#24
NOV: 2018

PHISH & SHIPS

BE CYBER AWARE AT SEA

Kindly sponsored by

JWC INTERNATIONAL

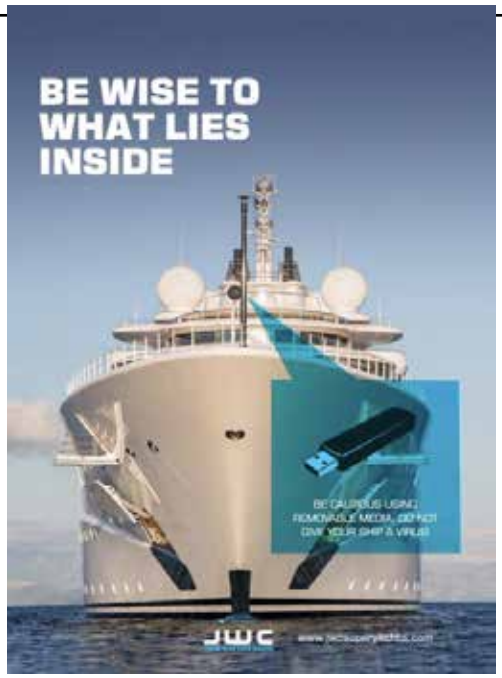
SMART4SEA TRAINING AND EDUCATION AWARD 2018
UNSUNG HERO OF INDUSTRY: HIGHLY COMMENDED, SAFETY AT SEA AWARDS 2017
BEST CYBER AWARENESS CAMPAIGN, INTERNATIONAL CYBER SECURITY AWARDS 2017

2018 Training Award SMART4SEA

Welcome to "Phish & Ships", the maritime cyber security newsletter, keeping you up to date with the shipping and offshore industry initiative, "Be Cyber Aware At Sea".

Issue 24, sponsored by JWC International, a world leader in maritime and cyber security training - https://www.jwcinternational.com - we look at a range of key issues affecting the shipping industry.

There are a host of key cyber security issues, and from training to vulnerability assessments, we look at how the maritime industry needs to do more to protect seafarers, cargoes, ships, assets and its very reputation. Find out more about the campaign at https://www.becyberawareatsea.com/ Stay safe, stay secure, be cyber aware at sea.



CYBER IGNORANCE IS NOT BLISS

US maritime law firm Jones Walker has released a new survey of cybersecurity preparedness at American maritime companies. The survey claims that nearly 40% of respondents had suffered a cyberattack or an attempted attack within the last year. Despite the evident risk, nearly two thirds of these firms said they are not prepared to prevent a data breach.

According to co-author Andrew Lee, a partner at Jones Walker, cybersecurity is often treated as a low priority in the industry because of the perception that it is merely an IT issue. "A cyber threat is a business risk; if the attitude doesn't align to acknowledge this, cybersecurity won't get the organisational attention that is needed," Lee says.

This attitude means that the industry's response to cybersecurity threats is often reactive. But waiting for a breach means accepting risks, potentially including the theft of customer or employee data; the operational impact of a ransomware attack, and potential state-level compliance issues, which vary by locality.

Companies need a holistic solution, Lee says. As a first step, a firm can work with its IT team to determine where its operations are visible on the internet and where it has vulnerable points of entry. On the human-factors side, practical cyber policies, training programmes and breach response plans are key.

"Companies often handle breaches poorly, and we can help them put together a written plan to guide their activities in the event of a breach," Lee says. "Once the plan is developed, we can help them conduct trainings and tabletop exercises on breach response."

Responses from smaller firms stood apart in the survey. About 30 percent of large firms reported that they had been successfully hacked in the past year, but none of the small firms surveyed said that they had suffered a data breach. Only one small company was aware of an attempted attack.

This raises questions as to whether the smallest firms have the capacity to detect a cyberattack, and 14 percent of the small firms acknowledged that they were unsure whether they had been attacked or not.

In part, this could be a question of budgeting: about one in ten survey respondents, almost all from smaller firms, said that they are not spending any money to address cybersecurity.

"Small companies may not even be aware that they have been attacked. They can't really diagnose the problem if they don't understand the problem, and a significant proportion are devoting little or no budget to the issue," warns Lee.

See joneswalker.com for further insight into the findings.

