BE CYBER AWARE AT SEA

Kindly sponsored by

AXIS

#44 / JULY 2020

PHISH & SHIPS

AXIS ON CYBER INCIDENT RESPONSE PLANNING FAILURES

IMO GUIDELINES SIX MONTHS TO GO

400% INCREASE IN REPORTED MARITIME CYBER ATTACKS

OUR AWARDS

NOMINATED 2019
SMART4SEA CYBER SECURITY AWARD

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.

After six months of uncertainty, slowly the world is opening up again and we are starting to see how the 'new normal' is going to look for many of us.

The impact of lockdown and remote working is still being calculated, with the 400% increase in shipping cyber attacks a significant indicator of the stresses the sector has been under. Now is the time, as workers start to return to offices, to ensure that systems are carefully reintegrated to prevent a second wave of cyber attacks.

Elsewhere we look ahead to post-COVID-19 cyber concerns, relaying the views of one industry player about the liability shouldered unwittingly by owners reliant upon lacklustre security support, while the British Ports Association and Astaara join forces to launch a white paper 'Managing Ports' Cyber Risks'.

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

BE CYBER AWARE AT SEA

Kindly sponsored by AXIS

CYBER INCIDENT RESPONSE PLANNING FAILURES

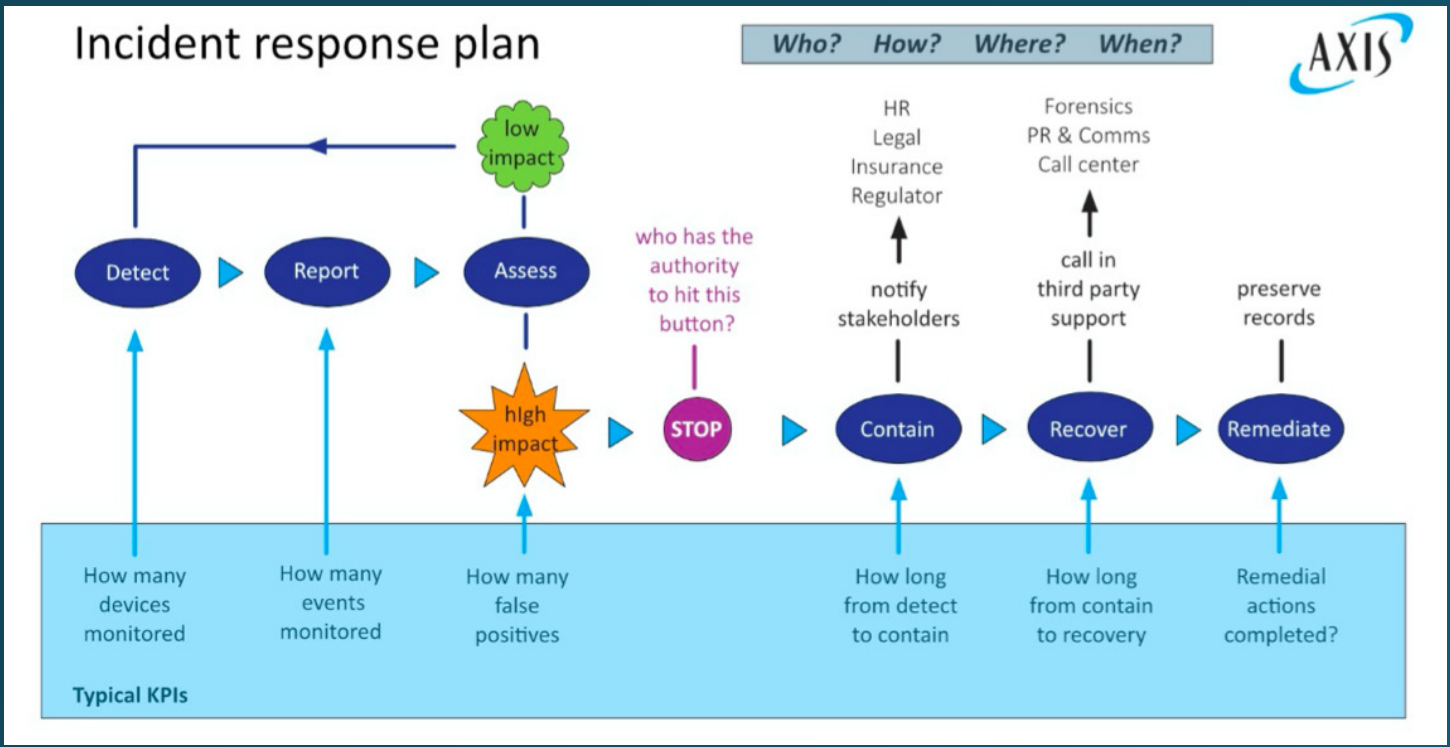
IF YOU FAIL TO PLAN YOU PLAN TO FAIL

WHAT IS INCIDENT RESPONSE?

Incident response is the process of detecting security events that may have a negative impact on network resources and information assets and then having the capability to respond and recover effectively in a timely manner. It is essential in today's operating environment that businesses can respond to incidents such as the loss of sensitive information, compromised credentials and the downloading of malware, not planning for these can lead to the risk of reputational damage and financial loss.

The shipping industry has become ever more reliant on technology over recent years and there are currently no signs that this is yet to slow down. In fact, with technologies such as blockchain to log cargo and the automation of vessels being introduced we are likely to see further growth in emerging technologies as they are still in the early adoption phase. This merging landscape has exposed vessels and shore-based facilities to a significant cyber risk. As part of a risk management based approached in securing the shipping it is essential to develop and exercise a Cyber Incident Response Plan CIRP.

A CIRP can be extremely effective and one of the most important tools when creating resilience within an organisation. At the same time there are some common mistakes that can hinder a business in making the most out of a CIRP.



PHISH & SHIPS

NO DOCUMENT OWNER

RESULTS: Having no specific person to lead with the management of the CIRP can result in a lack of accountability and diffusion of responsibility. This creates the perception of there's always another priority and consequently the document is likely to become stagnant.

