BE CYBER AWARE AT SEA

Kindly sponsored by

AXIS

#36 / NOVEMBER 2019

PHISH & SHIPS

AXIS ON 'THE END OF SILENT CYBER'

GET AHEAD OF THE HACKERS!

SHIPPING INDUSTRY TO PREPARE FOR A YEAR OF CHANGE

FROM THE EDITOR

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

There is almost one year to go until the IMO's ISM Code alterations come to effect, incorporating cyber security into Safety Management Systems. So far it feels as if the regulation changes are having the desired effect, propelling the industry to re-evaluate security measures and available solutions.

For example, we welcome the news of ABS and Atos' collaboration to provide full IT to OT protection. That businesses are coming together to bring more cybersecurity solutions to the industry is a great step forward.

However, we are also pleased to note that the human element is still front and centre in the fight against cyber criminals and we were delighted to read Mike McNally's advice outlining how employees should approach their emails. We would also like to highlight our website, full of FREE resources, including posters and guidance which is there for the benefit of everyone.

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

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

THE END OF SILENT CYBER

BE CYBER AWARE AT SEA

Kindly sponsored by AXIS

As we move towards 2021, the level of cyber awareness amongst the maritime community is increasing rapidly. There has been a marked change in attitude over the last few years, particularly since the well-publicised Maersk cyber-attack of 2017, which was a wakeup call to an industry who often thought cyber was a problem that might disappear.

We all now know that there are many more incidents occurring in this sector than are reported and that the underreporting of cyber crime is leading to a false sense of security (see page six of the September edition of Phish and Ships). To illustrate this, BIMCO offered seven examples of verified cyber incidents that have occurred onboard vessels within their guidelines to highlight a few of the problems shipowners have faced to date (see version 3.0 of the Guidelines on Cyber Security onboard ships). With anonymous reporting platforms such as the CSO Alliance, it will not be long before we start to understand the true scale of the problem.