JUNIOR STAFF MAKING BIG PORT CYBER MISTAKES

Junior staff in port operations are a crushing weak spot for ports as they look to build up their cyber security resilience, a specialist has warned.

Protection Group International (PGI) senior cyber threat analyst Olly Jones says, "malicious actors will intentionally target junior staff who may not be expecting to be the focus of a targeted intrusion".

There is a major concern that port management may mistakenly believe that attackers are only interested in network administrators or senior-level executives.

Mr Jones added that while responsibility for the procurement and implementation of technical defences and security processes should still rest within IT teams, "it is the responsibility of every employee to ensure that their online activity does not threaten the security and integrity of their organisation's systems".

He advises ports improve their employees' 'cyber hygiene' as building an awareness of basic social engineering techniques can defeat an estimated 80%-90% of cyber threats.

RESPONDING TO CYBER ATTACKS

The global maritime industry must do more to protect shipping firms against growing cyber-security threats, experts have claimed.

As such, an important first step is to create awareness and encourage the reporting of incidents, said Mr Mark Milford, vice-president in charge of cyber security at Finnish technology firm Wärtsilä.

The announcement came as Wärtsilä opened an International Maritime Cyber Centre of Excellence (IMCCE) in Singapore. The IMCCE consists of a Maritime Cyber Emergency Response Team (MCERT) and a cyber academy. Reportedly providing a world's first industry solution for the marine industry, the IMCCE will provide a focal point for the industry to help drive the cyber awareness and response to cyber incidents.

"Cyber is such a critical topic to all players in marine. Taking stewardship in something as important as this, shows that Wärtsilä is committed to transform and digitalize the marine industry. This is the next step in our Smart Marine vision and supports our Oceanic Awakening and Sea20 initiatives," says Marco Ryan, Chief Digital Officer at Wärtsilä.

The MCERT is an international cyber intelligence and incident support platform enhancing cyber resilience for the entire maritime ecosystem. It provides international intelligence feeds, advice and support, including real-time assistance to members on cyber attacks and incidents, and a Cyber Security Reporting Portal (CSRP) for its members.

PORTS PHISHED FOR BITCOIN

The cyber security attack that hit the port of San Diego recently apparently included ransomware and demand for Bitcoin, port officials have said in a statement.

"The port of San Diego continues to investigate a serious cybersecurity incident that has disrupted the agency's information technology systems, and the Port's investigation so far has determined that ransomware was involved in this attack," read the port of San Diego statement. "Port employees continue to have limited functionality which may have temporary impacts on service to the public, especially in the areas of park permits, public records requests, and business services."

As we have covered in earlier issues, it emerged the port of Barcelona also suffered a cyber attack around the same time, and back in July Cosco's massive cyber attack originated from its operations at the port of Long Beach.

Unfortunately the huge volume of information that ports handle makes them especially ripe targets for hackers. Ports also handle sensitive information that can be leveraged for financial fraud and spear phishing attacks.

Experts are therefore not surprised that sophisticated malicious actors are targeting these enterprises. Once more this means there are calls for the maritime industry in its entirety to increase awareness and levels of protection in order to counteract these attacks.

Asaf Shefi, CTO at cyber security firm Naval Dome, good friends of the Be Cyber Aware at Sea campaign, has repeatedly asserted that his company is seeing an increase in the number of cyber criminals targeting the maritime industry in general.

"We are seeing attacks happening more frequently across shoreside companies, ports and ships. The ship-to-shore interface does need to be protected as this could open the door to both the port and ship for hackers. Each system onboard a vessel needs to be protected to prevent the spread of an attack," Shefi said.

See https://navaldome.com/ for more details.

CYBER THREATS AND DATA THEFT KEEPING SHIPPING EXECUTIVES AWAKE AT NIGHT

The Global Maritime Issues Monitor 2018 report, published by a consortium of the Global Maritime Forum, global insurance broker and risk adviser Marsh, and the International Union of Marine Insurance (IUMI) has been released, and it features the views of the maritime industry on cyber issues.

'Cyber-attacks and data theft' sit alongside more traditional problems such as 'energy price fluctuations', and 'changing trading patterns', as being most likely to occur.

The report examines the impact and likelihood of 17 major issues based on research among senior maritime stakeholders across over 50 countries globally. According to the research, the maritime industry does not appear to be prepared for any of these issues.

