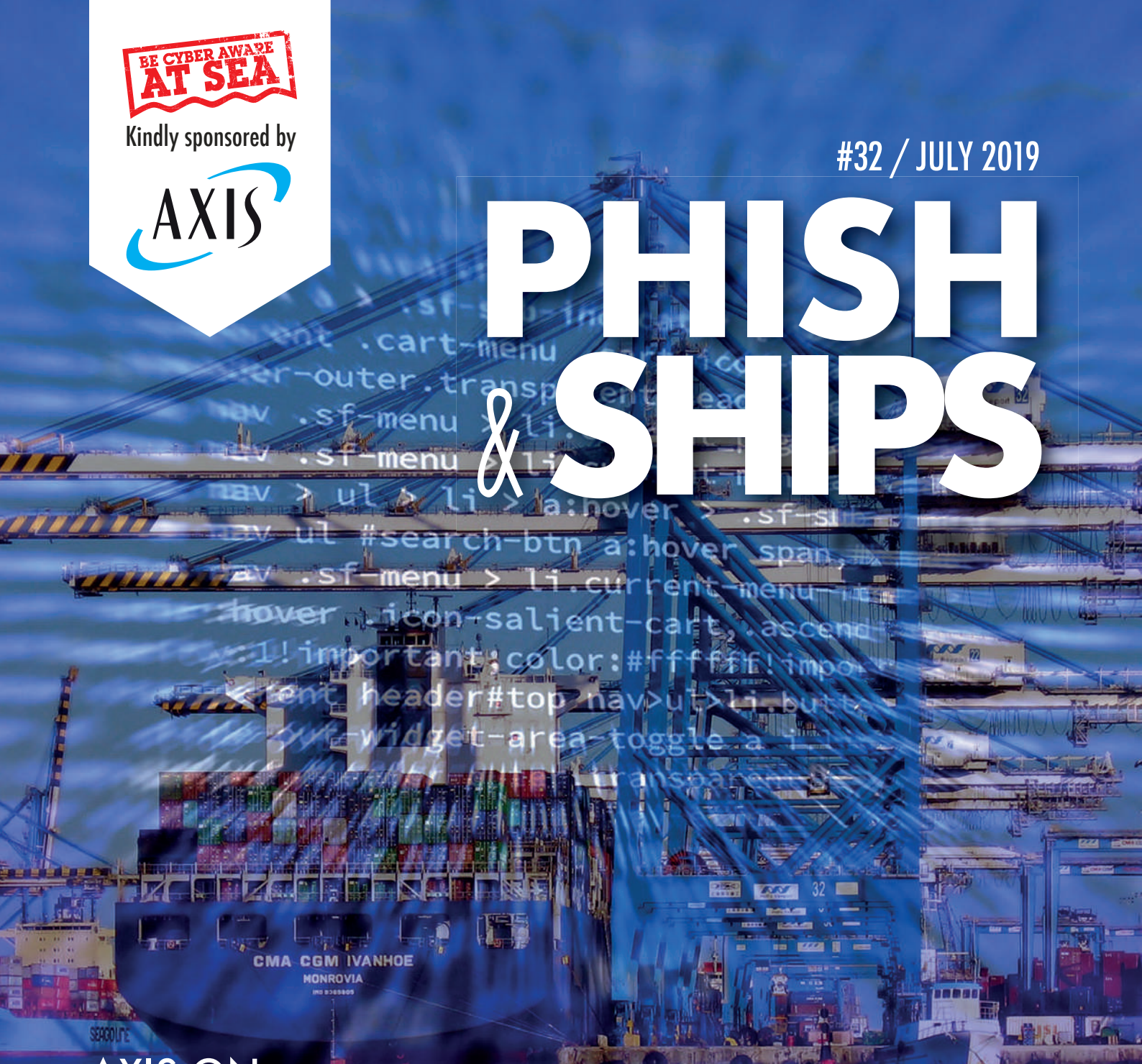
BE CYBER AWARE AT SEA

Kindly sponsored by

AXIS

#32 / JULY 2019

PHISH & SHIPS



AXIS ON UNDERREPORTING OF CYBER CRIME

KEY TAKEAWAYS FROM RECENT CYBER ATTACKS IN SHIPPING

CYBER RISK MANAGEMENT WHAT MARITIME PROFESSIONALS NEED TO KNOW NOW

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

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

It is unsettling times in our industry. The physical attacks in the Straits of Hormuz has turned the eyes of the world onto shipping and the geo-political tensions between Iran and the US. Donald Trump called off airstrikes due to the potential for mass casualties and instead turned his attention to deploying cyber-attacks. This shows the power of cyberspace, and whilst there isn't much many of us can do about state-on-state attacks, we must remain vigilant to the potential collateral damage that can arise from such attacks.

In an ever-increasing uncertain world, our thoughts are with the seafarers out on the ocean wave and we wish you all calm seas in every sense.

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

KEY TAKEAWAYS FROM RECENT CYBER ATTACKS IN SHIPPING

The ransomware attack on Norwegian industry giant Norsk Hydro in March this year, which forced the company to halt production in several plants and ended up costing them around USD 50 million, was yet another wake up call for the maritime industry.

What lessons can be learned from recent cyber attacks in shipping? First, here's a brief recap of three recent cases – the incidents involving Maersk, COSCO and Austal.

"When a company with Norsk Hydro's resources, expertise and systems is vulnerable to attack, then every company is, in every sector."

FROM DIGITAL INFANCY TO A HARSH NEW RISK REALITY

For the maritime industry, there has been a steep climb on the digital maturity ladder. IT used to be seen as an operational cost rather than as a strategic business approach. However, as ships have increasingly started using systems that rely on digitalisation, integration and automation, the associated risks and threats were historically not adequately factored in. Simply put, the industry wasn't digitally mature enough yet to safely navigate the rough waters of digitalisation.

Today, more and more ships, systems and networks are connected to the Internet, making them accessible from practically anywhere on Earth. At the same time, this makes ships much more vulnerable to cyber attacks, both targeted and random ones.

