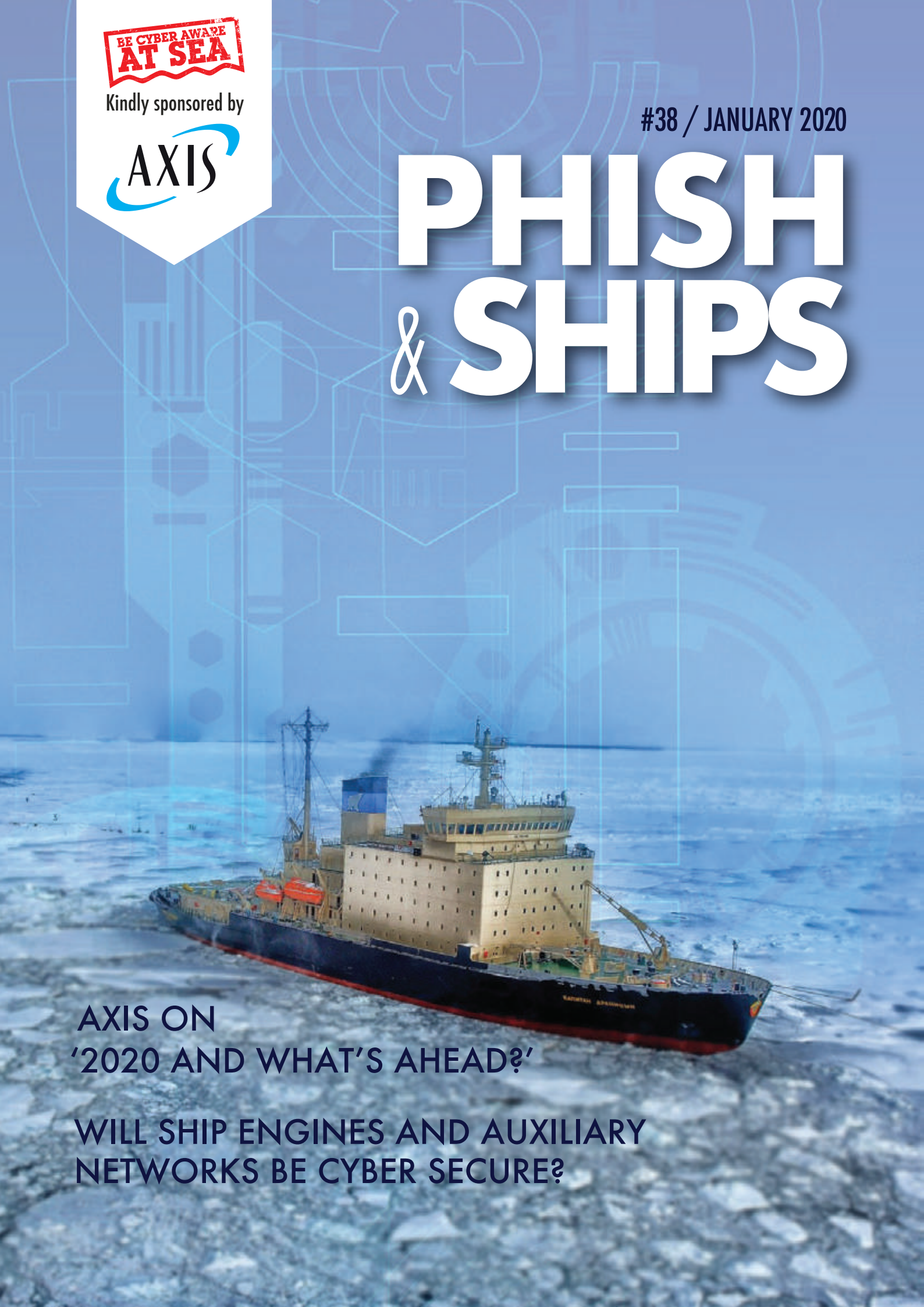
BE CYBER AWARE AT SEA

Kindly sponsored by

AXIS

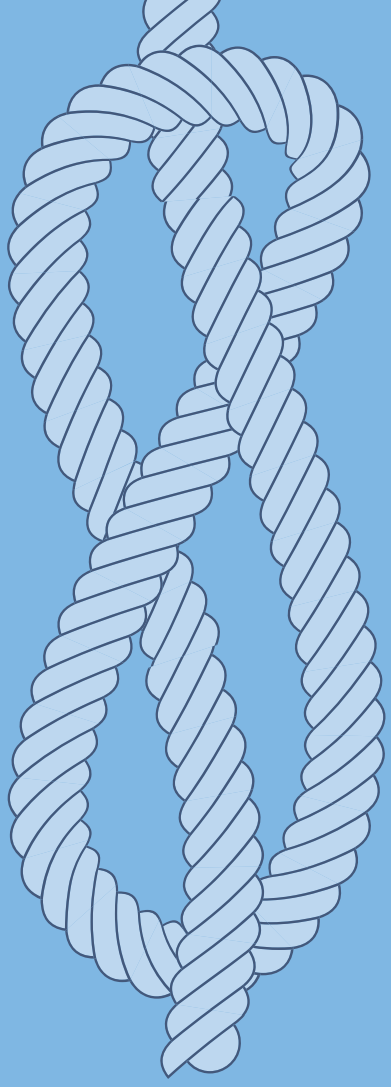
#38 / JANUARY 2020

PHISH & SHIPS



AXIS ON '2020 AND WHAT'S AHEAD?'

WILL SHIP ENGINES AND AUXILIARY NETWORKS BE CYBER SECURE?



OUR AWARDS

WINNER 2018
SMART4SEA TRAINING AWARD

HIGHLY COMMENDED 2017
SAFETY AT SEA AWARDS

WINNER 2017
BEST CYBER AWARENESS CAMPAIGN
INTERNATIONAL CYBERSECURITY AWARD

PHISH & SHIPS

FROM THE EDITOR

Happy New Year! Welcome to this month's edition of Phish & Ships, brought to you by The Be Cyber Aware at Sea campaign.

The start of a new decade, let alone a new year, is a time of fresh resolution. For the maritime industry it should be an opportunity for us all to take stock on how far we've come and what more we can do in tackling cyber-crime.

The cyber landscape is still as complicated as ever; this month we bring further details of another cyber-attack in the US which brought a facility to a standstill for 30 hours. Meanwhile the tensions rising in the Middle East mean state-sponsored cyber incidents look likely to increase.

We urge you all to hit the ground running this January – refresh your knowledge of cyber threats, check your procedures and ensure they are known and understood by employees, and explore the technology options that can support and protect you and your organisation. We wish you all well for 2020!

Please continue to follow us at:
