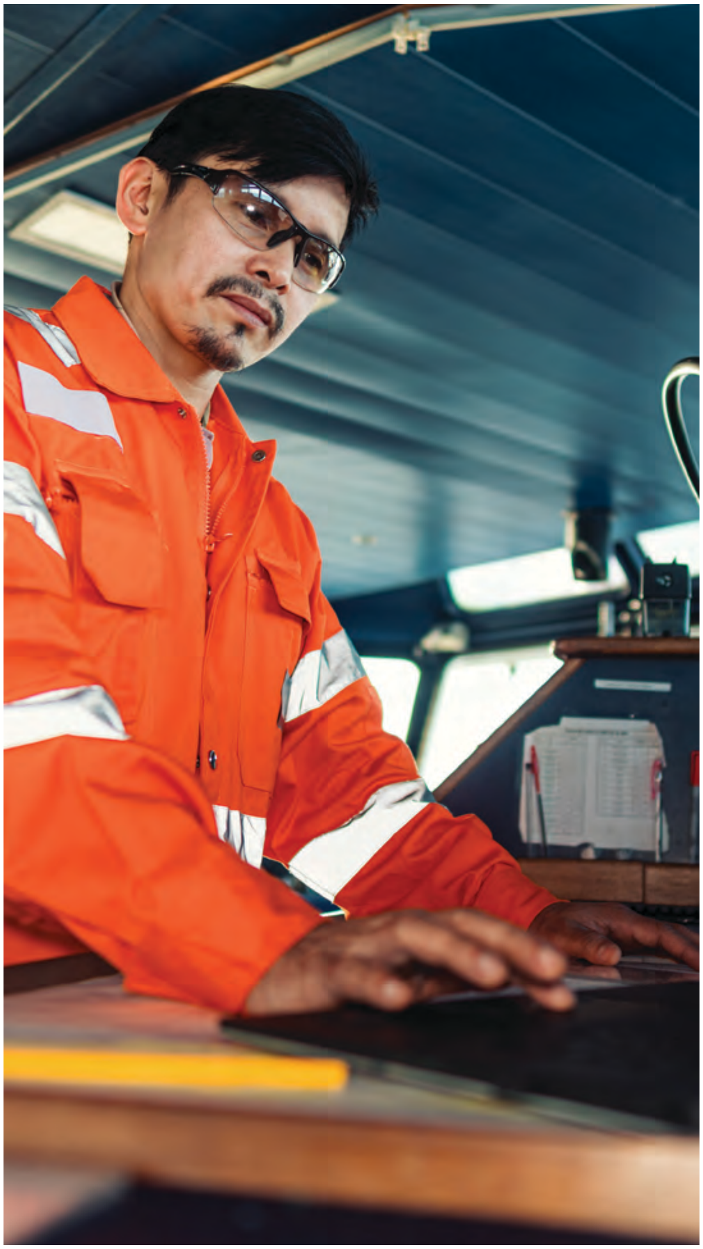
NAVIGATING THE DIGITAL SEAS: CYBER LIABILITY IN THE MARITIME INDUSTRY

Gallagher

Insurance | Risk Management | Consulting

EXECUTIVE SUMMARY

The maritime industry is undergoing a digital revolution by integrating advanced technologies such as automated navigation systems, electronic chart displays and integrated communication networks. While these innovations offer substantial benefits, they also expose the industry to cyberthreats that can disrupt operations, compromise safety and lead to significant financial and reputational damage. Operators are also exposed to threats like social engineering, which can have a significant impact on a company's financials. This article explores the impact of cyberthreats on the maritime industry, the inherent vulnerabilities in maritime operations and strategies for mitigating these risks.



CYBER EXPOSURES IN THE MARITIME INDUSTRY

The three main exposures that maritime operators face are operational vulnerability, data security risks and supply chain vulnerabilities. Operational vulnerabilities include navigation systems, communication networks and cargo management systems. These legacy systems are often outdated and unpatched and can be susceptible to cyber attacks. For instance, GPS spoofing can lead to incorrect positioning, affecting route planning and vessel safety. Similarly, breaches in cargo management systems can result in cargo mismanagement and theft.