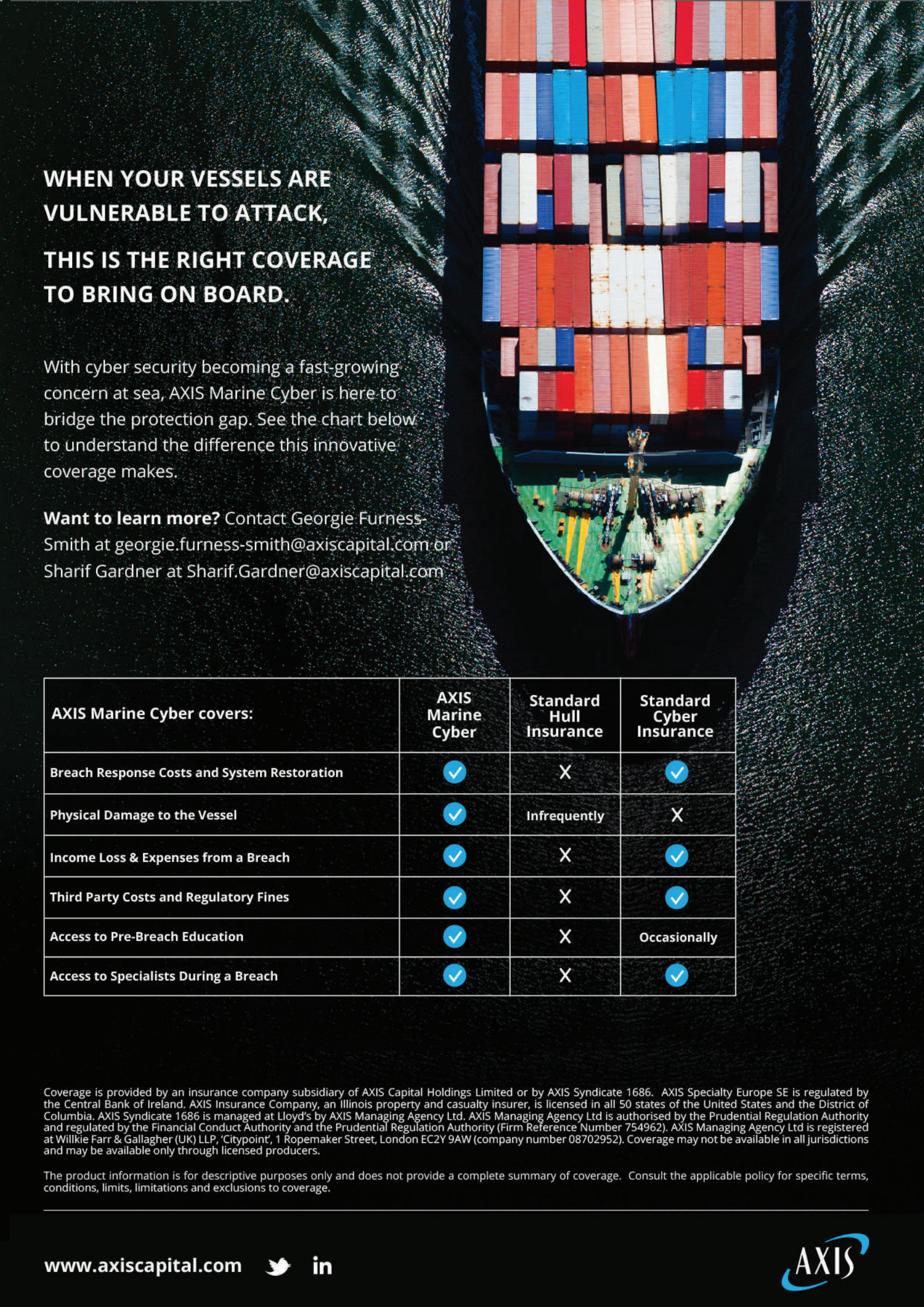
It is now a widely accepted view that the industry has moved from an 'if-it-happens' to a 'when-it-happens' approach, which means the demand for insurance to provide certainty around cyber coverage has intensified. Shipowners are becoming increasingly dissatisfied that their Hull and Machinery (H&M) insurance policies are excluding physical damage to their vessels caused by cyber, due to the CL380 exclusion. Occasionally, where no CL380 exclusion exists on the policy, shipowners face the uncertainty of "silent cyber" – no affirmative cover is given, but cover is not specifically excluded, either. So, shipowners are crossing their fingers and hoping that either their insurers decide to pay, despite cyber not being included as a peril, or that a court would rule in their favor should their vessel have an incident caused by cyber. This lack of certainty is something that Lloyd's of London and the Prudential Regulation Authority (PRA) have now addressed.

From 1st January 2020, Lloyd's will require insurers to provide certainty on whether cyber coverage is provided. This means that it must be absolutely excluded from H&M policies or affirmatively included. No more silent cyber! This removes the ambiguity that currently exists about cyber and ensures that insureds know exactly what is covered.

When the new Lloyd's rules come in to force, shipowners have several options if they are concerned about their exposure to cyber perils. If cyber is excluded from their H&M policies, cyber coverage can be bought from various specialist insurance providers. If cyber is included in their H&M policies, shipowners still have several concerns to think about. Is the cover sub-limited? Is loss of hire covered after a cyber event? What happens if a vessel cannot navigate due to a cyber event causing loss of income i.e. business interruption costs? Is the cover for malicious attacks only? What if the corporate network is affected – would that be covered? What happens in the event of a cyber incident/breach – are there breach response services who will know how to respond? All of these scenarios are insurable, but cover is unlikely to be available under a standard H&M policy.

To purchase cover for concerns such as those listed above, you will need a standalone maritime cyber policy which can cover everything from breach response, business interruption, loss of hire, physical damage to vessels, system restoration and more. If this is an area of concern for you, your insurance broker should be able to advise.

Article by Georgie Furness-Smith - Cyber insurance underwriter at Axis



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	✓

PREPARE FOR A YEAR OF CHANGE

NAVIGATION, COMMUNICATIONS AND DIGITALISATION

Cyber security plans will be finalised and IMO will modernise safety communications and e-navigation in 2020.

It is a busy year for maritime regulation in navigation, communications and digitalisation with important deadlines approaching. Top of the agenda for ship-owners and managers is implementing cyber security as ships become better connected and further integrated into corporate IT networks.

