BE CYBER AWARE AT SEA

Kindly sponsored by

AXIS

#39/ FEBRUARY 2020

PHISH & SHIPS

AXIS ON...
THE ISSUE WITH 'SHADOW I.T.'

WHAT DOES 5G MEAN FOR SHIPPING?

NEW PORT GUIDELINES FOR UK SHIPPING

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.

Asking the question is the first step to getting an answer, and in order to get to grips with how best to protect cyber security, we need to be prepared to ask some tough ones.

In this issue we look at some of the lurking questions we have to approach. Sometimes it's the question that goes unasked – AXIS's report on Shadow IT is an eye-opener for any firm in which the IT department are not fully aware of the services or devices employees use without even considering security implications. Then there are the questions we are almost afraid to ask, for example questioning the impact of future technologies on cyber security in the face of the undoubted benefits to the industry, in particular 5G and autonomous shipping.

In order to stay one step ahead of the cyber-criminal, we need to be asking these questions sooner rather than later.

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

THE ISSUE WITH SHADOW I.T.

BE CYBER AWARE AT SEA

Kindly sponsored by AXIS

Shadow IT is the term given to IT devices or services that are being used without the approval of, and often even without the knowledge of, your IT department. Shadow IT takes many forms, but some typical examples are: cloud storage services like Dropbox and Box, internet connected items like coffee machines and IP cameras, or unapproved wi-fi routers or extenders plugged into your corporate network to allow those near it to 'access the internet'.

Why is it an issue?

These services are often outside the scope of your organization's security and privacy controls. This means that they are not being protected by your security team. Your data may be more exposed to attack; it may not be backed up. It may be in a data center in a foreign country, contravening a data privacy law or regulation. As for physical devices, these may not be monitored for security threats or patched correctly, if patched at all, exposing your company to significant risk, fines and even jail for responsible executives.

Compounding these headaches is the fact that attackers look specifically for Shadow IT so they can use this 'chink in the armor' to attack the company. Why attack a well defended front door or back door when you can walk right in through the fire door that has been wedged open?

What does it look like in the marine industry?

The issues described above are already here for shore-based operations, but as modern ships and platforms become more digitized and connected, Shadow IT will become a significant risk to the off shore marine industry.

People are always looking to make their lives more comfortable, easier, more efficient, especially where 'getting things done' are at the core of your daily business. As communication bandwidth increases, and more technology is adopted off shore, peoples' thirst for services (normally only used on shore) and creature comforts, and the necessary workarounds to get them up and running, will also increase. Resulting in offshore Shadow IT.

How do we deal with it traditionally?

In order to deal with Shadow IT, you need to have visibility of it. Asset and inventory management, coupled with scanning technologies used to discover unregistered devices or services within the organization, are key to mitigating the risk of Shadow IT. Governance and policies try to prevent Shadow IT from happening in the first place or, manage requests for new services or devices, when requested. But governance and policies are not 'active' mitigation methodologies - they still require people to comply. Sadly, the most effective method- Training and Awareness - is often overlooked. If people don't understand Shadow IT, or the threat it poses, it is difficult to blame them for trying to be better at their job, or to discipline them if there is a policy that they didn't know about it.

So what?

Organizations need to start considering what additional challenges will come with the changing landscape of marine technology. The increasing use of personal devices offshore means there is already some experience in this space. However, more needs to be done to make staff, crew and contractors aware of the safety and security implications of connecting personal or internet enabled devices to ship or platform networks or accessing cloud based services while offshore.

However, you can lead a horse to water, but you can't make it drink?

Article by Stuart Quick, Centre of Excellence Lead at Axis Capital

Guidelines on Cyber Security Onboard Ships - 5.3 Procedural protection measures :
https://www.ics-shipping.org/docs/default-source/resources/safety-security-and-operations/guidelines-on-cyber-security-onboard-ships.pdf?sfvrsn=16

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	✓

WHAT DOES 5G MEAN FOR SHIPPING?

It appears so far that 5G is the buzzword of 2020. It was the centre of a recent conference and summit circuit in Singapore where Andre Wheeler of Splash 247 notes that "the debate has shifted from concept to the development of smart port technology". So, we have to ask the question, what does it mean for the maritime industry?