Increasing digital reliance has unlocked huge efficiencies and operational benefits, but it has also opened a Pandora's box of cyber threats – a risk reality that shipping needs to understand and navigate.

CYBERCRIME IS NO HYPE

Cyber risk has fast become the new normal for the maritime sector. According to the Allianz Risk Barometer 2018, cybercrime is considered one of the top five threats to the global maritime industry.

The past two years have seen a growing number of high-profile cyber attacks, making it clear that cyber attacks represent a real problem to be immediately and seriously addressed – and not just hype from vendors trying to sell cybersecurity products.

MAERSK

In June 2017, shipping giant Maersk was hit by a devastating cyber attack caused by the NotPetya malware, originating in Ukraine. Maersk was not targeted specifically, but was "collateral damage". The attack resulted in significant disruptions to Maersk's operations and terminals worldwide, costing them up to USD 300 million.

COSCO

In July 2018, COSCO Shipping Lines fell victim to a cyber attack that disrupted the company's internet connection within its offices in the Americas region. After a 5-day sprint to activate contingency plans, COSCO's operations were back to normal. Apparently, Cosco was aware of what happened to Maersk and had taken proactive steps to minimize their risk.

AUSTAL

In October 2018, Australia-based ferry and defense shipbuilder Austal was hit by a cyber attack that breached the company's data management systems. The attackers, believed to be Iranian hackers, managed to steal internal data and offered some of it for sale on the dark web in an apparent extortion attempt.

LESSONS LEARNED

Whether you call it disruption or revolution, digital is here to stay. The rapid implementation of IT systems and internet communication for ships in every part of the world brings new and exciting opportunities – but also cyber threats.

These are 4 key takeaways to keep top of mind...

1 Good IT hygiene is key to fighting cybercrime, but mindset is a big obstacle. There must be a shift in people's attitude towards IT security. IT is not something that is on the side; it is as important as the main office or the ship itself, if not more. Because if IT collapses, many parts of the business collapses.