On 31 December 2019, there will be just one year before changes to Safety Management Systems to incorporate cyber security are implemented, as required under alterations to IMO's ISM Code.

Owners need to implement cyber security not just to comply with IMO regulations, which come into force on 1 January 2021, but to ensure their assets, IT and operational technology is protected from rising cyber threats.

During 2020, many shipping companies will assess their risk exposure and develop IT policies to include in their Safety Management Systems to mitigate cyber threats.

2020 also kicks off with one of the most influential IMO regulatory meetings for ship safety communications and voyage execution.

IMO's Sub-Committee on Navigation, Communications and Search and Rescue (NCSR) meets on 13-24 January to discuss progress on modernising the Global Maritime Distress and Safety System (GMDSS) and performance standards for navigational and communication equipment.

NCSR will receive updates on implementing alternatives to, and upgrading Inmarsat's existing GMDSS service. Work will progress on implementing IMO's e-navigation strategy with input from the latest testbeds and smart navigation technology developments. This sub-committee will analyse feedback from joint working groups on harmonising aeronautical and maritime search and rescue, and from International Telecommunications Union's group on maritime radio-communications matters.

NCSR will also review changes to ship routeing and reporting, requirements of the long-range identification and tracking (LRIT) system and standards for navigation systems for polar operations.

Progress should also be made on developing regulations covering testing and operating maritime autonomous surface ships (MASS). NCSR's recommendations will be reviewed by IMO's Maritime Safety Committee, which will meet on 11-22 May.

One of the first tests for MASS will come in September 2020 when Mayflower Autonomous Ship attempts the world's first unmanned transatlantic crossing from the UK to Plymouth in the US. To achieve this, artificial intelligence, edge computing and voyage planning software will be combined for safe navigation and hazard avoidance.

In the meantime, ship operators are implementing digitalisation, smart navigation and advanced analytics to optimise ship operations to reduce fuel consumption and emissions.

PHISH & SHIPS

MARITIME MEETS CYBER SECURITY

As of October 2019, to the best of my knowledge, there has not been a single, dedicated hacking attack against a vessel at sea by malicious actors. While there have been rumors – specifically one from an American telco provider in 2016 – that hackers have teamed up with pirates to track high value cargoes, there has been no firm evidence.

Equally, the dire warnings from some quarters of ships having their navigation systems hacked so they can be directed to ports where pirates or criminal gangs could then ransack them have so far proven to be little more than interesting worst-case scenarios. Once you begin to dig in to the logistics of such a criminal enterprise, it quickly falls apart. After all, it requires the use of a pirate-friendly port or harbor deep enough to accommodate the hijacked vessel as well as a significant number of personnel to offload cargoes, crew and so on.

What has been noted in the maritime domain, however, is a rise in spear-phishing of vessels at sea. The maritime domain has seen malware introduced into ship systems by crew and third party providers by accident. While these incidents have been, in some cases, hugely expensive to put right – any delay to a vessel costs money – they have so far fallen short of the scare stories suggested by some parties.

This is not to dismiss or minimize the threat of an actual, focused attack by an Advanced Persistent Threat (APT) group on a shipping line or vessel. It could happen. Indeed, it probably will. But it hasn't happened yet for a number of reasons, the main one being, Why? Why attack a ship? If we assume that most cyber attackers are criminal rather than terrorist or hacktivist, then the motives for attacking a ship at sea begin to fall away; there simply isn't any profit in it, and return on investment is important to cyber criminals. It's like mugging a bank teller rather than emptying the cash drawer.

Vulnerabilities on board vessels exist, and often nobody knows anything about them. A recent investigation by Pen Test Partners noted that, unknown systems can be prevalent on board ships. "In every single [nautical pen] test to date we have unearthed a system or device, that of the few crew that were aware, no one could tell us what it is was for," said Andrew Tierney, researcher with Pen Test Partners, writing in a blog on October 14. "In other scenarios an undocumented system or device would be considered a malicious implant. In maritime cyber security it's business as usual."

In one case, a monitoring system was uncovered whose purpose was not known – although it was connected to the main engine. Fleet management had no record of its purchase or installation; all hardware was unlabeled. It had been installed by a third party with whom a commercial arrangement had stopped several years ago, Tierney said in an article by Threat Post.