Website: www.becyberawareatsea.com
Twitter: @CyberAwareAtSea
Facebook: Be Cyber Aware At Sea
Linkedin: Be Cyber Aware At Sea

Your Editor-in-chief,
Jordan Wylie MA, BA (Hons) Founder,
Be Cyber Aware At Sea

2020 - WHAT'S AHEAD?

BE CYBER AWARE AT SEA

Kindly sponsored by AXIS

The shipping industry saw a steady increase in cyber related problems in 2019. From the U.S. Coastguard reporting of a successful malware incident on a vessel that left it seriously debilitated, to the ransomware attack that hit Norsk aluminium and renewable energy leading to a $52 million loss. Whilst Norsk isn't a directly-related shipping company, it does serve as a wakeup call that if a company of that scale can be crippled, almost any maritime or logistics company of a similar size can suffer the same fate.

So, what lies ahead for shipping in 2020?
We can expect to see an increase in companies improving their cybersecurity on board vessels. The IMO regulation that commences enforcement in 2021 is a concern for major classification societies and it is likely that the more tech-enabled merchant categories such as the container, VLCC and LNG/LPG communities will continue to lead the way. Sadly, at the bottom end of the market, there will continue to be risk takers. Those risk takers should consider hardening onshore IT systems if they are to, at the least, protect themselves from the most basic malware attacks and scams.

