athena dynamics

Low Hanging Actionable Insights For Maritime Cyber Protection

Author: Ken Soh, Group CIO, BH Global and CEO, Athena Dynamics

Since BIMCO (Baltic and International Maritime Council) first published its cyber security guidelines in 2016 and followed by IMO's (International Maritime Organization) Resolution MSC 428(98) Maritime Cyber Risk Management guidelines in 2017, the maritime sector saw gradual progression of cyber safety awareness.

Subsequently, OCIMF (Oil Companies International Marine Forum) published cyber safety chapters in its Ship Inspection Report Program in 2018. This was followed by IACS' (International Association of Classification Societies) technical guidelines in 2021 which stipulated all new builds in 2024 onwards to be cyber compliant.

Today, we are not short of cyber incidents happening in onshore ports and offices, and offshore vessels and rigs as well, despite the above-indicated efforts in compliances and safety framework.

Unfortunately, cyber security is fundamentally an unceasingly dynamic "team sport". With 500,000 new viruses emerging globally every day, incidents are expected to grow. With the existing compliance frameworks, has the maritime sector ever started, or have it even started to cyber protect effectively?

The answer, in my opinion, is no.

Urgent need for cyber security

Looking back slightly a decade or so, the maritime industry faced major challenges such as global industry-wide slowdown, various forms of oil crisis, sulphur emission control and before long, the arrival of global covid pandemic.

Would there still be appetite for cyber protection? Unfortunately, whether the appetite is there, cyber protection is fast becoming an urgent mandate impacting businesses and operations, rather than a question of necessity.

With chapters and chapters of cyber-related controls published by authorities, do ship owners know where to begin in the first place?

Cyber protection is never a matter of throwing money into it and hoping that the matter will be taken care of by itself. The ship owners need clear and concise directions, and actionable insights to kick-start their long-term journey into achieve strong cyber security postures for their vessels.

To begin with, ship owners need to understand that cyber security is never a matter buying a protection or monitoring product. It is so important to always remember that the first step is always to find out what are they protecting and what are their vulnerabilities to begin with.

I would therefore suggest the following direction and actionable insights for ship owners to establish baseline on which various compliances could build. In other words, a friendly lighthouse to assist ship owners to start their journey with identifiable, tangible low-hanging fruits.

Low hanging fruits #1: Knowing my IT/OT assets, knowing my vulnerability

We observed that many ship owners do not have the most up-to-date or a complete list of their onboard information technology (IT) and operational technology (OT) assets. We need to be clear of what we own to know what to protect. Alongside that, it is also important to have visibility of the current assets and setup.

Today, there are automated tools which are fully software based, which are able to be done fully remotely via online access from onshore into the ships to minimize the logistics of onboard device or hardware installation and maintenance.

Such kind of tools, coupled with qualified service providers, could assist with swift re-discovery and re-construction of asset list and network topology, reducing effort which in the past which took months, to just a couple of days. The same tools could then be utilized for onboard cyber security monitoring too.

Low hanging fruits #2: Knowing what to do when incident happens

Professional “red teaming” services could be engaged to trial cyberattack from the outside. With that, a deeper understanding of how vulnerabilities are exploited for attacks, and therefore what to do and how to react when such matter happens.

These are critical processes which ship owners need to understand well in order to perform incident response accurately during “war time”, which is vastly different from protection operations during business-as-usual “peace time”.

Such services are already readily available nowadays. Unfortunately, they are mostly focusing on IT systems for onshore enterprises and industries. It is therefore important to sieve out experienced service providers with credentials in maritime IT and OT.

Low hanging fruits #3: Countering attack vectors via disruptive innovations

It is well-known that the three common attack vectors are: email, USB external devices and browser.

While the landscape is not short of commonly heard fundamentals such as “Zero Trust”, “Defense in Depth” and “Security by Design”, such concepts in my opinion have been overstated with superficial teaching.

Deeper considerations such as whether they are implemented with detection-based or detection-less is key. Realizing such concepts completely on detection-centric approach is almost like an oxymoron. This is for the simple reason that detection-centric technologies would never be able to protect us from the undetectable, regardless of whether which of the three concepts are deployed.