SOLUTION: Define a specific function along with a named individual as the document owner

NO DOCUMENT APPROVER

RESULTS: With no defined document approver/ approvers could mean there is a lack of organization-wide buy-in and the CIRP is deemed not to reflect the interests of the business. This can also lead to approval being requested during the time of an incident, which is not the time to be asking and will hinder the ability to respond timely.

SOLUTION: Define a document approver or committee a group of approvers who can review and sign off the CIRP at least once a year.

LACK OF REPRESENTATION FROM NON-TECHNICAL RESOURCES

RESULTS: A CIRP that is heavily reliant on technical resources only is likely to struggle during major incidents. If a business falls victim to a breach of a client's sensitive information the response will require more than just the IT / security team's involvement which is why cross-functional buy-in, and involvement is ideal.

SOLUTION: Ensure the CIRP has cross functional contribution from Legal, Media, Finance, Risk Management, Physical Security, Executive Management, Audit, Info Sec IT and Vendors. Define limitations of authority, know exactly who can do what, where, when and how.

SINGLE POINTS OF FAILURE

RESULTS: SPF's can occur in many forms within the categories of people, process and technology. For example, a CIRP that point to a single position which encompasses a variety of skills can easily lead to the burn out of this individual during a large incident, or if they are not able to respond due to other commitments this can leave gaps in the response. Managing and responding to an incident should be separate responsibilities, it can become problematic if a single person is responsible for both as it would extremely difficult to communicate with both technical and operational elements at the same time and both have unique roles during an incident.

SOLUTION: Recognize the SPF and diversify the team taking a team approach to the CIRP. Define the two specific lead functions for a technical and strategic response, they should work in tandem just have a different focus. Ideally the strategic lead should be 75% political 25% technical and vice versa for the technical lead.

NO PRE-DEFINED SEVERITY LEVELS

RESULTS: This can result in the CIRP having a binary response, it's either on or off and there are no clear levels in between. So, the binary response does not enable a variation of responses based upon the different levels of severity of the incident. If there are no defined severity levels this can result in the same response for all incidents, creating fatigue and a lack of seriousness during the time of a severe incident.

SOLUTION: Define the severity levels from 1-4 and break the levels down into symptoms not threats, threats are constantly changing so they are not effective to respond to.