Scams will increase. There's simply too much money to be made in Business Email Compromise (BEC) scams and the growing, more sinister, deep fake scams that use natural language techniques and AI to trick victims into handing over information or money. This will most likely increase first with phone calls to accounting departments. The maritime and logistics industries will continue to be a high-target sector because of the volume and size of transactions – it makes it a lucrative opportunity for criminals. It will require further investment from businesses in training and awareness initiatives to mitigate the risk.

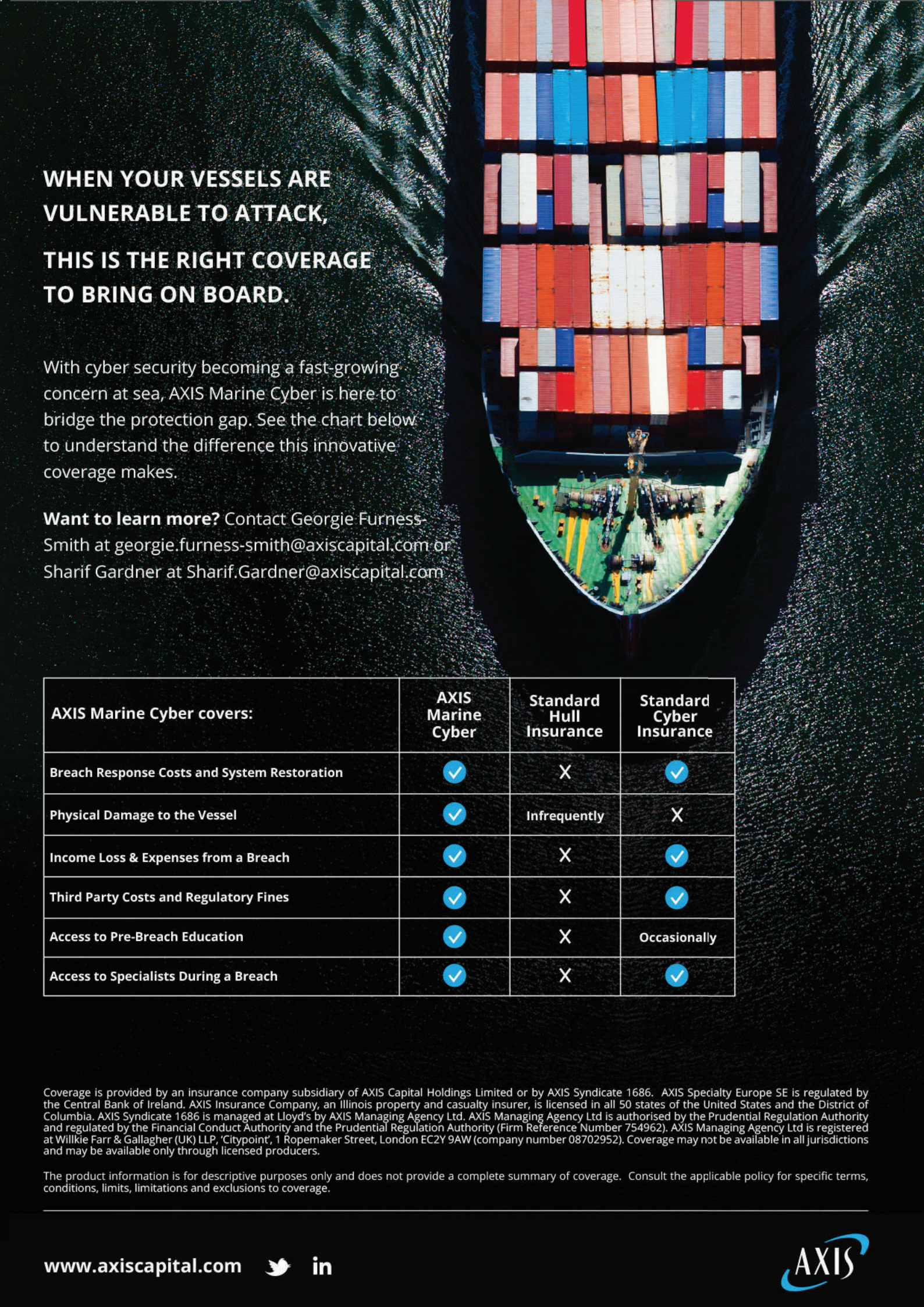
Awareness fatigue will also be discussed more in 2020 with methods to counteract its ability to permeate. Unfortunately, I believe that this will be a year that many will start to feel cybersecurity awareness fatigue. This is where terms such as 'the human firewall', 'skills shortage' and **'AI' will lose impact.** They have been useful terms in pricking the ears up of business leaders but now is the time that awareness should be supported by very real, structured training initiatives. Classroom based methods, 'tool-box talks', table-top exercises amongst leadership teams and IT teams, and YES, e-learning are all good trainings that work. Use these tools to reduce risk!

