The Maritime Executive
INTELLECTUAL CAPITAL FOR LEADERS

Navigating Through the Storm: Cybersecurity and its Stakeholders

iStock

PUBLISHED APR 23, 2024 10:29 PM BY JOEY CHUA

The global shipping industry, covering around 90% of world trade, faces a growing storm in today's digital age: cybersecurity threat. From disrupting critical navigation systems to potentially stealing sensitive cargo data, cyberattacks pose a significant risk to safety, security, and overall operational efficiency. In this article, we investigate the relationship between cybersecurity and stakeholders in the shipping industry and explore how a framework can offer solutions to mitigate these challenges.

The Ecosystem of Stakeholders

The shipping industry operates within a complex ecosystem of stakeholders, each with their own priorities and vulnerabilities in the face of cyber threats.

Internal Stakeholders:

- Crew: Often lacking extensive cybersecurity training, crew members may fall victim to phishing scams or unwittingly introduce malware. A BIMCO report found that 70% of crew members identified phishing as a major cybersecurity concern.

- Management: Balancing security needs with operational costs can be a struggle. Prioritization of cybersecurity investments might be hampered by short-term financial considerations. Third-party Ship Management in particular might be hampered by the competitive nature of the business.

External Stakeholders:

- Regulatory Bodies: Regulatory frameworks for maritime cybersecurity are still evolving, leading to inconsistencies and implementation challenges. IMO has issued MSC-FAL.1-Circ.3-Rev.2, a guideline on maritime cyber risk management, in July 2022 but as the guideline provide high-level recommendations, it is highly dependent on the interpretation of the individual or company implementing it. Similarly, with IACS UR E26 and UR E27, it was shortly revised again to reflect the extensive changes required after industry feedback.
- Adversaries: Motivations for cyberattacks in the shipping industry can range from financial gain to state-sponsored disruption. Cybercriminals may target specific companies, critical infrastructure, or even entire supply chains.

The Adversary's Advantage

The shipping industry presents a unique target for cyberattacks due to several factors:

- Legacy Systems: Many vessels operate on outdated software and hardware, which makes them more vulnerable. These systems include OT systems which are paramount for safe operations.
- Disconnected Operations: Ships frequently operate outside cellular service, relying on satellite networks that may have inherent vulnerabilities unknown to most.
- Limited IT Expertise: Crew members typically lack the specialized skills required to identify and respond to cyber threats. The BIMCO report mentioned earlier found that only 20% of crew members felt confident in their ability to identify and report a cyberattack.
- Tools: Social engineering, the advancement of Deepfake and other emerging technologies can create a breeding spot for adversary to take advantage of. The increasing adoption of automation and interconnected systems onboard vessels introduces new possible vulnerabilities. Technologies like autonomous ships, while promising in terms of efficiency, create new attack vectors that need to be addressed. Similarly, with high-speed low latency connectivity through low orbit satellite, the attack surface area has greatly widened.

Financial, Environment and Human Risks

The NotPetya attack, impacting critical systems, and causing an estimated $300 million in damages is a stark reminder of real-world impact of cyberattacks on the maritime industry. Cyberattacks can have far-reaching consequences beyond financial losses. Disruption of navigation systems can lead to accidents and environmental damage, potentially causing oil spills or collisions.

A Framework for Stronger Defences

To effectively address these challenges and risks, I would recommend a comprehensive approach incorporating People, Process, Technology (PPT).

People:

- Cybersecurity Awareness Training: Human error remains one of the leading causes of cybersecurity breaches. Regular training programs can equip crew members with the knowledge and skills to identify and prevent cyberattacks. This includes phishing scams, social engineering tactics, and secure password practices. An interesting way to go about this can be through gamification.

- Culture of Security: Fostering a culture of security within organizations encourages open communication of cybersecurity and promotes a sense of shared responsibility amongst all stakeholders. This can mean encouraging crew members to report suspicious activity without fear of reprisal. A blame-free environment paves the way for early detection and response to cyber threats. Imagine a scenario where a crew member accidentally clicks on a phishing email but feels hesitant to report it for fear of punishment. This allows time for the adversary to disrupt and infiltrate the network.
- The Importance of Cybersecurity Talent: Addressing the cybersecurity skills gap by attracting and retaining talent within the shipping industry is vital. The industry can benefit from collaborating with educational institutions to develop specialized cybersecurity training programs tailored to the maritime sector. This is something the Singapore Shipping Association (SSA) is actively working on.

Process:

- Risk Assessments: Regularly conducting risk assessments can help identify potential vulnerabilities and prioritize mitigation strategies. This includes evaluating onboard systems, crew training, and external threats.
- Incident Response Plans: It is not if, but when. Having a clear plan in place for responding to cyberattacks can minimize damage and expedite recovery.
- Data Security Policies: Data is our license to trade. Implementing robust data security policies includes data classification, access control, and encryption protocols.

Technology:

- Network Segmentation: Segmenting a ship's network can limit the potential damage an attack can cause by isolating critical systems. This can prevent malware from spreading throughout the entire network if it infects a single device.
- Intrusion Detection & Prevention Systems (IDS/IPS): Deploying these systems on board allows for real-time monitoring of network activity and enables the detection of suspicious activity. IDS/IPS systems can identify and block malware, unauthorized access attempts, and other malicious activities.
- Software Updates & Patching: Regularly patching software vulnerabilities is crucial as it can prevent more than 80% of cyberattacks. Automated patching solutions can help ensure that critical systems are always up to date with the latest security patches.
- Access Control: Robust access controls and user authentication mechanisms can help prevent unauthorized access, thereby reducing the risk of insider threats or non-intentional malicious insider activities.
- Emerging technologies: Leveraging on emerging tech like AI and ML can enhanced the ability to detect and respond to cyberattacks in double quick time. Automation tools can also be deployed to take defensive actions that is not possible to be achieve with normal human intervention.

Collaboration is Key

The shipping industry cannot address the issue of cybercrime in isolation. Effective cybersecurity requires collaboration between stakeholders.

Government and Industry Partnerships:

- Standardized Regulations: Collaborative efforts between governments and industry leaders can lead to the development of clear and consistent cybersecurity regulations for the maritime sector.
- Information Sharing: Open and transparent information sharing between governments, industry players, and cybersecurity experts can provide valuable insights into emerging threats and best practices. This is why trade events like Asia Pacific Maritime serves as an important platform where different stakeholders convey and contribute to insightful discussions like what was discussed during APM 2024 on “Addressing Emerging Threats and Future Mitigation Strategies”. SSA which I am part of also contributes significantly and serves as the voice of the industry to the Singapore Maritime Port Authority (MPA).

International Cooperation:

- Cybercrime Jurisdiction: Given the global nature of shipping, international cooperation is essential to ensure no hiding spot for cybercriminals. International agreements and law enforcement cooperation can help apprehend cybercriminals who target the shipping industry.

Continuous Improvement and Adaptation

The PPT framework provides a solid foundation for a robust cybersecurity posture, but it's vital to recognize that cybersecurity is not a one-time fix. We need to adopt a continuous improvement approach, regularly revisiting RA, updating training programs, and patching vulnerabilities. Staying abreast of the latest cyber threats and adapting security measures accordingly is crucial in this ever-evolving environment.

The shipping industry is the engine of global trade. Its secure and efficient operation underpins the global economy. By implementing a comprehensive cybersecurity strategy based on the PPT framework, fostering collaboration with all relevant stakeholders, and adopting a continuous improvement approach, the shipping industry can navigate the storm and ensure a secure future for global trade.