While cyber risks on the water remain a concern, the ongoing, real threat is and will always be found at a company's head office. How a company deals with that will decide what an attacker does next. Outside the realm of hacktivism, criminals are looking for a payday, and that means they're going to be looking for any vulnerability which can give them access to company finances.

In the last few years, I've seen numerous reports of highly specific and convincing email fraud attempts against shipping companies, ports and ship brokers. In several instances, the hackers have infiltrated a company's systems and then sat dormant, often for months, waiting for their opening. In one case, this involved sending spoofed emails to a client and redirecting payment of hundreds of thousands of pounds to the hacker's bank accounts. Fortunately, thanks to quick-thinking staff, the fraud was discovered and the banks and police were able to stop the transfers. But this isn't always the case.

Directed attacks remain a significant threat to any company, regardless of the business sector, and maritime is no different. Shipping has so far managed to avoid the headline-grabbing attacks such as the $4.2 million stolen from an Oklahoma pension fund, or the $47 million initially stolen from networking firm, Ubiquiti in 2016, but the sector remains highly exposed.

David Rider is a consultant who has worked with leading maritime security firms since 2009 as an intelligence analyst, working in both the maritime and cyber sectors. He maintains the blog maritimesecurity.news.blog in his spare time.

https://maritime-executive.com/blog/maritime-meets-cyber-security

GET AHEAD OF THE HACKERS!

CYBER SECURITY EXPERTS ADVISE SHIPPING COMPANIES TO TRAIN STAFF TO IDENTIFY FAKE EMAILS AND ENSURE THEY ARE READY FOR IMO 2021 CHANGES

Shipowners, managers and operators have just over a year before their fleets need to comply with IMO's ISM Code from 1 January 2021.

Many shipping companies are already assessing their exposure to risk and developing IT policies to include in their Safety Management Systems aimed at mitigating it. But many companies will not be prepared for IMO 2021, and even more will not be aware of the ease with which cyber criminals can access passwords and use emails to penetrate maritime companies.

CHECK OUT THIS EMAIL SECURITY CHECKLIST . . .

A checklist for all personnel involved in maritime on what to question and check from emails, from GT Maritime director Mike McNally.

Question unusual requests
Be alert to suspicious instructions from high-level executives – especially those involving financial transfers. If in any doubt, contact managers to verify requests. Do not hit reply. Do start a new email chain.

Do not follow suspect links
There is no fool-proof way to tell whether an email is genuine. It is better to err on the side of caution and not click on any links.

Check the email sender and URL
Check whether the sender's domain (detailed after the @ sign in the email address) matches the claimed source of the email. Fraudsters deliberately use incorrect spellings of legitimate domains in the hope of evading detection.

Check links lead to where they are supposed to
Hovering a mouse over a link will reveal its destination URL. If the link bears no relation to the claimed destination, do not click.

Check for a personal salutation
Legitimate senders will usually address their customer by name, while phishing attempts will likely to use a generic greeting.

Take time to review the email
To encourage a hasty response, phishing emails often include time sensitive requests. Make time to review all emails to ensure they are genuine before acting on any request.

Do not give out personal or sensitive information
Be wary of emails requesting account details or other sensitive information. Contact the sender in another way to confirm the legitimacy of their request.

Check the design and quality
Phishing emails often contain poor spelling and grammar, or incorrectly reproduce graphics stolen from the claimed source.

Ask for help
If you receive a suspected phishing email, forward to your IT department.

SEE ARTICLE IN FULL:

https://www.rivieramm.com/news-content-hub/news-content-hub/getting-ahead-of-the-hackers-56466

CYBER HACK: FORTIFYING MARITIME, PORT SECURITY

The United States Coast Guard Marine Safety Alert 06-19 (USCG MSA 06-19) outlines a February 2019 incident aboard a deep draft commercial vessel that called on the Port of New York / New Jersey after experiencing a significant cyber incident that impacted their shipboard network.

The Safety Alert stated in part:
"An interagency team of cyber experts, led by the Coast Guard, responded and conducted an analysis of the vessel's network and essential control systems. The team concluded that although the malware significantly degraded the functionality of the onboard computer system, essential vessel control systems had not been impacted. Nevertheless, the interagency response found that the vessel was operating without effective cybersecurity measures in place, exposing critical vessel control systems to significant vulnerabilities."