Worryingly, this is amplified by the fact that the issues the industry are least prepared for are the ones deemed to have potentially the biggest impact on the sector. The Issues Monitor shows that there is a need for a greater awareness of the long-term forces shaping decision-making.

Of the five issues that the maritime industry appears to be least prepared, two relate to our area of interest, as 'cyber-attacks and data theft, 'join global economic crisis', 'geopolitical tension', 'air pollution' and 'governance failure' as the greatest concerns.

Indeed, cyber-attacks and data theft very much appear to be the maritime industry's weak spot. In addition to being ranked as the top issue that the industry is least prepared for, executives believe it has the highest likelihood of occurring and is only surpassed by a 'global economic crisis' and ´energy price fluctuations' in terms of impact.

"Emerging digital technologies are challenging conventional business models and are creating new opportunities for the global maritime industry. But, along with its transformative power, this digitalisation is creating rapidly evolving risks such as cyber-attacks and data theft. It is worrying that, despite recent high-profile attacks, the industry is failing to get to grips with cyber risk. By taking a more strategic approach, firms are better positioned to capitalise on these opportunities, while protecting their people and assets from digital threats," says Marcus Baker, Chairman of Global Marine Practice at Marsh.

Access the full report: http://bit.ly/2PtNEBY

12 STEPS TO CYBER SAFETY

The International Association of Classification Societies has issued 12 recommendations on cyber safety, to mark a step change on delivery of "cyber resilient" ships.

IACS has published 9 (nine) of its 12 (twelve) recommendations on cyber safety with the aim of enabling the delivery of cyber resilient ships whose resilience can be maintained throughout their working lives.

As a result, the IACS Recommendations address the need for:

- A more complete understanding of the interplay between ship's systems
- Protection from events beyond software errors
- In the event that protection failed, the need for an appropriate response and ultimately recovery.
- In order that the appropriate response could be put in place, a means of detection is required.

IACS also recognised at an early stage that, in order for ships to be resilient against cyber incidents, all parts of the industry needed to be actively involved, and so convened a Joint Working Group (JWG) on Cyber Systems. A significant part of the JWG work has been in identifying, best practice, appropriate existing standards in risk and cyber security and identifying a practical risk approach.

Consequently, the 12 IACS Recommendations, collectively, not only provide guidance on the most pressing areas of concern but work as building blocks for the broader objective of system resilience.

The IACS Chairman, Mr Jeong-kie Lee of the Korean Register, stated "These 12 Recommendations represent a significant milestone in addressing safety concerns related to cyber issues. IACS focus on Cyber Safety reflects our recognition that cyber systems are now as integral a part of a ships safety envelope as its structure and machinery and IACS is committed to providing industry with the necessary tools as part of our wider mission to deliver safer, cleaner, shipping."

Importantly, and noting the challenge of bringing traditional technical assurance processes to bear against new and unfamiliar technologies, IACS has launched these Recommendations in the expectation that they will rapidly evolve as a result of the experience gained from their practical implementation. Furthermore, IACS recognises that these Recommendations are only an 'interim' product and that they will be subject to amalgamation into a larger document with more consistent language, overlaps removed and common material consolidated.

Commenting on this approach, IACS Secretary General, Robert Ashdown, explained "The decision to publish these new materials as stand alone documents as Recommendations was made explicitly to give industry stakeholders access to the developing material. IACS continues to make significant efforts to work ever more closely with industry and believes this approach provides the right balance between delivering the detailed guidance that is urgently required while remaining receptive to input from the industry stakeholders via JWG/CS on how they would like to see IACS proceed."

IACS recognises this is only the start in the ongoing struggle to maintain the cyber integrity of vessels. IACS remains confident, however, that the flexible and structured approach being adopted positions it well to further evolve and enhance these offerings, quickly and responsively, and in a manner which is practical and supportive of the needs of the largest number of industry stakeholders.

See the full report: http://bit.ly/2CSxv2c

The 12 Recommendations are:

Rec 153: Recommended procedures for software maintenance of shipboard equipment and systems

Rec 154: Recommendation concerning manual / local control capabilities for software dependent machinery systems

Rec 155: Contingency plan for onboard computer based systems

Rec 156: Network Architecture

Rec 157: Data Assurance

Rec 158: Physical Security of onboard computer based systems

Rec 159: Network Security of onboard computer based systems

Rec 160: Vessel System Design

Rec 161: Inventory List of computer based systems

Rec 162: Integration

Rec 163: Remote Update / Access

Rec 164: Communication and Interfaces

IACS
International Association of Classification Societies

BEFRIEND A CYBER SECURITY EXPERT

A major talking point in cyber security circles at the moment is that too few potential beneficiaries of expertise have ever actually met a cyber security expert.