Key takeaways

- A CIRP requires cross functional input and buy-in from senior management
- A CIRP is a live document and requires an owner, approver and regular maintenance
- Must address a range of security incidents from simple malware all the way to complex breaches by detecting the signs and symptoms of an attack.

The common failures discussed are not exhaustive but simply a good start point for considerations when planning. At AXIS we understand the importance of incident response planning and exercising that's why we have developed our Tabletop cyberattack simulation which prepares businesses and builds resilience and understanding throughout the workforce.

References:
nvlpubs.nist.gov/
www.itgovernance.co.uk
www.secureworks.com

Article by Simon West, Cyber Risk Advisor at Axis Capital

HACKERS MAY BE TARGETING YOUR SHIPS. IT'S ONLY FAIR OUR NEW COVERAGE DOES, TOO.

In an era when evolving technology is making the maritime industry more innovative and efficient, it's also making companies and their vessels more vulnerable to crippling cyber attacks. Fortunately, AXIS Marine Cyber bridges the protection gap in today's insurance offerings. To see how we can help shield your shipping business from the unknown, contact Georgie Furness-Smith at **Georgie.Furness-Smith@axiscapital.com** or Sharif Gardner at **Sharif.Gardner@axiscapital.com**

www.axiscapital.com

IMO GUIDELINES: SIX MONTHS TO GO!

With the IMO's deadline now less than six months away, this is a critical period for maritime and shipping industries to be implementing their measures.

This month, as reported by John Snyder for Riviera, the North Sea OSV operator – Atlantic Offshore – have disclosed their cyber protection measures and detailed why it matters more than ever to be rigorous with regards to cyber defence.

Underlying their approach is the fact that the requirements of the crew and vessel means digital connectivity is more important than ever. "The shift towards digitalisation, crew welfare needs and demand for greater vessel efficiency are all drivers for reviewing and upgrading our ship/shore connectivity needs," said Atlantic Offshore chief executive Roy Wareberg. "Meeting next year's IMO cyber security rules in the same step was an opportunity too good to miss".

Atlantic Offshore have adapted Inmarsat's Fleet Secure Endpoint and all vessels use a Fleet Xpress bandwidth upgrade. The Fleet Secure Endpoint focuses on protection of the ship's 'endpoints' – the personal or business devices such as laptops which are a key vulnerability. The system scans the network and 'eliminates malicious encryption, blocks forbidden sites, shuts down malicious connections and runs anti-spyware/anti-phishing software'. All new devices must be verified before they can connect to the system while USBs that introduce malware provoke 'guardian portal' intervention.

"We are seeing data usage on board ship doubling roughly every eight months and owners develop a competitive edge by upgrading connectivity to anticipate crew welfare and vessel operational needs," said Inmarsat Maritime vice president offshore and fishing Eric Griffin.

"Forward-looking companies such as Atlantic Offshore recognise that the threat from cyber criminals is also rising, which is why they choose Inmarsat as a secure connectivity provider across all touch points, including endpoints."

As shipowners and managers count down to the 1 January 2021 deadline, these are the sorts of systems and solutions that must be considered among others to protect the industry at large.

With six months to go, there are resources available to help organisations negotiate their way to compliance with IMO's Resolution MSC.428(98) such as, for example, the Digital Container Shipping Association's security guidelines which you can find online (https://dcsa.org/initiatives/cyber-security/).

Please also find further guidance and resources for crew and managers alike on the Be Cyber Aware At Sea website – all FREE to read online, download and use onboard (https://www.becyberawareatsea.com/).

https://www.rivieramm.com/news-content-hub/shift-towards-digitalisation-requires-greater-cyber-protection-for-osvs-59865

400% INCREASE IN REPORTED MARITIME CYBER ATTACKS

According to Naval Dome there has been a 400% increase in attempted cyber attacks across the maritime and offshore sector since February 2020. It is Naval Dome's belief that travel restrictions, social distancing measures and economic recession may be impeding companies' abilities to sufficiently protect themselves against the considerable spike in malware, ransomware and phishing emails.

"COVID-19 social restrictions and border closures have forced OEMs, technicians and vendors to connect standalone systems to the internet in order to service them," says Naval Dome CEO Itai Sela.

