ARTICLE

ASTAARA
COMPANY LIMITED

Shipowners beware – not only can hackers get in, they can also run off with your ships

Summary

Two recent reports will have alarmed shipowners, ship managers and charterers: their ships are seriously at risk.

1. a UK cyber[1]penetration testing company found serious gaps in IT security aboard ships and rigs, and claimed it could have taken full control of an oil rig;
2. a report[2] that the Department of Homeland Security, Pentagon and Commerce Department have been tasked to reduce US reliance on GPS for navigation and time keeping following high profile GPS spoofing events, citing inter alia the Stena Impero.

The level of alarm that these trigger within the boards of shipowners / ship managers and charterers might well fairly represent their levels of voyage planning and cyber maturity:

- The mature will redouble their efforts to improve safety and the enterprise's resilience to cyber attacks.
- The immature will brush both issues aside, saying it is someone else's problem.

A cursory understanding of the issues might focus criticism on the captain and crew. But it important to realise that the hackers are far more sophisticated in their understanding of technology: It is the ship and shore-side management and, in particular, the captain and crew that **need support** rather than criticism.

The GPS and security risks and vulnerabilities are already identifiable and capable of management. They can be prioritised (by safety) and the risks can be mitigated by prudent ship operation.

Detail

The Register in their 18th February 2020 article reported Pen Test Partners' claim to have breached the cyber security of a number of marine assets, including an oil rig, and to have identified many serious failings in cyber security on board these vessels.

It would be easy just to blame the shipping company, captain and crew for a generally slapdash attitude to cyber security and move on. But this would miss the point.

Equally, in events where ships have steamed off course due to external interference, the finger of blame has pointed to poor navigation on the bridge. But GPS spoofing is insidious – and potentially life threatening.

There are several key questions:

- When does a watch keeper know when their position is wrong?
- How does the shipowner evidence passage planning to make the ship seaworthy (and cargo worthy) at the commencement of the voyage in light of such risks?
- How does a shipowner minimise the GPS vulnerability?
- How do you make your ship more resilient?

It is no secret that maritime cyber security is not as good as it should be. A lot of work is going on to improve the situation at every level: global, national and local. Nor is it a secret that marine systems are vulnerable to exploits if left undefended and a number of large shipping companies have suffered from large breaches in the last few years.

[1] https://www.theregister.co.uk/2020/02/18/shipping_cybersecurity_rather_poor/

[2] https://splash247.com/trump-adds-to-growing-concern-about-gps-interference/

Mind the Gap.....

The realisation for shipping companies is in fact sobering. Hackers are getting more sophisticated over time. Every day that passes with shipowners not investing in cybersecurity and the training, education and awareness-raising of its staff (crew and shoreside) necessary to protect their interests, the gap widens.

A question the affected companies should reflect on is whether the adoption of the basic measures enshrined in Cyber Essentials Plus (CE+)[3], for example, might have prevented such exploits.

Each case will differ, and it will be for the experts to determine, but by following CE+ in the technical environment and training their people, shipowners could have mitigated the consequential losses posed by many exploits such as the ones described in both articles.

It is not just on the ship.....

While most of the threat to the ships comes from their own head office, it is also plausible that an attacker can attack a ship through its own IP address rather than travelling down a VPN to attack the ship itself.

The drive for digitisation of shipping, while an important initiative, needs to address cyber security upfront, following the principles of 'security by design'. If security is left to the end, it will be regarded as an expensive afterthought not as an integral capability, and therefore create vulnerabilities that are harder (and more expensive) to deal with.

Equally planners and owners must take into account particular events that may impede the safe prosecution of a voyage, including the GPS spoofing events in the Persian Gulf and Black Sea - in the same way that they would for navigation through areas of enhanced risk due to piracy/ terrorism.

Owners and operators will be aware that the mere existence of a passage plan does not prima facie give a ship owner the evidence to support their contention that their ship was seaworthy - a point recently reaffirmed in the Admiralty Court where Teare J[4] stated:

> *“Given that, as stated in the IMO Resolution of 1999, a "well planned voyage" is of "essential importance for safety of life at sea, safety of navigation and protection of the marine environment" one would expect that the prudent owner, if he had known that his vessel was about to commence a voyage with a defective passage plan, would have required the defect to be made good before the vessel set out to sea.”*[5]

The era of isolation between ship and shore for the duration of a voyage is over. Ships can talk to each other, crew can keep in touch with loved ones at a relatively low cost. This connectivity will only increase with all the attendant issues and opportunities such developments in technology will permit.

As these technologies become ever more prevalent, users must be ready to take responsibility, undergo regular and ongoing training to ensure that voyage planning and their use of the technology is secure. Without training, the two complacencies will return:

- old habits die hard; and
- workarounds will multiply

and so will vulnerabilities which hackers will be all too willing to take advantage of.

[3] https://www.cyberessentials.ncsc.gov.uk/

[4] *Alize 1954 v Allianz Elementar Versicherungs AG* (The CMA CGM LIBRA) [2019] EWHC 481 (Admlty) (8 March 2019)

[5] For a commentary of the case in full see: https://www.quadrantchambers.com/news/unseaworthiness-and-passage-planning-the-cma-cgm-libra-john-russell-qc-and-emmet-coldrick

What is the answer?

Doing the minimum badly is easy. Believing that ships are safe purely because they are away from shore, and solely facing traditional marine perils misunderstands the ability of hackers to access, reconnoitre, wait and craft an attack. Using a few simple techniques such as Cyber Essentials+ can eliminate a number of the basic risks.

This also extends managing these vulnerabilities and integrating risk management into voyage planning. While we are not advocating reversion to celestial navigation, equally we assert that bridge management teams might / must, amongst many more additional actions, employ increased use of dead reckoning on the chart routinely to challenge position keeping devices, and ensure that passwords on the underlying primary technology systems have been changed from their factory defaults, under a formal access management regime.

Digitisation also provides a useful – and rare – opportunity to review fully the security posture of both ships and land-based systems. To the extent possible Business Continuity and Disaster Recovery Plans need to be tested and lesson learned in the context of what is known.

The Astaara view

As the attack surface widens, the basics of cyber security and the implementation of sound risk management activities can no longer be ignored:

- policy and governance needs to be updated;
- technical, logical and physical security measures all need to be implemented and maintained;
- people need to be trained to spot the unwanted or the unexpected.

Furthermore, where third parties provide services to ships and ports, their bona fides need to be established with respect to their security posture, and their obligations enforced through contract. Ship and shore need to assess the risks and work together continuously to maintain an appropriate balance between risk and return – it is an issue for the whole enterprise.

Robert Dorey
William Egerton
2nd March 2020

Contact

Robert Dorey:	robert.dorey@astaara.co.uk	+44 (0)7775 515 878
Bill Egerton:	william.egerton@astaara.co.uk	+44 (0)7747 051 806

#AstaaraCyber #ResilienceandRecovery #marinecyber