A Kaspersky study last year showed that most young people hadn't met someone who worked in cyber security and that "63% of women think more positively about cyber security after meeting someone who works in the sector." We suspect that the figures may be even higher for maritime professionals.

Just how many directors, managers and executives within shipping companies have met cyber security specialists? How many masters, chief engineers or junior officers will have met the people who can explain or encourage their views on cyber security at sea?

The wise money would be that neither groups often, if ever, come across the cyber security community. That is a real issue, and one which is perhaps hampering efforts to get shipping companies and seafarers to better understand the threats facing them, what they can to do to deal with them and the actions to respond to vulnerabilities.

So, our advice? Get to know the people who can help. See if you can get someone in to do a talk, or ask your P&I Club - they will likely only be too happy to arrange something. When it comes to cyber security, get to know the people who know!

BULK PORT ACTIONS

Improving bulk terminals' cyber security was a key theme at Bulk Terminals 2018, the Association of Bulk Terminal Operators' annual conference last month. "Cyber security and safety can be investment drivers for bulk terminal operators, and for good reason," said ABTO Director Simon Gutteridge.

Upping the industry's ante in terms of cyber protection, following a number of hacking events, continues to be a priority for terminal operators.

While Ian Adams, Chief Executive of the Association of Bulk Terminal Operators, said: "Both physical and cyber security remains a particular weak spot for the ship-to-shore interface. Ports and terminals are not only at risk from breaches in their own security but also their customers". Adding, "Terminal operators do need to have robust business continuity plan in place".

TRAINING IS KEY

87% of firms see untrained staff as their greatest cyber risk, according to Willis Towers Watson and ESI ThoughtLab. This is compounded by staff training ranked as one of the weakest progress categories measured against the NIST cybersecurity framework.

The research also identified the most common types of attacks to include malware/spyware (81%) and phishing (64%), with external unsophisticated hackers (59%) and cyber criminals (57%) identified as the next biggest external threats.

The survey found that a company's threat perception varied based on the firm's cybersecurity maturity. For example, cybersecurity leaders tend to focus more on "Hacktivists" (52%) and malicious insider threats (40%), whereas cybersecurity beginners spend more time worrying about external threats (42%), such as partners, vendors, and suppliers.

Additionally, the research highlights that when it comes to cyber resiliency, or post-cyber incident processes, cybersecurity leaders invest more in cyber resilience versus their beginner counterparts. As companies become more advanced in cybersecurity, they increase their investment in cybersecurity resilience, with cybersecurity beginners spending 14% of their cyber budget, and cyber leaders spending 18%, on recovery.

Some other key findings around cybersecurity maturity and investment in cyber risk include:

- 91 percent of cybersecurity leaders feel their investment is adequate to meet their needs
- 33 percent of cybersecurity beginners view their investment as adequate to meet their needs
- 73 percent of companies plan to use behaviour analytics as a cybersecurity tool over the next two years
- 80 percent of companies have at least a small amount of cybersecurity insurance, with healthcare companies averaging one of the highest amounts ($16.4 million) and manufacturing averaging one of the lowest ($8.6 million)

"Leaders in cybersecurity are devoting significant resources towards protecting IT and risk functions within their organisations against external threats, but employee processes and training as well as corporate culture play a more integral role than many realize." As the report highlights, "The vast majority of cyber incidents result from employee behaviour and human error," says Anthony Dagostino, global head of cyber risk, Willis Towers Watson.

"In addition to mitigating cyber threats through technology and risk transfer, cyber managers need to take a step back and assess their organisations cyber defences within. Cyber managers must adopt a continuous assessment strategy, one that focuses on the overall culture of engagement, talent preparedness and the role

PHISHING PAYS!

Gideon Lenkey, Technology Director at EPSCO-Ra shares his thoughts on how phishing emails pay.

It has to be said because quite simply it's true. It takes very little skill to execute a phishing scam and collect a crypto-currency ransom. Take for example an email received by a friend recently:

Hello!

Iâm a member of an international hacker group.

As you could probably have guessed, your account [EMAIL ADDRESS] was hacked, because I sent message you from it.