2 Every shipping manager needs to approach cybersecurity as an integral part of the overall safety management. If disruptive cyber attacks can happen to some of the biggest players globally, it may well happen to you. This means you need to have an effective cybersecurity management plan in place to manage all possible threats. Response and recovery plans should be tested and updated frequently.

3 There is NO zero cyber risk environment today. You will never mitigate all risk, as new cyber threats and vulnerabilities are constantly emerging. But you can minimise it – by continually assessing risk exposure, understanding the impact, and then working to implement safeguards that will counter risk and help you steer clear of cyber attacks.

4 Despite all precautions, vulnerabilities still remain in your systems and networks – attackers are constantly finding new targets and refining the tools they use to break through cyberdefenses.

So perhaps the most important takeaway from cyber attacks in the maritime sector is this: Establish appropriate contingency plans for cyber incidents, including the loss of critical systems and the need to use alternative modes of operation. In the event of the worst happening, you can still operate.

BE CYBER AWARE AT SEA

Kindly sponsored by AXIS

UNDERREPORTING OF CYBER CRIME IS CREATING FALSE SENSE OF SECURITY

There is a significant gap between the number of cyber-related incidents that occur in the maritime industry and the lower number that are being reported. Underreporting is not surprising for a number of reasons – most notably, to broadcast one's business as a victim of a cyber event could lead to serious repercussions.

There are occasions when reporting is a lawful duty – for example, where customer data has been compromised. Yet, when companies are the target of other types of attacks, such as ransomware attacks, a company may not be required to, or want to, disclose the attack because they fear the consequences of negative publicity on their business.

Underreporting is a serious issue in the industry, and it provides a false sense of security. If a company only hears of the occasional cyber event within the maritime industry, such as the extreme stories of Maersk's $300m+ event, one may not understand how likely an attack actually is. This creates a sense of denial or wishful thinking, 'why would it be me?'.

