Offshore innovation breeds rapid evolution of emerging cyber threats

Cormac Mc Garry, maritime analyst and Bianca Miclea, researcher in cyber threat intelligence at Control Risks

The offshore sector’s pivot towards innovations in automation and internet-enabled communication, control and navigation systems brings with it a new threat dynamic concerning cyber security. While the traditional threats of piracy and armed robbery persist in a number of hotspots around the world, new technologies are attracting new threat actors who are learning how to target our offshore assets anywhere at any time. In response, our attitudes and practices towards securing our offshore industries will have to quickly adapt to this rapidly changing risk environment.

Offshore innovation has inevitably led to regulation, with a number of key developments set to change the maritime risk environment leading to a new cyber paradigm that is dominating conversations between maritime security professionals. There are, broadly speaking, three key developments set to change the maritime risk landscape in the coming years that must be addressed sooner rather than later to ensure organisations mitigate their risks:

- By July 2018, most merchant vessels will be required to on-board Electronic Chart Display and Information Systems (ECDIS). These new systems will leave offshore assets vulnerable to a range of emerging cyber threats that previously posed no threat to vessels carrying only paper charts.

- By January 2021, vessels will be required, under an International Maritime Organization (IMO) resolution, to incorporate cyber security measures into existing risk management practices in order to adhere to International Safety Management (ISM) regulations. This will include requirements to address cyber-related threats, appoint risk control personnel and data protection officers, and implement impact assessments, response measures, and contingency and recovery plans. Failure to comply could lead to costly vessel detentions by port authorities.

- This reflects broader developments that also affect the maritime sector, such as EU directives on security of network and information systems (the NIS Directive), which seek to enhance the culture and infrastructure of cyber security across EU member states, and the General Data Protection Regulation (GDPR), which will also require the introduction of data protection officers and cyber impact assessments.

Many maritime professionals may be frustrated by yet more upcoming compliance issues to adapt to. However, the modification to the ISM Code and other regulatory changes are a reflection of the increasing number of vessels found to have malware on board, and to have been affected by attacks such as GPS spoofing and other relatively basic cyber incidents that could seriously affect ship operations and navigation safety.

Understanding cyber threat actor motivations

Despite these incidents and the growing concerns of regulators, cyber threat actors – particularly nation states and sophisticated cybercriminal groups – remain largely focused on sectors such as finance and IT and communications, and have yet to demonstrate effective tactics, techniques and procedures (TTPs) to seriously breach seagoing vessels. However, amid an overall lack of security – such as the use of default access credentials and bring your own device (BYOD) – and with a high volume of assets and high sensitivity of data held in ports and vessels, such threat actors are taking an increased interest in the sector.
However, our own cyber threat intelligence suggests this interest is likely to grow in the years ahead as cyber threat actors begin to study internet-enabled devices used on vessels, such as SAILOR 900 VSAT and ECDIS, to collect critical information about the location or cargo of vessels and manipulate it for malicious purposes. This will also contribute to the further development of cybercrime as threat actors increasingly seek to exfiltrate sensitive data for financial gain. As well as financial and reputational damage, such attacks could threaten vessels’ seaworthiness.

So far threat actors targeting the sector have been largely limited to email phishing, malware, ransomware and exploiting network vulnerabilities enabled by satellite communications. However, attacks such as that on the navigation systems of 20 Russian vessels off the port of Novorossiysk on 11 June have shown an emerging threat of GPS spoofing and signal disruption attacks. A large-scale GPS spoofing attack could easily lead to vessel collisions and severely disrupt ports and shipping bottlenecks, such as the Singapore or Hormuz Straits.

We assess that these types of attacks have been largely initiated by state actors, either as part of espionage and sabotage campaigns or simply to test their own capabilities. Such methods may allow threat actors to conduct cyber operations in maritime zones of geopolitical significance, such as the South China Sea, the Black Sea, the Eastern Mediterranean and the Baltic Sea.

### Protecting the offshore sector from the cyber menace

To help protect their vessels from these emerging cyber threats and to comply with the 2021 deadline, while still allowing for technological innovation, maritime operators should implement specific cyber security programmes tailored to their specific threat landscape. These should include employee education about the use of default access credentials and BYOD on board, and measures to identify vulnerabilities that affect critical internet-connected or computerised vessel systems.

These programmes should also be a part of bringing cyber space into existing offshore risk management practices. We regularly see offshore operators enjoy tremendous success in areas of traditional danger because they take a robust multi-levelled approach to risk management. This allows them to seize opportunities by building resilient assets while ensuring a duty of care to their people. The same approach to
cyber space can bring companies smoothly into the new risk environment. Operators should assess their cyber risk exposure based on their current level of cyber security maturity, develop measures to detect early signs of potential infection, and develop processes for responding to, recovering and learning from cyber security incidents.

Any assessment of such exposure will be informed by an understanding of the rapidly shifting landscape of cyber threat actors’ intentions and capabilities. Instituting a cyber-threat intelligence programme focused on both the motives and the methods of such threat actors will help maritime companies understand who might target them and how, allowing them to defend themselves against the emerging threats facing the offshore sector while also complying with the changing regulatory environment.

For more information please email Enquiries@controlrisks.com