We may mostly think of 5G in so far as our mobile technology and how much faster we will be able to download a video or music using it, but in global logistics, it will be a revolutionary technology. As we gather huge amounts of data to drive decision making, faster data speeds should result in a more responsive network, enabling this transformation. The benefits to the maritime industry are severalfold.

In a world where smart devices are proliferating at great speed, there is simply more bandwidth for all these devices to operate on a 5G network than a 4G one. It will enable companies to sync many multiple devices and systems on a more or less continuous basis, driving the collection and usage of big data. This means we will be able to track and trace cargo at all stages of delivery, while also collecting potentially vital information such as container humidity, temperature, etc which can then be remotely managed. This amount of observation and management should have positive security implications which should be reassuring for consumer and company.

In autonomous technology 5G will be an essential supportive system due to its extremely low latency (time lag of data being sent to and from devices). In autonomous technology, for example the autonomous boats we expect to see afloat in short order, there is a continuous flow of data to and from the vessel. The latency of 4G means a time lag is inevitable, with possible security or safety issues when it comes to remote time-critical decision-making. 5G transfers information at one millisecond, as opposed to 4G's 50 milliseconds – creeping much closer to the 'real time' operation that makes this technology safer.

While this latency speed is a key part of security and safety in various technologies, it will also quite simply save time. In the Port of Livorno there is a 5G enabled digitalised platform in which the transportation system devices, from sensor to cameras and beyond, are networked and unmanned ground vehicles automatically load and unload. 5G is essential to the smooth efficiency of this data-driven system.

As Andre Wheeler points out, this technology is being used in several ports around the world, most notably in China where they are developing 'intelligent port centralisation' that is set to reduce costs and improve efficiency. In Qingdao they have reduced labour costs by 70% using this technology for those ends. Meanwhile in Singapore they are seeking to optimise performance in loading and unloading of vessels – given this activity accounts for 75% of a port's costs, this has huge implications.

Where 5G has hit the headlines has been in who we let invest in and build the network. Certain companies may get the job done but risk giving an external state significant access to the network, with implications for establishing trusted long-term security. However, when considering your average cyber-criminal, it should bring some benefits with further encryption of data and the ability to 'network slice' in which virtual networks can be customised and managed in segments.

Nevertheless, caution should always be taken – new technology may bring new security features, but how long before cyber-criminals work round them? Already there is evidence that 5G is not a silver bullet to cyber-crime; Ravishankar Borgaonkar, a research scientist from Norwegian tech analysis firm SINTEF Digital told Wired magazine that "there's always room for improvement" having found and reported a number of security vulnerabilities in 5G.

So, as we await the transformation of the maritime sector with 5G technology, we should remember that cyber hygiene will still be an important part of enjoying this technology safely.

https://splash247.com/will-5g-change-logistics-and-ports/
https://logisticsofthings.dhl/5g-five-things-it-means-for-logistics/

WHY DIGITALISATION AND CYBER SECURITY SHOULD GO HAND-IN-HAND

Cyber-risk management is at the heart of a NYK Group's investments in digitalisation

With a goal of safe navigation, ClassNK released its Cyber Security Management System for Ships in March 2019, providing guidance on ensuring, implementing, maintaining, and continuously improving shoreside and shipboard CSMS. ClassNK's guidance covers management measures regarding protection against cyber risks in not only the navigation stage, but also in the construction and design stage of ships.

The 98th session of the IMO Maritime Safety Committee (MSC98) approved guidelines on maritime cyber-risk management in June 2017. MSC98 recommended that a description of cyber-risk management be included in the safety management systems (SMS) manual of ship-owners and ship management companies, encouraging strengthened measures against cyber attacks internationally.

The NYK Group plans to strengthen cyber-risk management for both LNG carriers and other cargo vessels.

Focus on digitalisation

NYK Group has made digitalisation a core part of its business plan in the years ahead. The NYK Group's medium-term management plan, Staying Ahead 2022 with Digitalisation and Green, emphasises digitalisation and environmental initiatives to enhance safety, vessel efficiency and reduce downtime.

While promoting digitalisation and the use of Internet-of-Things (IoT) in vessel operations, NYK has been strengthening cyber security measures throughout the group, making cyber security a high priority.