This incident provides valuable guidance on how we should evaluate the security readiness of terminals, vessels and associated infrastructure. It also highlights the importance of how security drills and crew training should be developed and conducted. A key take away is that the Coast Guard strongly encourages all vessel and facility owners and operators to conduct cybersecurity assessments to better understand the extent of their cyber vulnerabilities. This needs to be a vessel and facility specific review as each asset can have unique exposures.

The good news is that there are very good free assets available to help conduct this review. The Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA) website provides cybersecurity resources and best practices for businesses. One resource that should be studied is the Cyber Resilience Review (CRR). The CCR Self-Assessment provides a measure of an organization's cyber resilience capabilities and provides a helpful User's Guide that provides information on conducting self-assessments, evaluating cyber resilience capabilities and providing guidance for follow-on activities. In the UK, the NCSC has some excellent resources on cyber safety and there's other maritime publications, such as the BIMCO guidelines and of course, the Be Cyber Aware at Sea campaign!

All employees have a role in cybersecurity and cyber is a critical component of overall physical security. ID cards and swipe cards are in regular use for facility access and these are just a few of the many operational systems that can be compromised in a cyber incident. Training needs to start with new hires and include all employees. As with any business plan, it is critical that upper management be invested in the success of operational security. It is also important to solicit and respond to rank and file input. The best procedures are those that are developed with robust involvement and communication, as well as being subject to regular review and evaluation. A procedure should not just look good on paper; it also needs to be functional and address a real need.

In 2017, the International Maritime Organization (IMO) adopted its Maritime Cyber Risk Management in Safety Management Systems resolution, which requires ship owners and managers to incorporate cyber risk management into ship safety by 2021. However, this is a current threat that needs to be acted on now, not put off until the regulations go into effect. While new technology and the Internet of Things have introduced many new exposures and threats, in many ways current security training reflects the same goals and objectives we had when steaming in piracy waters in the 1980's; present a hard target and have a plan that can survive a punch in the mouth.

https://www.marinelink.com/news/cyber-hack-fortifying-maritime-port-471724

ABS AND ATOS COLLABORATING TO IMPROVE CONTROL OF CYBER RISKS

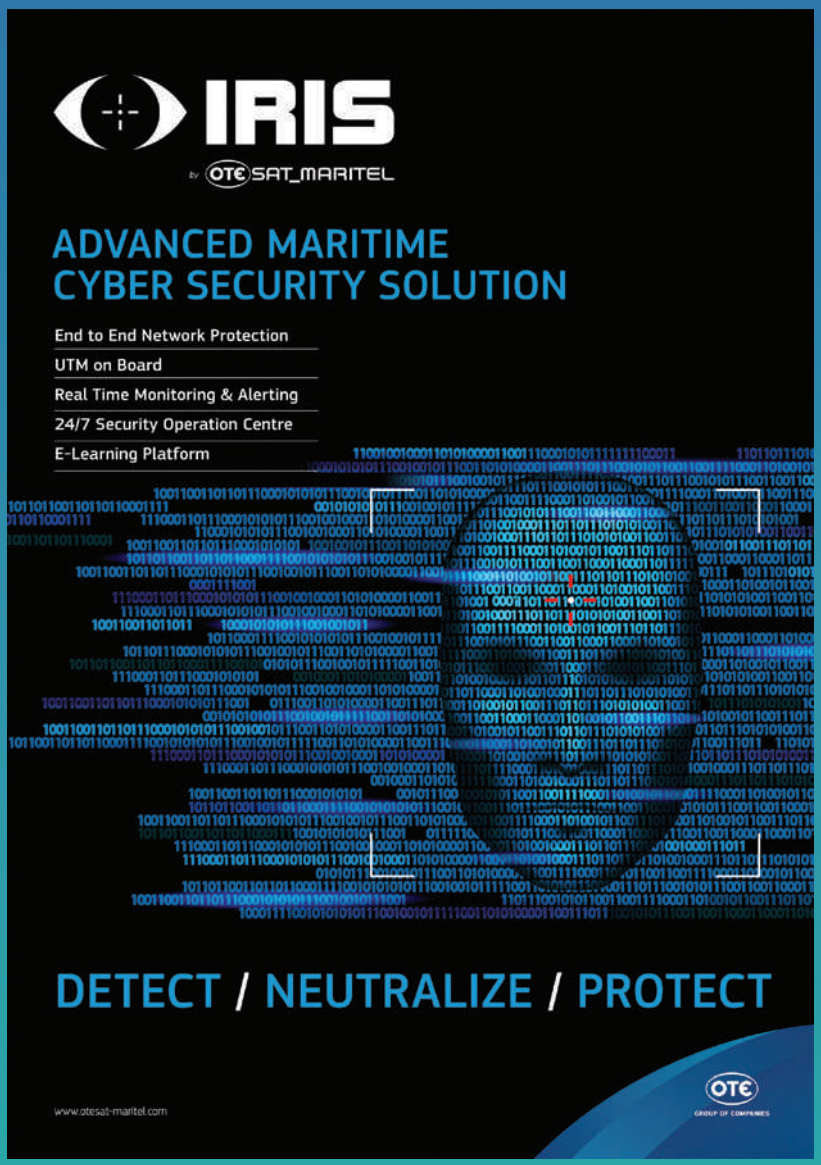
It was announced this month that ABS Group and Atos are planning to provide the industry's first full-service Information Technology (IT) and Operational Technology (OT) cybersecurity solution to reduce cyber risk across the global marine and offshore energy supply chain.