Sela continued: "As budgets are cut and in the absence of service engineers, we are seeing ship and offshore rig staff connecting their OT systems to shoreside networks, at the behest of OEMs, for brief periods of time to carry out diagnostics and upload software updates and patches themselves."

"This means that their IT and OT systems are no longer segregated and individual endpoints, critical systems and components may be susceptible. Some of these are legacy systems which have no security update patches and are even more susceptible to cyber attack."

In addition Sela explained that remote working has provided cyber criminals with new targets, with attacks on home workers increasing tenfold. McAfee have also reported an increase in cloud-based cyber-attacks across all businesses by 630% which has also added to the problem.

"It is not sufficient to protect only networks from attack," Sela says. "Each individual system must be protected. If networks are penetrated, then all connected systems will be infected.

"Our philosophy is that all systems must be protected using a risk ranking. If it is, then the entire platform is protected from both internal and external attack vectors. If only the network is protected, then whatever enters the net (such as an unintentional attack from authorized personnel) will infect all connected systems. This philosophy is more cost-effective."

For Ido Ben-Moshe, Vice President Business Development, there is reason to believe that remote working and the introduction of remotely-controlled, autonomous technologies is likely to be brought in at a faster pace. While this is a positive step forward for business, he voices a concern that "this will see companies face new cyber security challenges if they fail to implement adequate protective measures."

"COVID-19 social restrictions and border closures have forced OEMs, technicians and vendors to connect standalone systems to the internet in order to service them."

- Naval Dome CEO Itai Sela.

SOURCES:

https://www.marinelink.com/news/surge-maritime-cyber-attacks-reported-479334

https://www.hipaajournal.com/attacks-on-cloud-services-increased-by-630-jan-apr-2020/

WE HACKED A SHIP – YANGOSAT REVEAL ALL

In May Ewan Robinson, director of maritime communications and solutions provider Yangosat, wrote a piece for Smart Maritime Network in which he outlines his serious concerns for the industry after an exercise in which his firm ethically hacked a ship.

It is a sobering read as he explains not only how easily the systems were overcome but also the lack of reaction by the owners and various manufacturers when he attempted to inform them of their failings.

"Owners and operators are being badly supported and advised by these super providers, or poorly trained engineers, and leave systems in an exposed state," he writes. "Equipment manufacturers and developers are so guilty of poor techniques and security that using 'industry best practice' is a total contradiction".

The poor quality support and advice being offered is, he contends, all to the detriment of the owners who, in the event of a cyber attack, may be refused their insurance claims and left liable for the incident.

In the exercise the failures included "the most basic mistakes. Mistakes like default admin passwords remaining in place." In their exercise they were able to use the default username and password that was still in effect on their target's VSAT system.

Access was made to the administration area, "so all usernames and passwords could be changed. It also gave us access to the system by FTP." Here was, he said, the first major security flaw as the FTP gave access to the entire operating system of the device.

Once in, they found a second major flaw upon discovering "a text file in every folder with a map of the entire structure of the operating system". This enabled the team to find and copy the 'hidden' password file which, while encrypted, was never-theless cracked within two hours, providing them with all the manufacturer's usernames and passwords, which they could use to bypass where the default admin usernames and passwords had been changed.

The clearly written piece is a must-read and highlights the importance of owners taking a proactive interest in the cyber security of their vessels.

As Ewan Robinson summarises: "The operators are trusting their providers to correctly implement systems on board, but with some manufacturers and developers failing to ensure security at such basic levels they will likely be left with the legal responsibility in the first instance."

The message is clear: "The owner is liable."

In the exercise the failures included "the most basic mistakes. Mistakes like default admin passwords remaining in place." In their exercise they were able to use the default username and password that was still in effect on their target's VSAT system.

https://smartmaritimenetwork.com/2020/05/25/hacked-a-real-life-story-of-exploiting-vessel-vsat/

BRITISH PORTS ASSOCIATION TEAMS UP WITH ASTAARA TO HIGHLIGHT GROWING CYBER RISK MANAGEMENT

Guernsey-based cyber insurance and risk management specialists Astaara has today launched a white paper in partnership with the British Ports Association aimed at highlighting the strategies to promote cyber security in ports.

The explosion in remote working and reliance on technology in maritime business continuity throughout the covid-19 crisis has boosted interest in cyber security and resilience in the wake of a fourfold increase in cyber-attacks in the maritime industry since February.