Among NYK Group's digitalisation research and development is the implementation of the paperless Unmanned Machinery Space (UMS) check system, which focuses on engine safety and reducing maintenance costs.

During a traditional UMS check, a crew member must take a number of measurements, conducting a large number of checks, if an engine plant and equipment are to be operated unattended. This data is recorded manually by the crew member.

Using the electronic UMS check system, the crew member can use a mobile device, lowering data entry time and reducing data entry errors. The mobile platform also allows data trends to be displayed graphically, storage of photos and videos and transmission of data directly to onshore servers, allowing shoreside personnel to examine the data.

Another NYK-MTI joint development is Kirari Ninja, a camera that can automatically photograph the interior of an engine's combustion chamber to allow inspection.

By installing it on the upper part of the engine piston in the combustion chamber, Kirari Ninja can take images of the interior. The images make it possible to view in detail the condition of the inner part of the combustion chamber.

In 2018, NYK launched a ship management platform, NiBiKi to digitise applications, approval, and operation workflow within the SMS. The NiBiKi system enables data to be shared between the ship operation company and the management company, compiling data for analysis to improve safety, crew performance and training and eliminate vessel and machinery downtime.

In November, NYK inked a long-term agreement with Norway's Dualog to develop a cyber-risk management system to provide multiple layers of security to protect ship-to-shore data sharing. Developed under the Cepa Shield project, the cyber-risk management system will be implemented in trials on 50 NYK-operated vessels, with the intent of future installation across 250 vessels. The system will provide NYK shoreside personnel with the ability to quickly assess the condition of each vessel under attack.

https://www.rivieramm.com/news-content-hub/why-digitalisation-and-cybersecurity-should-go-hand-in-hand-57714

1 Hour MCA Recognised & GCHQ Approved Training

Maritime Cyber Security Awareness Course (MCSA)

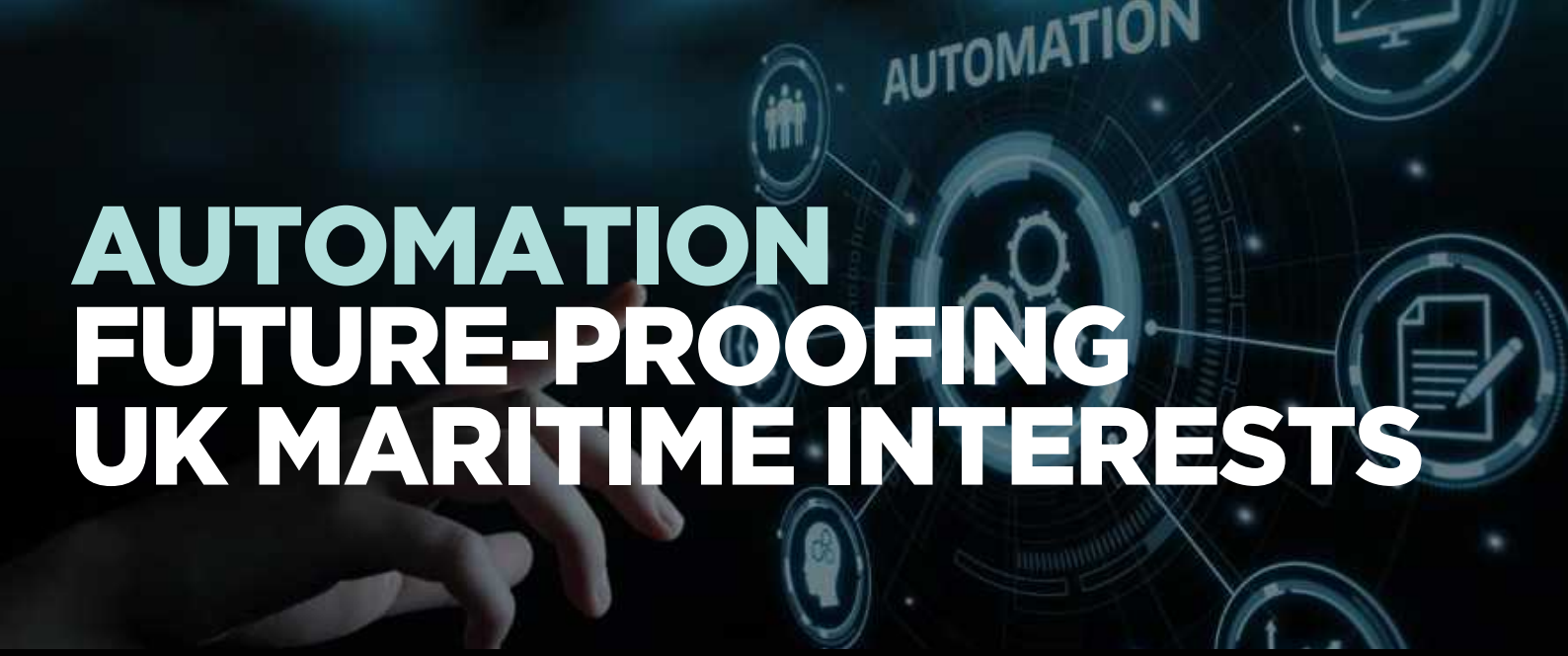
The ‘human factor’ is your biggest vulnerability to cyber crime.