Ransomware will rage on so make sure to conduct your business impact analysis. Ransomware has not only increased in ferocity, it is also putting companies out of business. A small U.S. healthcare firm, Brookside ENT & Hearing Services shut its doors for the final time in 2019 because it refused to pay a $6,500 ransom. The city of Georgia in the US paid a $400,000 ransom demand. According to a U.S. Government technology blog, one insurer analysed 3,300 ransomware attacks against their clients and found the highest ransom demand $8.5 million, with the highest demand paid by one of their clients being $935,000. The stats suggest that demands are increasing and businesses need to be able to recover from back-ups effectively or risk having to make the decision to pay potentially millions to criminals.

Finally, conflicting nations will fuel cybercrime.
Geopolitical supremacy and political unrest, especially in the Middle East could spur state-sponsored cyber attacks that would certainly spill over and affect businesses. Given the current tensions between the U.S. and Iran, this could come to life as a devastating cyber attack on a port or shipping company with operations in the region. What is more likely is that hackers globally will continue to recycle and reuse existing attack vectors for new cyber attacks – and they may use previous nation state weapons to conduct them. IT teams need to be rigid with patch management programmes to ensure they do not fall victim.

Article by Sharif Gardner, Head of Training and Advisory Services, AXIS

https://www.theguardian.com/business/2019/apr/11/small-business-ransomware-attacks-precautions-prevent
http://m.startribune.com/all-of-records-erased-doctor-s-office-closes-after-ransomware-attack/508180992/
https://www.govtech.com/blogs/lohrmann-on-cybersecurity/ransomware-attacks-becoming-are-more-widespread-destructive-and-expensive.html



WHEN YOUR VESSELS ARE VULNERABLE TO ATTACK,

THIS IS THE RIGHT COVERAGE TO BRING ON BOARD.

With cyber security becoming a fast-growing concern at sea, AXIS Marine Cyber is here to bridge the protection gap. See the chart below to understand the difference this innovative coverage makes.

Want to learn more? Contact Georgie Furness-Smith at georgie.furness-smith@axiscapital.com or Sharif Gardner at Sharif.Gardner@axiscapital.com

AXIS Marine Cyber covers:	AXIS Marine Cyber	Standard Hull Insurance	Standard Cyber Insurance
Breach Response Costs and System Restoration	✓	X	✓
Physical Damage to the Vessel	✓	Infrequently	X
Income Loss & Expenses from a Breach	✓	X	✓
Third Party Costs and Regulatory Fines	✓	X	✓
Access to Pre-Breach Education	✓	X	Occasionally
Access to Specialists During a Breach	✓	X	✓

SHIP ENGINE AND AUXILIARY NETWORKS WILL BE CYBER SECURE

A leading classification society has awarded one of the first cyber security certification to a key original engine manufacturer.