In one high profile attack last month, (9 May) computer systems at the Shahid Rajaee port in the strategically important Strait of Hormuz were attacked, creating traffic jams of delivery trucks and delays in shipments. It is understood that the attack came in direct response to a failed Iranian cyberattack on an Israeli water facility last month.

Whilst attacks from criminal groups are far more common than suspected state-based attacks or 'hacktivist' incidents, the overall upward trend is concerning and driving increased interest in security. The global cyber security market is expected to grow from £144 billion to £182 billion by 2021, although that will still be only around 10% of the value lost to cyber-attacks each year.

'Now, more than ever, the advantages of digitisation should be capable of being realised, but only if the corresponding management resilience and recovery plans are in place and practiced to ensure those digital control systems and data flows are uninterrupted and uncorrupted,' said Robert Dorey, CEO of insurance service and risk management advisory business, Astaara.

'Processes need to be continually reviewed and updated as necessary, training provided, and new approaches to monitoring assessed and adopted.'
Mr Dorey added that marine companies were at increased risk of cyber-attacks, as scammers prey on the coronavirus disruption.

'The Covid-19 restrictions mean that many activities, for example crew change, marine warranty survey or superintendent spot check will be done differently or just may not happen. This means that maritime business are more vulnerable,' said Mr Dorey.

'Criminals realise this and do not care about the human cost of Covid-19, or their crimes. They are not interested in the morality of their action. Instead they are interested in disruption and making money; they see Covid-19 as an opportunity.'

Remote working has been highlighted as a major risk for security, as the attack surface is broadened. Spoofing to misdirect payments long being a favourite of cyber criminals; classically, hackers will plant a virus, enabling them to monitor emails and change the text of a message from suppliers, adding a different bank account.

“Covid-19 impacts the maritime industry like no other, principally due to complex supply chain relationships.” - Mr Robert Dorey CEO of insurance service and risk management advisory business, Astaara.

‘Covid-19 impacts the maritime industry like no other, principally due to complex supply chain relationships,’ said Mr Dorey.

Astaara white paper – ‘Managing Ports’ Cyber Risks’ – is launched today with The British Ports Association, as part of The Port Futures thought leadership programme. The paper looks at the ever more complicated business environment a of a port, with increasing regulation and risk.

The BPA programme was launched in 2018 to examine global emerging trends in the ports and shipping industries. This rolling programme of activity addresses key issues for ports over the next 50 years, including new technology and new applications of technology, infrastructure, and skills, as well as potential opportunities for and challenges to British ports that these issues present.

The British Ports Association (BPA) represents over 100 port members and over 80 associate members. Our port members own and operate over 350 ports, port facilities and terminals of all sizes across the UK, facilitating more than 85% of the UK’s maritime trade, 95% of which is carried by sea.

Mark Simmonds, Head of Policy and External Affairs at the British Ports Association, said: “As key gateways for 95% of the UK’s international trade, ports are critical to the UK economy. The British Ports Association is keen to explore the benefits that technology can bring to our industry, whether through increased productivity or new ways of providing services.

As port systems become ever more connected and digitalised, it is important that security and resilience is built in in to processes and training. Cyber security should be a board-level issue for all ports and we are committed to sharing and improving both Government policy and industry practice wherever we can. We hope this paper will serve as a useful reminder and guide for UK ports.”

Source
https://www.britishports.org.uk/news/bpa-teams-up-with-astaara-to-highlight-growing-cyber-risk-management

LATENT CYBER RISK POST COVID-19

This month The Maritime Executive raised the question of 'latent cyber risk' with regards to COVID-19 and the gradual resumption of regular working practices after the lockdowns have ceased and employees can return to their work environments.

They explain that a latent cyber risk is one that is 'undetected, unplanned and unanticipated' and point out that normally this sort of risk is noticeable when organisations start connecting old and new systems that were never designed with each other in mind. These latent risks are a key part of why cyber risks are so plentiful: the recent constant development of systems, at such a fast pace, means there are far more likely to be gaps in security that have simply not been considered.