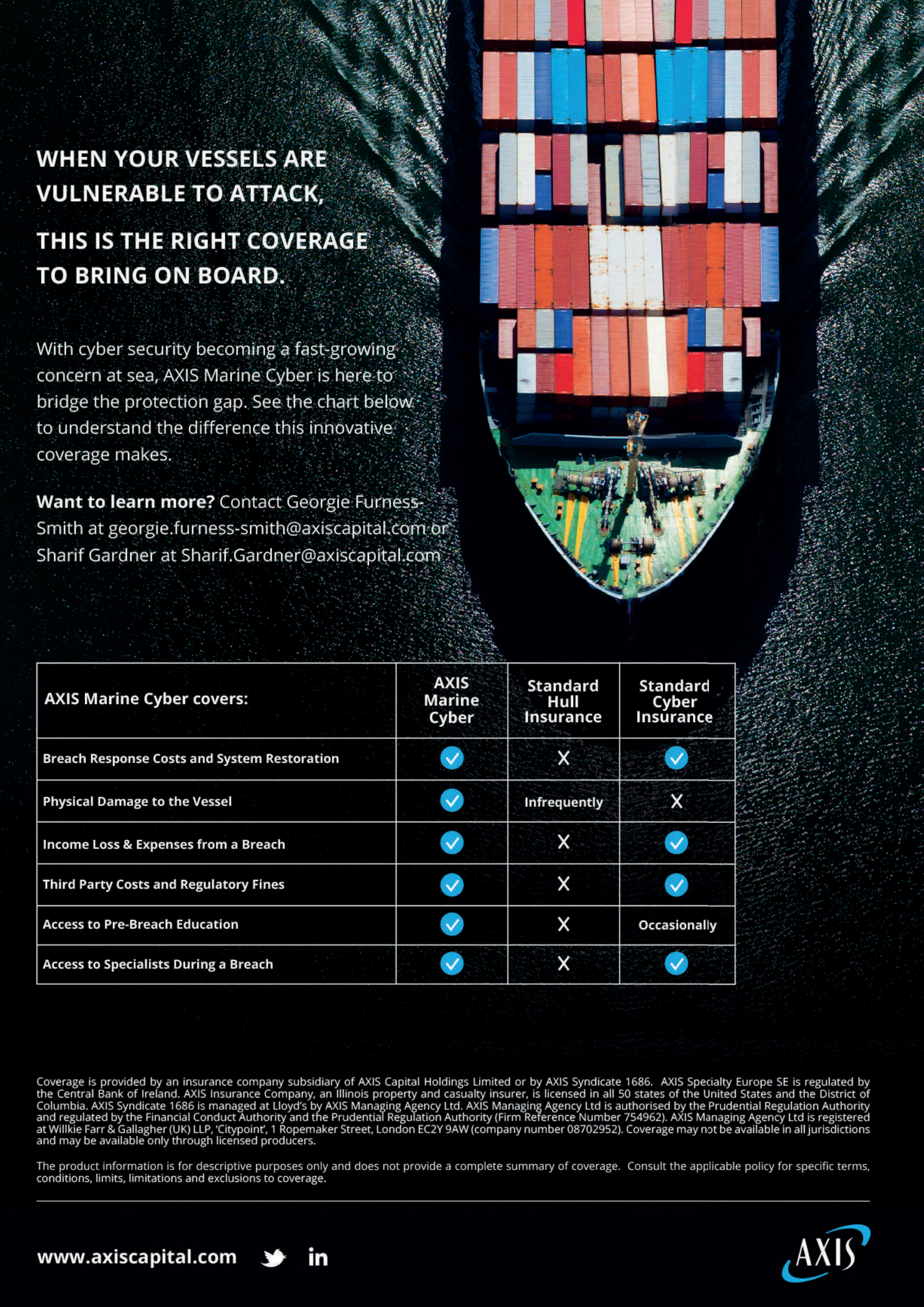
The CSO Alliance, a maritime-focused organization, has set up an anonymous reporting facility designed to help maritime companies report cyber incidents with absolute anonymity and confidentiality. This helps to alleviate the problem of underreporting and raises awareness of the scale of the issue. The more the industry can understand about the nature and volume of attacks, the easier it will be to raise awareness, increase preparedness and mitigate the risks.

The BIMCO guidelines which address the requirement to incorporate cyber risks into the ship's safety management system and provide guidance for dealing with supply chain risks come into effect in January 2020, and their new BIMCO Cyber Security Clause was launched in May 2019. BIMCO say the new clause was drafted 'in the wake of recent costly security incidents' and 'requires the parties to implement cyber security procedures and systems, to help reduce the risk of an incident and mitigate the consequences should a security breach occur'. BIMCO's efforts have considerably increased awareness within the industry, but as no major incident involving a vessel has been reported to date, there is still a level of complacency by many within the industry, despite the number of events impacting the shipping industry increasing. The facts need to be seen to be believed, and for the scale of the problem to be clearly identified, reporting, anonymous or otherwise, is vital.

With the first commercial autonomous vessel to cross the North Sea completing a cargo run in May, the opportunities for cyber criminals to cause chaos are expanding as vessels become increasingly connected. The US Coastguard released a bulletin in May warning shipowners to verify email addresses after several phishing emails were used to gain sensitive information from commercial vessels, posing as official Port State Control authorities. They also added that they had received reports of 'malicious software designed to disrupt shipboard computer systems. This highlights the importance of remembering that maritime companies need to pay equal attention to their onshore business networks, which have been the focus of the reported attacks to date, as they should to their offshore assets. A breach of a corporate network can result in business interruption, critical data loss and complicated IT problems, which can have a huge economic impact.

The scenario of cyber criminals being able to take control of a vessel to cause unpresented harm both physically and economically might seem like a doomsday event, but imagine if an event like this had already happened, but had not been reported? Anonymous reporting is vital to allow the shipping community the ability to clearly understand with tangible data what is happening within the industry so that thorough and educated risk management strategies can be deployed.