Marine technology and engines group Wärtsilä has been awarded Lloyd's Register (LR) system-level cyber certification, one of the first to be awarded globally.This relates to Wärtsilä's network architecture for its integrated main and auxiliary machinery.

This certification comes as more ships being built and delivered have information and operational technologies (IT and OT) networked together, increasing their vulnerability to cyber attack.

Therefore, it is a top priority of Wärtsilä to build resilience against unauthorised access, software failures or attacks on ships' systems. LR's certification is a reassurance for shipowners that their IT and OT systems are secure from cyber threats.

"This certification validates Wärtsilä's work in mitigating cyber security risks with the appropriate controls in the integrated system, when collecting and sharing operational data," said Wärtsilä's general manager for cyber security in the marine business.

"This takes Wärtsilä lifecycle offering to the next level and knowing that these systems are cyber secure provides customers with the assurance that they are safe to use."

Wärtsilä has made other inroads in cyber security. It opened an International Maritime Cyber Centre of Excellence (IMCCE) in Singapore, in 2018. This comprised a Maritime Cyber Emergency Response Team (MCERT) and a cyber academy.

Wärtsilä has also made progress with its vessel traffic technology in 2019. It secured a contract in October to supply its Vessel Traffic Service (VTS) solution to two of France's leading northern ports. Calais and Boulogne will upgrade vessel traffic control with this VTS to deliver greater operational efficiency and safety.

This VTS will help the ports manage vessel traffic in these busy harbours, optimising planning and traffic monitoring to reduce waiting time for vessels and allow just-in-time pilotage.

Calais is the leading port in France for passenger traffic and the second largest port in Europe for RoRo vessel traffic. Boulogne-sur-Mer is the leading fishing vessel port in France.

Wärtsilä secured this order from Région Hauts-de-France, the government entity responsible for this tender.

This will be delivered during the Calais Port 2015 project deployment, which is one of the France's largest maritime construction undertakings, and is the first maritime project within the European Union's investment plan for priority infrastructures.

Cyber AiP explained

Lloyd's Register defines 'cyber-enabled' systems as those installed on ships that have traditionally been controlled by the ship's crew. However it increasingly includes the capability to be monitored, or monitored and controlled, either remotely or autonomously with or without a crew on board. The level of cyber risk varies from system to system, and mitigation actions need to be made appropriately.

This AiP award comes just one year before the enforcement of IMO's Resolution MSC.428(98), which means shipping companies must have appropriately addressed cyber-security risks in their Safety Management Systems (SMS) by 1 January 2021.

Guidance and standards on how these cyber-security risk controls shall be built is currently defined by classification societies.

Riviera Maritime Media will be expanding its series of Maritime Cyber Risk Management events in 2020.

This is another development in the professionalisation of accreditation and compliance to cybersecurity in shipping. At the Be Cyber Aware at Sea campaign, we are constantly assessing the future of cyber risk and risk management. Having Lloyd's Register award Wärtsilä the system-level cyber certification helps set the standard for all engine manufacturers going into the new decade.

https://www.rivieramm.com/news-content-hub/news-content-hub/ship-engine-and-auxiliary-networks-will-be-cyber-secure-57283

ABS RELEASES MARINE AND OFFSHORE CYBERSECURITY TOOLKIT

The push for digitalization is driving the need for greater cyber protection across the marine and offshore value chain.

As vessels, ports and facilities become more automated, connected and digital—and information technology (IT) converges with operational technology (OT) systems—operations are increasingly vulnerable to cyber risks and the uncertain threat of a cyber attack.

Cyber risks in OT assets are linked to serious safety, financial and environmental consequences for mariners, offshore operators, regulators and the public.