Maritime industry has the advantage to start from a clean slate as the relatively slower mover to cyber protection. It is timely hence for maritime to start from a clean slate, adopt and adapt to well-tested technologies, avoiding the mistakes and pitfalls encountered by the onshore enterprises and industries thus far.

Specifically, ships and vessels could deploy well-proven detection-less sanitizers to cleanse files coming in via email, USB devices and browsers. Such kind of sanitizers (also technically named Content Disarm Reconstruction, i.e., CDR), when coupled with Remote Browser Isolation (RBI) technologies, would help to form a formidable protection again advanced malware and attacks than traditional protection paradigm.

Low hanging fruits #4: Addressing weakest point in people, process, technology

The three dimensions to cyber security of people, process, and technology is well known. “People” as the weakest point has been well said too. How could we effectively address it in the maritime sector?

It is impractical to conduct class-based awareness training to seafarers when the nature of their job requires them to be “away and apart” most of the time.

Self-paced computer-based training is therefore a directly effective option. I foresee such option will gradually transform from offline to online possibilities going forward as cost-effective offshore accessible bandwidth improves. It would be useful to design such training with qualifying tests that forms part of career advancement framework for the seafarers.

This, coupled with regular phishing campaigns would help aplenty in identifying the weakest in the weakest point so that education and re-learning could be focused on the highly-focused group.

athena dynamics

Low hanging fruits #5: Re-thinking of IT and OT connections onboard ships and vessels

While onshore, Industrial Control Systems (ICS) are critical, and cyber security expertise and resources are readily available when needed. Unfortunately, ICS onboard ship does not come with such privileges when such skills and resources typically does not exist. The effect of an incident could be catastrophic if it happens in the open sea where the ship has only its own to call for.

It is not uncommon now to observe weak IT and OT separation onboard ships and vessels. Some may just depend on access control means, or simple firewall. The proven practices in onshore OT such as uni-directional conduits are therefore highly encouraged. The use of such measures as data diode and protocol breakers may seem remote at the moment.

This is unfortunate, but is also fortunate that low-cost, well-certified data diodes is starting to emerge lately. I encourage such transition and adoption soonest for the ultimate wellbeing of ships, before major incident happens to the most critical infrastructure of the ship as technology and bandwidth improve.

Low hanging fruits #6: Harnessing technologies for quantum leap in incident response time

The average time to perform conclusive digital forensic and effective incident response (DFIR) is about two to three weeks. This is unfortunately way too late before further complication could happen in common scenarios.

Fortunately, the advancement of DFIR technologies have resulted in new concept platform that shrinks DFIR effort from weeks to minutes.

While Security Operation Centers (SOC) grows, it is also important for the monitoring platform to adopt and incorporate such new generation DFIR platform, on top of common End Point Detection and Response (EDR) or Extended Detection and Response (XDR) systems to achieve high speed recovery should incident happens which may impact not just operations, but the lives and wellbeing of seafarers onboard vessels.

In conclusion, the maritime industry should take advantage of the advancement in protection technologies, which are well-practiced in onshore platform, and transit them for offshore purposes.

There is no better time than now since awareness of cyber security has risen rapidly over the last couple of years.

Do remember that cyber protection is not about going out to source for a protection product. It is about full visibility of our own assets, and our security weaknesses to begin with.

While the industry is not short of cyber security expertise, it is important to engage one with credentials in the maritime sector – a sector with needs and etos vastly different from the onshore counterparts.

athena dynamics

Source: https://athenadynamics.com/low-hanging-actionable-insights-for-maritime-cyber-protection/

Disclaimer: The outcome of general best practices introduced in this material may vary due to environmental and contextual parameters. Neither BH Global Corporation Ltd, Athena Dynamics Pte Ltd nor the writers are responsible for any direct or indirect implications/impacts to the readers due to the adoption of these practices.

ATHENA DYNAMICS PTE LTD
8 Penjuru Lane, Singapore 609189.
Tel: 65 6291 4444 Fax: 65 6291 5777
www.athenadynamics.com

A Member of BH GLOBAL CORPORATION LTD