Author
Georgie Furness-Smith
Cyber Insurance Underwriter
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	✓

US CARRIED OUT CYBER ATTACKS ON IRANIAN ASSETS

Donald Trump called off a military strike on undisclosed Iranian assets this week after reports Iran's Revolutionary Guard shot down a RQ-4A Global Hawk surveillance drone, the incident itself following accusations of Iranian responsibility for attacks on oil tankers in the Gulf of Oman. But U.S. Cyber Command launched a retaliatory cyber attack on "an Iranian spy group that supported last week's limpet mine attacks on commercial ships," Yahoo News reported on Friday.

The Yahoo News report was light on details and sourced from "two former intelligence officials," but does state that the targeted organization has "ties" to the Revolutionary Guards and has some role tracking the flow of shipping through the Strait of Hormuz (which links the Persian Gulf to the Gulf of Oman and thus the Indian Ocean):

The group, which has ties to the Iranian Revolutionary Guard Corps, has over the past several years digitally tracked and targeted military and civilian ships passing through the economically important Strait of Hormuz, through which pass 17.4 million barrels of oil per day. Those capabilities, which have advanced over time, enabled attacks on vessels in the region for several years.

Though sources declined to provide any further details of the retaliatory cyber operation, the response highlights how the Persian Gulf has become a staging ground for escalating digital — as well as conventional — conflict, with both the United States and Iran trying to get the upper hand with cyber capabilities.

According to Bloomberg, abundant skepticism that the Trump administration was telling the truth about Iran involvement in the tanker attacks has waned somewhat. However, it is clear that if Iranian assets did carry out the attacks, it is much more likely they intended to send a signal about their ability to disrupt shipping in the region than start a war.

Analysts from US based security firms have confirmed an increase in Iranian state-sponsored attacks hacking attempts, largely against companies in the oil and gas industry.

It is so important that crew of vessels and shore based operations understand the risks they face in this space. This type of posturing between nations will likely spill over into the cyber domain within shipping. The industry is not immune from this threat and training up crew and employees is one of the most effective ways of introducing malware into any systems. The Be Cyber Aware at Sea crew will continue to raise awareness and in direct response to this, the monthly awareness poster is on Spear Phishing!

https://gizmodo.com/report-us-carried-out-cyber-attacks-on-iranian-assets-1835764177

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

FAX MACHINES MAKE A COMEBACK AT NORSK HYDRO FOLLOWING RANSOMWARE ATTACK

LockerGoga ransomware attack in March saw a return to pen-and paper drawings and fax communications between offices.

Aluminium producer Norsk Hydro has revealed that it has had to resort to the use of pen and paper to continue business following a ransomware attack in March.

According to a report by the BBC, "five weeks on, they're still recovering" and have had to dig out "long-since forgotten about paperwork". It was also revealed that workers have been "forced to use pen and paper".

Norsk Hydro is one of the leading manufacturers of aluminium, with 35,000 employees in 40 countries in every continent. The company serves over 30,000 customers worldwide.

On March 19th Norsk Hydro suffered a major attack on its network, which forced it to shut down or otherwise limit its use of technology for production of materials.

The attackers who delivered the ransomware demanded payment in return for full restoration of the company's services. It also resulted in a temporary shutdown of the company's website and updates on the situation had to be posted onto the company's social media pages.

Norsk Hydro is not alone in being attacked by this new variant of ransomware known as LockerGoga. France-based Altran Technologies in was also attacked in January. Both attacks have had catastrophic consequences for production and for profit. The total cost of the cyber-attack on Norsk Hydro was revealed to be $52 million.

The attack appears to have had a financial motive rather than an act of hacktivism. The Norway-based company is still trying to overcome damage and has had to turn to manual operations to prevent further damage to production. In the UK the customer service team has been taking orders via fax, WhatsApp and Facebook, while the network is repaired, with the technical department creating hand-drawn plans and diagrams.

The attack has led to long-term, extensive co-operation between Norsk Hydro's global premises in an effort to neutralise the extensive damage dealt by the individuals responsible and many fixes have and are being implemented and executive vice president of Hydro Extruded Solutions Egil Hogna stated: "we are getting very close to our normal output".

