Online is quickly becoming the new frontline

Jordan Wylie, Communications Officer, Be Cyber Aware at Sea Campaign, argues that it is time for shipping companies to prioritize cyber security on their agenda and explains how this new campaign, which launched in June 2016, supports the industry towards that end. SAFETY4SEA is glad to have become a supporter of this campaign to actively encourage global awareness of the emerging cyber risks at sea. You can explore more about the Campaign or show your support at www.becyberawareatsea.com

SAFETY4SEA There has been an increase on the smart technologies and applications which they are constantly changing the landscape of shipping industry. How vulnerable may these be to cyber-threats and how can we avoid a possible attack? Jordan Wylie Today’s onboard Operational Technology and Information Technology systems are becoming increasingly connected like never before, this hyper-connectivity greatly increases the risk of critical systems such as safety, propulsion, or navigation being exposed to internet-based and insider cyber-threats. Additionally, shipping companies and their vessels are not immune to the relentless cyber-criminal threat, seeking financial rewards as well as sensitive company or employee information by using common social engineering techniques such as phishing, business email compromise and other basic scams. Whilst certainly not as catastrophic as the loss of a ship’s navigation systems, the loss of money and/or critical information can have a significant financial, legal, and reputational impact on the shipowner, manager or charterer.

Avoidance of a possible attack on either IT or OT systems from either an internet-based or insider threat starts with companies understanding the threat; understanding their IT and OT environments and how they’re connected; assessing where those environments could be exposed to the threat; and then managing that exposure. Shipping companies need to recognize and prioritize cyber security in their risk registers and assign accountability for managing this risk to appropriately qualified senior executives. This is NOT an IT issue, as I am often told by senior executives, CSO’s/DPA’s and onboard senior officers.

How would you assess the levels of maritime cyber security awareness in the industry? What does the industry need to build cyber security awareness? J.W. Cyber security awareness across most industries globally is still relatively poor but it is particularly lacking in the shipping industry, as part of my own Master’s Degree in Maritime Security I spent a significant amount of time exploring this area, the findings after extensive research, interviewing and questioning was the catalyst for the launch of ‘Be Cyber Aware At Sea’. Organizations’ employees remain one of their biggest cyber security vulnerabilities due to a lack of understanding and awareness of the risk. Instead of using highly technical and time consuming hacking methods to breach a company’s systems, cyber criminals often prefer to target the employees themselves who are considered the “soft target” in order to get access to information and systems.

Education for the senior leadership team, shore side staff and onboard crew members is key to raising awareness of the developing cyber security risk – but this needs to be a constant process, not a once off box-ticking
exercise. Company executives, heads of IT departments, CSO’s and SSO’s onboard should be regularly communicating the cyber security message across the organization with the help of awareness courses, awareness campaigns, and regular testing. Heightened awareness will greatly improve a company’s ability to effectively manage the cyber security risk, when at sea and onshore.

**W45 What are the Campaign’s goals and aspirations and feedback received so far across the industry?**

**J.W.** The ‘Be Cyber Aware At Sea’ campaign is a completely free not for profit initiative to help raise awareness of the cyber risks and threats to international shipping. Our main objectives are to inform and educate in order to increase awareness and understanding. After spending 2 years researching what shipowners understand about cyber security risks and how they managed those risks, it was clear there as a lot of work to be done to ensure this issue is taken seriously and I felt an innovative messaging campaign and suite of free resources was the best way to do this. I hope I can make a significant contribution to the international shipping and offshore sectors by simplifying a subject that is often considered too technical and complex for most people. I have been overwhelmed by the support and traction the campaign has gained to date worldwide and I am delighted that some of the biggest names in shipping from all sectors such as Teekay, Imarsat, North & Standard P & I Clubs, P & O Ferries, Navarino, Holman Fenwick Willan marine lawyers and even the British Royal Navy have come onboard, to name just a few.

**W45 What is your key message to the industry regarding cyber security? What do you think should be the industry’s priority to move forward?**

**J.W.** Unfortunately, with the rate of new malicious software (viruses) and attack methods being discovered every day, a data breach or cyber-attack is no longer a matter of “if” but “when”. The business, financial and reputational impact experienced by a company resulting from an attack will be completely dependent on the measures they implement today to adequately manage the risk. Key control measures include awareness and education, vulnerability management and cyber insurance. This needs to be an issue that is understandable and managed from the boardroom all the way through to the depths of the engine room onboard. My final message would be to highlight that ‘online is quickly becoming the new frontline’ and fortune favors the cyber prepared.

---

**How to secure your System/Personnel from Cyber Incidents**

- Cyber Security Policy
- Threats / Risk Assessment
- Risk Management
- Office / Vessel Contingency Plans
- Incident Investigation
- Cyber Risk Assessment Library

Explore and Learn more at: sqemarine.com/solutions