This comprehensive solution supports implementing cybersecurity at the earliest stages of asset design and development, making cyber risk management a consistent and integral part of operations from the beginning.

"Cyber security is the new frontier in marine and offshore safety," commented Ian Bramson, Global Head of Cybersecurity at ABS Group. "As these assets become more digital, the industry must be ready to deal with a broader range of threats. Atos is a digital transformation leader in cloud-based cybersecurity and high-performance computing. Working together, we are able to deliver a converged IT/OT solution for safer, more secure assets and operations."

"Historically, OT and IT acted as stand-alone systems in the maritime industry. Uniting Atos' established cybersecurity expertise with ABS' marine and offshore operational expertise provides a new industry solution in securing both IT and OT assets, devices and networks," said Jerome Sandrini, Senior Vice President and Head of Big Data and Cybersecurity, Atos North America.

Be Cyber Aware At Sea welcome these developments – by working together the security service industry can truly assist maritime businesses to protect themselves from the substantial digital threats at large, particularly when combined with rigorous staff cyber-discipline and industry initiatives.



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

MPA TO STRENGTHEN CYBER COLLABORATION EFFORTS

To strengthen collaboration on cyber resilience and response amongst 15 port authorities, the Maritime and Port Authority of Singapore (MPA) tabled a proposal to form and lead a "Port Authorities Chief Information Officer (CIO) Cybersecurity Network" (PACC-Net) at the 5th edition of the Port Authorities Roundtable (PAR) 2019.

The proposed network will enhance cybersecurity awareness in the maritime sector and facilitate early sharing of cyber-attack information to counter cyber-attack threats.

Organized by the Port and Urban Projects Bureau of the Kobe City Government of Japan, with support from MPA as the Secretariat, the closed-door event brought together port authorities from major ports around the world. The objective is for members to network, share insights on pertinent issues and best practices, as well as to explore areas of collaboration.

With this year's PAR theme being "Managing Disruptive Changes and Risks for Future Ready Port", participants discussed how to respond to various challenges and risks related to ports and shipping, such as IMO emission regulations, smart technologies in enhancing port productivity, natural disasters and the threat of terrorism. Through mutual sharing of experience and knowledge, PAR sought to enhance the ability of each port to cope with these challenges and risks.

Two new participants joined this year's event held in Kobe, Japan, from October 15 to 17. Abu Dhabi Ports Group is the first Middle Eastern port to attend PAR, along with the Port of Seattle.

Ms Quah Ley Hoon, Chief Executive of MPA, said: "The exchange of best practices to address issues of common interests at the 5th Edition PAR2019@Kobe has enhanced the ability of each port to cope with the various challenges and risks it faces. With increasing interconnectedness and digitalization of the maritime sector, ports and shipping will also face greater vulnerabilities to cyber threats. We hope for PACC-Net to be established to further enhance collaboration amongst leading ports to mitigate against such threats."

