company (MSC) suffered a network outage due to a malware attack, however, they weren't alone. All four of the world's largest shipping organisations were hit by an attack. The International Maritime Organisation (IMO) was forced offline from a cyberattack. The CMA CGM SA was also hit by a ransomware attack in September 2020.

Even before these incidents took place, the shipping community was already growing more alert to cyber risks. However, there are still challenges. Some of these include:

1. The threat to vessels is growing, and more ships are linked to onshore systems for navigation and performance management.
2. Smart ships are coming, which in turn, increases attack surfaces.
3. Incidents are not being reported due to fears of reputational risk.
4. Geopolitical conflict is increasingly played out in cyberspace, as illustrated by spoofing attacks on ships. For example, there has been a growing number of GPS spoofing incidents. This can cause vessels to believe themselves to be in a different position than they are.

Intigriti: Why is it important for maritime businesses to test their cybersecurity?

Vlad: An increase in automation, innovative technologies and digitalisation in maritime operations has also increased cybersecurity incidents. Maritime organisations must make the necessary moves to protect their business, vessels, and personnel from cybercriminals.

Positively, regulations and laws are being introduced that require owners, operators, and managers to consider cyber risks. For example, in January 2021, the IMO's Resolution MSC.428(98) came into effect. This requires cyber risks in maritime organisations to be addressed in safety management systems. The EU's Network and Information Systems Directive also extends to ports and shipping.

Intigriti: Can you elaborate on the importance of continuous testing at PortXchange and within the industry?

Vlad: Continuous testing allows us to periodically assess how strong our security defence systems are against cybercriminals who poke around our product line. It also aims to identify the security vulnerabilities and flaws that could leave our product open to vulnerabilities should a malicious actor find them.

From the maritime industry perspective, we see an increase of cybersecurity systems within ships and mobile units that can be classified as IT (standard information systems) and OT (operation and control systems.)

IT (standard information systems) generally has greater security maturity, with defined processes and procedures, technology and training available. While a breach of IT systems can have a significant reputational and financial impact, it doesn't impact the safe operation of ships and units ordinarily. In

contrast to IT, OT is typically less mature when it comes to cybersecurity. An attack on an onboard OT system could put the vessel and crew safety in danger.

For maritime businesses, tests can include (but aren't limited to):

- Auditing onboard and offboard systems for known vulnerabilities in software or hardware.
- Auditing and measuring the suitability of current security systems.
- Pinning down all possible vectors of access to systems.
- Identifying what data or systems are vulnerable to access.

There are several methods of testing security, including penetration testing and bug bounty programs.

Intigriti: How does a bug bounty program benefit PortXchange's security model?

Vlad: Bug bounty programs and penetration tests both aim to enable you to see your vessel the way a hacker sees it. However, there are some key differences.

The typical engagement time of a penetration test is 1 to 3 weeks, meaning you're seeing more of a glimpse in time of your security posture rather than the whole picture. Whilst you'll receive proof of attestation and an overview of identified vulnerabilities, your security posture will change as soon as you release new updates or make a change to your systems. This is where bug bounty programs work well as a follow-up.

A bug bounty program allows thousands (or a select group) of independent security researchers to test your systems and assets, and report bugs to your business in a legally compliant manner. Maritime organisations can leverage the skills, experiences, expertise, and creativity of thousands of security experts, without the additional headcount. If your team accepts the submission, the researcher is paid a reward or compensation which is better known as a 'bounty'. This acts as a great incentive for researchers to participate in the program.

To summarise, at PortXchange we aim to have a robust product security model that benefits from both worlds. By applying security testing continuously through Intigriti's platform, we give ourselves the best chance of staying one step ahead of cybercriminals.

About Vlad Gust

Vlad Gust

Vladislav is the Information Security Officer for PortXchange. He is responsible for delivering a robust security program to achieve product security goals and organisational information security milestones.