However, as regards COVID-19, The Maritime Executive outline how the necessary rush of companies to remote working to enable them to survive the pandemic precautions meant they have had to 'adapt expanded and stretched networks way beyond their normal limits'. In the process, key cyber security procedures have been neglected as 'work networks mingled with home networks, people emailed documents to personal accounts and USB drives were used to help move and share files like never before.'

The upshot has been clear to see; by exchanging control for flexibility, offices have opened up their networks to the realities of personal computer choices and security with the visible results seen as cyber threats have escalated.

Now, as workers readjust to a post-COVID working environment, alongside the new measures such as wearing masks and checking temperatures, there must be due consideration shown to how to reintegrate computers, devices and systems that have been exposed to threats for months.

In fact, as the article makes clear, most of the measures we are wielding against COVID-19 are not very applicable to the cyber environment. After all:

- You cannot socially distance a network. As systems and networks are reconnected to each other and the internet, malware can spread. It is recommended to 'segment, protect and monitor those networks'.
- Contact tracing a cyber attack is difficult. Malware attacks can spread in seconds and attackers are adept at covering their tracks.
- No system is stand-alone. Almost all systems will have some form of connectivity, even just an update run from disk, so the assumption should be that everything is vulnerable to attack.
- Cyber hyper-mutates. Like natural viruses, cyber ones can, and do, mutate, and at hyper speed, reflecting the determination of the attackers who are refining their tactics as they keep pace with the rapidly changing cyber sector itself. While aware of the last attack, you must try and anticipate the next one.

However, one key lesson shared between COVID-19 and cyber threats? Good (cyber) hygiene, as noted in the article:

- Account and plan for cyber security as a daily part of risk management.
- Proactively manage it with an all-encompassing programme, from assessment and planning, to protection and defence, to detection and response.
- Consider cyber technologies, services and solutions, finding the right partners with the right expertise for your specific situation.
- Start from day one of your restart, considering new policies and staff education in addition to scanning, monitoring and management of your networks.
- 'Remember that COVID-19 is not the only virus that your employees can bring back into your work place.'

https://www.maritime-executive.com/corporate/covid-19-s-other-viral-threat-cyber

1 Hour MCA Recognised & GCHQ Approved Training

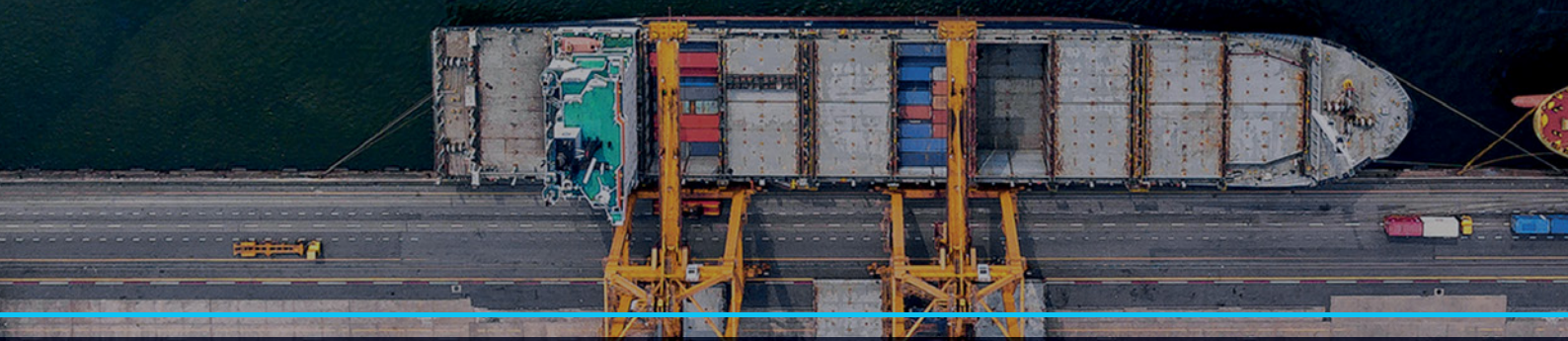
Maritime Cyber Security Awareness Course (MCSA)

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

VISHING

Voice phishing (Vishing) is a form of phone fraud, using social engineering via voice call to access sensitive information, often for financial reward

IF YOU SENSE SOMETHING SUSPICIOUS, VERIFY THE CALLERS'S IDENTITY