"With increasing interconnectedness and digitalization of the maritime sector, ports and shipping will also face greater vulnerabilities to cyber threats."

- Ms Quah Ley Hoon, Chief Executive of MPA

https://www.maritimeprofessional.com/news/strengthen-cyber-collaboration-efforts-351744

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.

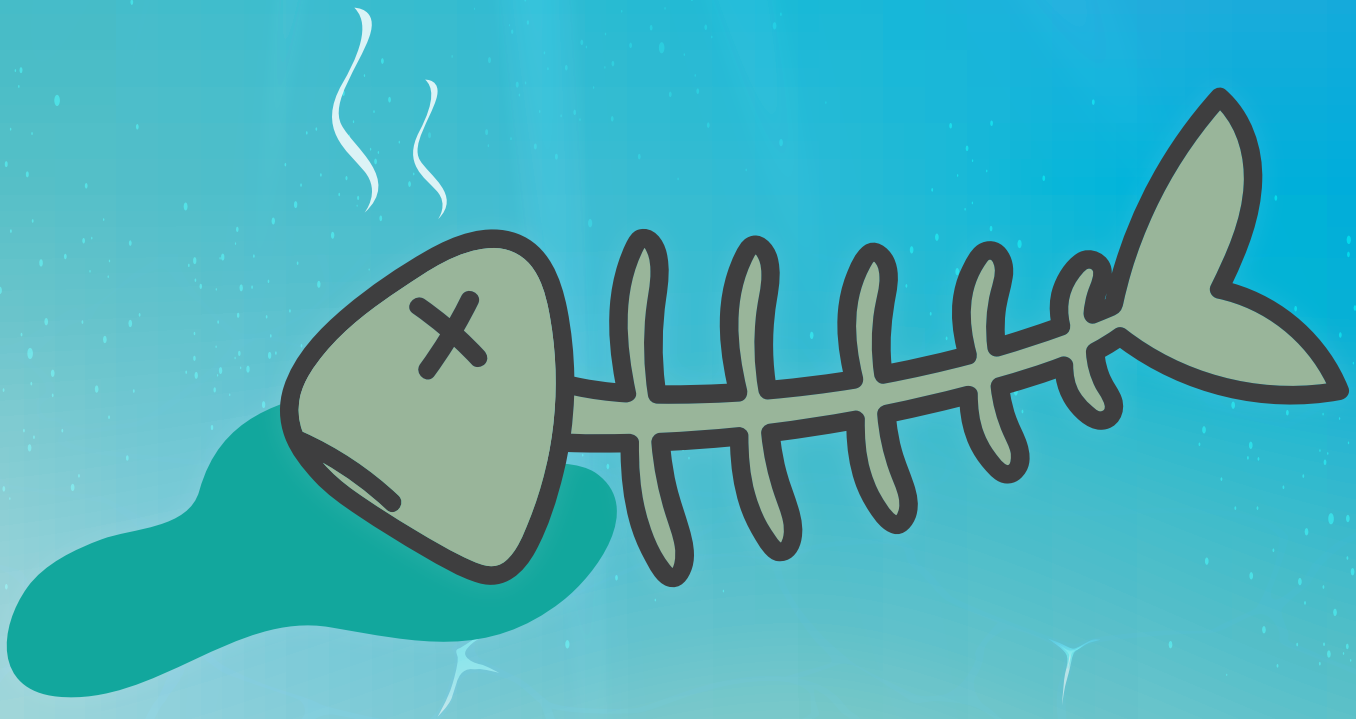
- Easy access 1-hour online course
- Designed to complement current approaches to cyber security
- Suitable for all personnel – onboard and ashore
- MCA Recognised and GCHQ Approved

JWC INTERNATIONAL

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

BE CYBER AWARE AT SEA

CHECK YOUR EMAIL, IS THERE SOMETHING PHISHY GOING ON?



Look out for misspellings and grammatical mistakes in Phishing emails. Be aware before clicking on an attachment or link, that may just stink!