Now I have access to you accounts!

For example, your password for [EMAIL ADDRESS] is [PASSWORD]

Within a period from July 17, 2018 to October 3, 2018, you were infected by the virus weâve created, through an adult website youâve visited.

So far, we have access to your messages, social media accounts, and messengers.

Moreover, weâve gotten full damps of these data.

We are aware of your little and big secrets...yeah, you do have them. We saw and recorded your doings on porn websites. Your tastes are so weird, you know..

But the key thing is that sometimes we recorded you with your webcam, syncing the recordings with what you watched!

I think you are not interested show this video to your friends, relatives, and your intimate one...

Transfer $800 to our Bitcoin wallet: PwruptLamUfKTuMW39Qy1q4ohX9w

If you donâ€t know about Bitcoin please input in Google ôbuy BTCö. Itâs really easy.

I guarantee that after that, weâll erase all your ôdataö :)

A timer will start once you read this message. You have 48 hours to pay the above-mentioned amount.

Your data will be erased once the money are transferred.

If they are not, all your messages and videos recorded will be automatically sent to all your contacts found on your devices at the moment of infection.

You should always think about your security.

We hope this case will teach you to keep secrets.

Take care of yourself.

Sounds scary and a bit convincing right? They have an actual password, not the one for the account like they say, but one of her actual passwords. The email goes on to make a few assumptions, primarily that the recipient has visited a website with adult content, has a webcam and well, had done something embarrassing in front of it. While they were a little off base on their target, in this case they're probably right more often than they're wrong.

Before she pays the ransom maybe we should have a closer look at what is actually going on here. Firstly, her email address in the from field is not evidence of a hacked account, it's simply evidence of how easy it is to spoof email headers.

Secondly, having a password might not be evidence your computer is hacked but rather a data breach on a system or service you use, like Dropbox or LinkedIn, for example. Fortunately there is a website that made it fairly clear where the attacker got the password from. By searching the site https://haveibeenpwned.com/ for her email address, she was able to confirm the exact data breach that leaked her email and password. In this case it was from a major breach in 2012. The attackers simply acquired a list of email addresses and password pairs, likely purchased on the darknet, and went phishing.

So how successful is a low tech scam like this? Well because they provide a bitcoin wallet address to send the ransom to, we can see for ourselves.

By going to the site https://www.blockchain.com and searching on the bitcoin wallet provided in the email wruptLamUfKTuMW39Qy1q4ohX9w) we can see that about 16 people fell for the scam for a total of about $12,672 USD, at the time of writing this article. The contents of that wallet were transferred to another wallet: RWdNeQNKwspX1o9ycRW6o2CKbsu) containing about $52,000 USD. This wallet was then emptied into another iqik4h6HoQgEDWXPoeR3R89B9dnA) that had received a total of approximately $430,000 USD within the timeframe of the attack.

This is just a small window into a simple phishing scam but should give you an idea of how profitable phishing is and why you are a target. With just an email list and passwords from an old data breach an attacker can turn a tidy profit.

I've even seen this scam without any passwords, just an email address. Due to the anonymous nature of blockchain crypto-currency transactions there is very little law enforcement can do to 'follow the money' either. If you receive an extortion email, take a step back, take a deep breath and make sure you're not being hustled by a low tech scammer before deciding how to best deal with it.

To learn more about EPSCO-Ra see https://www.epsco-ra.com

THE COST OF ACTION v INACTION

In the light of the stats released by the Fairplay/BIMCO/ABS maritime industry survey, that half the respondents believe their company's annual cybersecurity budget is less than $10,000, we must ask the question about investment in the world of cybersecurity; how do you know you are spending the right amount on your cybersecurity?

The question is poignant and the terms are, according to Gary Kessler, professor of cyber security at Embry-Riddle Aeronautical University, misleading. Kessler shared his insights into the psychology of expenditure/investment: 'Priority, of course, is given to those line items for which we get the most "bang for the buck". We are constantly asked by managers, "What are we getting for this expenditure?" This is, of course, an indirect way of asking us to determine the ROI on every check that goes out of the door.'

Gary believes ROI is 'an erroneous way to think about cybersecurity' as cybersecurity is not 'a tangible asset' and therefore cannot be evaluated as such. To do so would be to talk yourself out of investing in it at all, particularly if you haven't encountered a threat directly. He instead coins the phrase 'return-on-negligence, or the cost of doing nothing', ie, we should consider the true costs of not investing at all in cybersecurity.