Trusted risk advisors to the global marine and offshore industries, ABS Group offers comprehensive cyber security risk management solutions, capabilities and training for protection, defense, detection and response. The optimal time to consider implementing a robust cyber security program is now. You can request and explore the ABS' Cyber Security Toolkit today, just follow the link below.

https://www.abs-group.com/Knowledge-Center/Knowledge-Toolkits/Marine-and-Offshore-Cyber-Security-Toolkit/

SEE ARTICLE IN FULL:
https://www.abs-group.com/Knowledge-Center/Knowledge-Toolkits/Marine-and-Offshore-Cyber-Security-Toolkit/

1 Hour MCA Recognised & GCHQ Approved Training

Maritime Cyber Security Awareness Course (MCSA)

The ‘human factor’ is your biggest vulnerability to cyber crime.

Educate your workforce today to protect themselves and your organisation tomorrow.

- Easy access 1-hour online course
- Designed to complement current approaches to cyber security
- Suitable for all personnel – onboard and ashore
- MCA Recognised and GCHQ Approved

JWC INTERNATIONAL

For more information or to book, please visit us: www.maritimecybertraining.online

2021 MARITIME CYBER RULES ARE ALREADY OUTDATED, SAY CRITICS

With just under one year to go until the IMO's cyber-security guidelines are to be implemented, there are concerns that the guidelines will already be out of date.

The problems are several-fold, starting with the simple issue of time and technological advancements. Drawn up in 2016, the addition of cyber-related guidance to the Safety of Life at Sea Treaty reflected the issues highlighted at the time and was, rightly, heralded as an important step forward in an industry that had yet to react fully to the growing threat of cyber-crime.

However, while the International Maritime Organisation had to allow time for their guidance to be absorbed and for organisations to implement them before making it an enforceable requirement, almost five years will have passed. In that time, new cyber-technologies have been developed and adopted widely by maritime businesses.

Tom Kellerman, chief cybersecurity officer at security firm Carbon Black Inc. and a former chief information security officer at the World Bank, outlined the gaps. "They don't address the modern cybersecurity exposures created by mobility, applications and the cloud," he told James Rundle of the Wall Street Journal. "The guidelines, drafted in 2016, single out the use of 'memory sticks', for instance, and don't mention the cloud or artificial-intelligence systems prevalent today."

Patchy guidance can open the door to varied interpretations and an uneven application of standards, particularly for shipowners who only act reactively to rulings, rather than proactively to problems.

Indeed, the guidance does not cover the potentially huge development that is autonomous shipping, although the IMO Safety Committee is set to review the status of such shipping. It cannot happen soon enough: the speed at which the maritime industry is waking up to the benefits of autonomous technologies means that companies are fast on their way to deploying vessels without human crew, with one of the first, Yara Birkeland operated by Yara International ASA, due to operate this year.

The pace of change is set by the technologies and the firms willing to use them, and so, ideally, it in turn should set the scale of security guidance required, and the pace of implementation for effective protection.

There are further concerns that the IMO's guidelines will not be rigorously enforced. There are 164 country signatories to the IMO Safety of Life at Sea Treaty, accounting for 99% of all commercial shipping, but the IMO is not the enforcer of its own rulings. Instead the signatory countries must ensure compliance, meaning that enforcement varies.

However, while enforceable rules and standards may be slow off the mark, they are nevertheless welcome and the 2021 additional guidance will be for many an important step towards cyber resilience. The problems highlighted by experts as above, are reflective of this particular digital era, and it will take time to respond fully to the new rate of change.

In the meantime, the most important takeaway is for businesses to be more proactive and to take ownership of their cyber-security. Regardless of standards and rules - customers, investors and the industry will not accept excuses should a preventable cyber-attack undermine your business.

https://www.maritime-executive.com/magazine/more-than-meets-the-eye-1

https://www.wsj.com/articles/maritime-cyber-rules-coming-in-2021-are-outdated-critics-say-11563442201

US COAST GUARD DETAILS MARITIME PHISHING ATTACK

In a security bulletin published before Christmas, details have emerged from the US Coast Guard concerning a ransomware infection that took down an unnamed maritime facility, believed to be a port authority, for over 30 days..