The second exposure is data security risks. The maritime industry handles vast amounts of sensitive data, including cargo manifests, passenger information and financial transactions. This data is an attractive target for cybercriminals seeking to exploit vulnerabilities for financial gain or competitive advantage. Moreover, a variety of state, federal and international compliance obligations may be imposed relating to data protection, increasing regulatory risk.

The last exposure relates to supply chain vulnerabilities. The interconnected nature of the maritime supply chain means that a cyber attack on one entity can have cascading effects throughout the network. Third-party vendors and partners with weaker cybersecurity measures further increase exposure to cyberthreats.

Another prevalent cyber exposure is social engineering, which doesn't just apply to maritime operators. Social engineering is a risk that every industry faces. This exposure exploits human error rather than technical vulnerabilities. For example, a hacker might infiltrate your internal system undetected, spending months (or even years) monitoring all incoming and outgoing emails and invoices. Once they determine certain patterns, they reach out to you, pretending to be a vendor or customer that you frequently do business with. It's difficult to realize they're not your normal contact because they often only change one small part of their email address, such as a dash instead of an underscore or a period between names. Assuming they go undetected, any payment sent is most likely gone forever. Social engineering poses a significant risk because it can happen easily and without notice. When you're expecting an email or invoice on a particular day and receive it, you're often quick to complete it without hesitation.

MITIGATING CYBER RISKS

To navigate the digital waters safely, the maritime industry must adopt a proactive approach to cybersecurity:

1. **Robust cybersecurity framework:** Regular risk assessments and the implementation of appropriate security measures are essential. Developing and maintaining a comprehensive incident response plan can help quickly address and mitigate cyberthreats.

2. **Technology solutions:** Encryption technologies and strict access controls can protect sensitive data and limit exposure to critical systems.

3. **Training and awareness:** Regular training sessions can ensure employees are aware of cyber risks and best practices. Engaging stakeholders and collaborating with industry partners to share information and strategies for cyber risk management is also crucial.

4. **Insurance solutions:** Investing in comprehensive cyber liability insurance can cover potential losses and liabilities, providing a safety net in the event of a cyber incident. Most policies provide 24/7 support with a variety of incident response vendors. These include breach coaches, IT forensics investigators, ransomware negotiators, credit monitoring firms, call centers, public relations experts and data asset restoration service providers. Cyber liability policies are very affordable when compared to other lines of coverage like Hull, P&I, Marine General Liability and Bumbershoot.

CONCLUSION

As the maritime industry continues to embrace digital technologies, addressing the growing cyber exposure and liability risks is imperative. By implementing robust cybersecurity measures, fostering a culture of awareness and leveraging insurance solutions, the industry can confidently navigate the digital seas, ensuring the safety and security of its operations and stakeholders. The journey towards a secure digital future in maritime is challenging but essential for sustaining global trade and commerce in the modern world.

REFERENCES

- International Maritime Organization (IMO) Guidelines on Maritime Cyber Risk Management
- Industry reports on cybersecurity trends in the maritime sector
- Case studies on cyber incidents in maritime operations

AJG.com **The Gallagher Way.** Since 1927.

Gallagher

The information contained herein is offered as insurance Industry guidance and provided as an overview of current market risks and available coverages and is intended for discussion purposes only. This publication is not intended to offer financial, tax, legal or client-specific insurance or risk management advice. General insurance descriptions contained herein do not include complete Insurance policy definitions, terms, and/or conditions, and should not be relied on for coverage interpretation. Actual insurance policies must always be consulted for full coverage details and analysis.

Insurance brokerage and related services provided by Arthur J. Gallagher Risk Management Services, LLC License Nos. IL 100292093 / CA 0D69293