He makes the case that the consequences for firms which are not cybersecure will become increasingly punitive, citing new Californian law coming into effect in 2020 where 'consumers may be able to sue a holder of information up to $750 for each breach of privacy'. This law will affect companies with business gross of a minimum of $25 million meaning it will surely affect shipping lines and large ports in the state. Meanwhile, in Europe, the GDPR means huge fines for non-compliance or breaches due to negligence.

He also highlights other areas where cybersecurity has strong repercussions for negligence; loss of intellectual property for example, or a vessel being hacked or even, in extreme circumstances, a death. The costs here would be substantial. And, of course, there are the other intangibles, the losses both reputational and of consumer confidence, as well as impacts further down the supply chain and loss of confidence from peers.

Thinking of your investment in cybersecurity as being RON or 'return on negligence' makes it easier to consider spending money. But how much should one spend? And in what areas?

A survey in 2016 by Gartner found that most organisations spent 5.6% of their IT budget on security, although the range covered 1-13%. These days that figure will have undoubtedly increased, with 50% of businesses increasing their spending by 2018.

The key thing, when deciding how much of your budget to spend on cybersecurity, is to thoroughly evaluate your business' risk factors: consider how reliant you are upon cyber technology and data, realistically evaluate both internal and external threats, and don't forget to explore thoroughly your third-party suppliers and their risk factors and cybersecurity too.

BitSightTech offer a clear breakdown of where to consider spending:

1. Risk Management Framework Implementation – a framework to reduce risk, which would likely entail paying a consultant for advice on building the programme.
2. Third-Party Cybersecurity – these are a weak link in the chain and hackers do exploit third parties in order to gain access to first party networks, so this is a strong area to spend.
3. Endpoint Security – your employees' devices, all the endpoints that link your network to human contact. Most contain sensitive information and are easy gateways to more, so security and the ability to lock these down if you've been compromised it important.
4. Employee Training – a simple but effective area that helps with tidying up your employee cyber hygiene and protects from phishing.
5. Privileged Users – a hacker will target a 'super-user' and their 'super-privileges', allowing them to access almost all data in an organisation. Limiting access so individuals can only access the data they need to do their job is one way to limit this.
6. Cyber Insurance – while the above suggestions are about reducing or mitigating risk, buying insurance transfers it.

You can read more from Gary Kessler here: https://www.garykessler.net/ and BitSiteTech here: https://www.bitsighttech.com

1 Hour MCA Recognised & GCHQ Approved Training

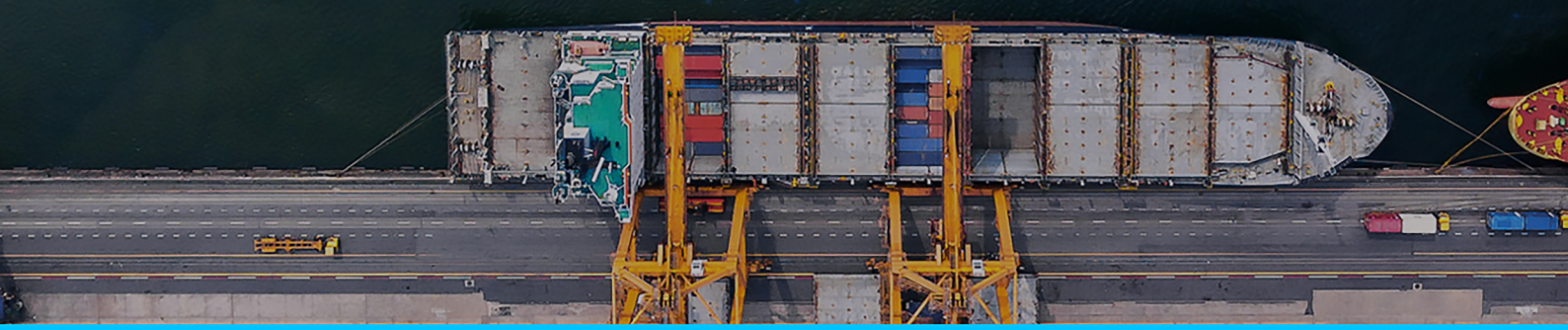
Maritime Cyber Security Awareness Course (MCSA)

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