The 'Ryuk' ransomware was believed to be contained in an email sent to a maritime employee. "Once the embedded malicious link in the email was clicked by an employee, the ransomware allowed for a threat actor to access significant enterprise Information Technology (IT) network files, and encrypt them, preventing the facility's access to critical files," reported the agency.

This is a classic phishing scenario, and a nightmare one at that, as the virus was able to spread unchecked through the network, going so far as to impact "industrial control systems that monitor and control cargo transfer and encrypted files critical to process operations."

The US Coast Guard revealed the virus caused "a disruption of the entire corporate IT network (beyond the footprint of the facility), disruption of camera and physical access control systems, and loss of critial process control monitoring systems." What this means is that the virus interrupted the usage of cameras and door-access control systems – a worrying development for further security risk.

The message from this phishing event must be to be ever vigilant, to ensure your employees at every level are confident in knowing what they are looking for, have clear protocols to follow and that they understand the ramifications if they don't. Organisations should closely examine their IT systems, limiting employee exposure to possible threats and limiting the pathway of a virus should they enter the network. As this incident demonstrates, your defences are only as strong as your weakest links, and they are most likely to the human element.

It seems highly likely that attacks like these will continue, if not increase, in the new decade and it is up to organisations to defend themselves and their employees robustly.

We would encourage anyone interested in starting the new year with a cyber awareness refresher to explore the resources on the Be Cyber Aware At Sea website. From a series of eye-catching posters, to these newsletters and further reading, it is all FREE to download and use.

Read more here: https://www.globenewswire.com/news-release/2019/10/15/1929891/0/en/ABS-Group-and-Atos-collaborate-to-deliver-first-end-to-end-IT-OT-cybersecurity-solution-for-global-marine-and-offshore-operations.html

PHISH & SHIPS

TYPE APPROVAL-FREE CYBER SECURITY FOR TANKER AND TERMINAL OT

A new product allows owners of oil and gas tankers and terminals to swiftly secure their critical systems from cyber threats without requiring type approvals.

As reported by Martyn Wingrove, Israeli cyber security firm Naval Dome has introduced software-based cyber protection for operational technology (OT) on ships, ports and offshore installations.

The security can be installed on navigation and cargo handling equipment and on machinery control systems and comes in two formats. S-Marine Dome was developed to secure ship bridge systems, engine room and propulsion control devices from online threats while S-Port Dome offers cyber protection for port, terminal and offshore energy infrastructure operators.

These software products can be installed without ship and port operators having to go through lengthy type-approval processes and without needing upgrades from system suppliers.

Naval Dome vice president for business development Ido Ben Moshe explained the products are streamlined versions of the company's T-Marine and T-Port security solutions that already have security level 4 (SL4) certification from classification society DNV GL.

T-Marine products were developed primarily for installation by original equipment manufacturers.

"We introduced the S-Model to provide an easy-to-install, level 2 security solution to offer an immediate remedy to the cyber problem," said Mr Moshe.

"Until now, there has been little by way of an effective software solution with which operators can use to immediately protect their systems," he said. "The S-Model fills that void."

S-Marine and S-Port can be installed on legacy OT and IoT systems or newer systems awaiting upgrade to provide improved cyber protection.

They are compatible with classification society SL2 requirements and all OT systems using computer operating systems.

They block unauthorised network intrusions and executable files from running on the computer inside OT and IT. Only approved, valid files can run on the computer and there is an 'endpoint' security event logger to defend systems against denial-of-service, ransomware, zero-day and malware attacks.

> **" We introduced the S-Model to provide an easy-to-install, level 2 security solution to offer an immediate remedy to the cyber problem "**
>
> **- Mr Moshe., VP for business development at Naval Dome**

https://www.rivieramm.com/news-content-hub/news-content-hub/secure-tanker-and-terminal-ot-without-the-hassle-56873

BE CYBER AWARE AT SEA

TURN OFF AUTO CONNECT WHEN DEVICES ARE NOT IN USE

Disable features like Bluetooth connectivity. If left on, nearby assailants can connect to your device and potentially hack into it.