For the shipping industry, it is cases like this that should refocus the mind on prioritising the protection of IT systems. The firewalls and anti-virus may work when configured correctly, but when things go wrong – and they do – organisations need to respond very quickly and recover. Quite simply, there are shipping companies out there who could fold if they were hit with this loss. Insurance can help, but are shipping companies prepared to pay for it?

https://www.computing.co.uk/ctg/news/3077830/fax-machines-make-a-comeback-at-norsk-hydro-following-ransomware-attack

CYBER RISK MANAGEMENT

WHAT MARITIME PROFESSIONALS NEED TO KNOW NOW

The IMO January 2021 deadline for shipping interests to incorporate cyber risk management into their existing Safety Management Systems is fast approaching. It is critical that stakeholders understand their vulnerabilities.

The IMO has issued MSC-FAL.1/Circ.3 guidelines on maritime cyber risk management that does a good job of outlining the many vulnerable systems within marine operations, including:

1. **Bridge systems**
2. Cargo handling and manage ment systems
3. **Propulsion and machinery management and power control systems**
4. Access control systems
5. **Passenger servicing and management systems**
6. Passenger facing public networks
7. **Administrative and crew welfare systems**
8. Communication systems

The IMO Guidelines also raise an important point on understanding the distinction between information technology (IT) and operational technology system (OT). In short, IT focuses on the use of data as information while OT focuses on the use of data to control or monitor physical processes.

These distinctions become important when it comes time to conduct a risk assessment of your operations.

Risk assessments should be the first step when examining your company, terminal or vessel's cyber exposure. All parts of your business that are controlled or supported by computer systems need to be identified, and there are likely more than you realise.

Often we are faced with unique risks in the maritime field, and while the cyber threat at sea does have some unique characteristics, most threats are the same as those faced by shore-side enterprises. The cyber threat does not care if you are in port or at sea. As long as you are connected to the internet, you are at risk.

The Be Cyber Aware at Sea campaign has numerous awareness material, guidance and other resources that help educate crews and shore-side staff to help protect themselves, the companies they work for and the industry as a whole.

Preparations to prevent or minimise a cyber incident are your first line of defence, however, companies still need to have a response plan in place that outlines how to respond when a cyber incident occurs. An important part of this plan is to working with your Insurance Broker and Underwriters to understand how to properly manage your risk with adequate insurance coverage.

The key here is to identify what is and is not presently covered. The big unknowns are so-called "silent" cyber exposures in most traditional insurance policies, which were designed when cyber was not yet a major risk and do not explicitly consider it. This can create uncertainty for businesses, brokers and insurers about which loss scenarios are covered. Insurers are working hard to remove the uncertainty of coverage for their business customers.

Cyber security is a race without a finish. The IMO has given the maritime industry a deadline to get their cyber risk practices in order by January 2021. It is clear that the work will not end there. Cyber threats will continue to evolve in frequency and severity as we become more reliant on the technology. The Technology will be a positive for both increasing vessel safety and reducing risk, however, it requires staying vigilant for new and emerging threats. This vigilance is essential for the future of the industry because complacency is not an option.

THREE CORNERSTONES FOR EFFECTIVE CYBER SECURITY

Speaking recently at Lloyd's Register Asia Shipowners' Forum, Wallem Group chief executive Frank Coles highlighted how operators can fail to update critical processes when embracing new onboard technologies. By overlooking the human elements of cyber security, he said, operators can undermine the potential benefits of acquiring a new technology – introducing risk instead capitalising on the rewards it can offer. While cyber security risks posed to the shipping sector are real and pressing, they can be quantified and managed, if the right approach is taken. Safeguarding critical assets in a fragmented digitalisation process and ensuring profitability in the years to come depends on three cornerstones:

CORNERSTONE 1:
THREAT-INTELLIGENCE ASSESSMENT

The cyber security landscape is rapidly changing and the insights gained as little as five years ago are of less and less value as threat actors adjust their approaches in response to advances made by security professionals and technical defenders. Regular threat intelligence and assessment activities allow an owner to view their organisation through the eyes of a potential attacker, to perceive their attack surface in detail, and to assess the real-world threats to their business.

CORNERSTONE 2:
CRISIS-MANAGEMENT CYBER ATTACK SIMULATION

With knowledge of the attack surface and adversaries already in hand, owners can take steps to safely, effectively and efficiently ensure they are prepared to respond to a cyber attack by using a simulated cyber attack known as a 'red team' exercise. Such exercises allow a company to define and simulate real-world attack scenarios using the same tactics, techniques, and procedures as a genuine threat actor. They also help determine the level of assurance and ability needed to effectively detect and respond to a genuine cyber attack and educate defence teams about effective responses within a controlled and forgiving environment.

CORNERSTONE 3:
DEFINE A CYBER SECURITY STRATEGY

An effective cyber security strategy completes the foundation of a secure technological and organisational infrastructure. Designing a cyber security strategy is a complex task for most firms as the strategy must be robust and responsive enough to address a dynamic operational environment. Security professionals can work to create a cyber security strategy to create operational efficiencies, maximum return on technology investments, and assured data and asset protection into the future.

Given the cost and reputational risks associated with a cyber attack – estimated at £11.7M (US$15.4M) per company according to a World Economic Forum 2017 study – there is no doubting the importance of taking a strategic approach to cyber security.

Ultimately, a truly cyber resilient shipping organisation is one that gains intelligence on evolving cyber threats to inform decisions and plans, going beyond the minimums needed to achieve compliance.

Digital Ship

iSHIPPING CONFERENCE

ACHIEVING DIFFERENTIATION THROUGH DIGITAL INNOVATION

Copenhagen, 5 September 2019

iShipping, to Digital Ship, means making the best possible use of data and digital technology to make the shipping industry operate as safely and efficiently, with the best possible quality of life of people involved, as we possibly can.

Data is not the "new oil" (or the "new shipping") But better use of digital technologies can improve its contribution to efficiency and safety, and in a world of fine margins, that can mean the critical difference between survival and failure.

By iShipping we mean the right piece of data in the right place at the right time to support decision making, helping us run our vessels as efficiently and safely as possible, giving us fast access to the right expert in the event of any problem, and getting that expert the right data to help them resolve it.

Efficiency and safety involves increasingly high levels of vessel performance, improving maintenance and purchasing strategies, being fully prepared for vetting inspections, and making the right decisions about crewing, new builds, equipment and scrapping. It means making sure seafarers and superintendents have the right understanding of what is going on, both from their training and from the information that is given to them. It means people feeling clear about what is expected from them, rather than overloaded by information.

Delivering digital systems which provide this is an enormous technical and organisational challenge, requiring empathy, extensive modelling of what the organisation does and the people do. Technically it requires the most we can get from our satcom, software systems, e-navigation systems and other electronics. It also involves a lot of communications.

Getting this right is what we call 'i-Shipping'. At our 3rd iShipping Copenhagen on 5 September 2019, we'll learn more what is required to deliver true iShipping and create the best shipping industry that we are capable of. Topics to be covered include:

Digitalisation – how should shipping companies determine how best to allocate their resources?
Satellite communications – which services have the most to offer a shipping company and how should they choose?
Cybersecurity – what are the best practical steps a shipping company can take to maximising it?
Data integration and sharing – how can a shipping company get more value from their data through better sharing?

Venue: DA Conference Centre, Kalvebod Brygge 31-33, DK-1780 København V.
No admission charge for ship owners, operators, managers and builders.
To register: https://www.copenhagen.thedigitalship.com/register/
Enquiries: lyndell@thedigitalship.com

PHISH & SHIPS

BE CYBER AWARE AT SEA

SPEAR PHISHING

DON'T BE THE TARGET

THIS EMAIL-SPOOFING ATTACK TARGETS A SPECIFIC INDIVIDUAL OR ORGANISATION, SEEKING UNAUTHORISED ACCESS TO SENSITIVE INFORMATION