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



AUTOMATION FUTURE-PROOFING UK MARITIME INTERESTS

During January the UK Maritime Minister Nusrat Ghani completed a tour of southern ports 'to see the innovative work underway to future-proof the maritime industry', referring to the British investment in automation. In the same month the Norwegian Kongsberg Group was granted funding from the EU's horizon 2020 research programme to test autonomous technology on vessels in operational use. Automation is round the corner.

Logically it is the next step for global trade. As seaborne-trade is predicted to rise by nearly a third by 2030, the increase in offshore traffic will be much higher, as will associated risks (90% of marine casualties and incidents are caused by human error). Automated, unmanned ships may be the safest option going forward, although only when supported by sufficient and strong technology, for example with the roll-out of 5G.

Taking crew off ships would have further benefits to the industry, many financial. Rolls-Royce stated that 'Many facilities and systems on board are only there to ensure that the crew is kept, fed, safe and comfortable. Eliminate or reduce the need for people, and vessels could be radically simplified'. Studies show removing accommodation infrastructure would save 6% in fuel and 5% in construction costs, while simultaneously releasing more space for cargo and income.

Therefore investment in autonomous technology is essential and inevitable. In the UK there are plans developing for an autonomous ship to sail independently across the Atlantic for the Mayflower's 400th anniversary. The maritime minister's meeting with MSubs, the company leading this transatlantic plan, drew attention to how 'such innovations could revolutionise the shipping industry by increasing safety, efficiency and delivering environmental benefits'.

However what of the cyber concerns about autonomous shipping?

While the technology is in its infancy, this question is being tentatively asked and just begetting more questions. The technology will be reliant upon constant ship to shore communication – will this make it more vulnerable to cyber-attack? How would you solve a cyber-attack on an unmanned vessel? What could its potential impact be? How would you know that an unmanned vessel has been hacked – could it send false data to hide its intent?

These are questions that will need answering in tandem as the technology progresses and we creep closer to it being in operational use. Therefore Be Cyber Aware At Sea are pleased to note that as part of the same tour, the UK maritime minister visited the MARLab which is currently developing ways to better regulate 'smart' and autonomous shipping, so these state-of-the-art developments can be utilised by UK shipping. It is hoped the work at the MARLab will form the foundation for the future regulation and legislation of this fast-moving industry. Let us hope this combination of innovation with caution is continued over the next decade – it is the true definition of future-proofing.

https://shipinsight.com/articles/norwegian-autonomous-ship-project-gains-eu-funding
https://seanews.co.uk/features/artificial-intelligence-and-the-era-of-autonomous-shipping/
https://www.gov.uk/government/news/maritime-minister-undertakes-future-of-shipping-industry-tour-as-ports-cyber-security-guidance-is-updated
https://www.dnvgl.com/to2030/impact/impact-on-maritime.html

NEW PORT GUIDELINES FOR UK SHIPPING

In January the UK Department for Transport released a fresh cyber security code of practice, focusing on ensuring that UK ports remain among the safest in the world.

The guidance helps ports develop cyber security assessments, allowing them to effectively identify gaps in their security, while also providing advice on managing cyber security attacks, and clarifies points raised by the industry from previous iterations. It should be used in conjunction with the 2017 publication 'Code of practice: cyber security for ships'.

CENTRAL THEMES IN THE GUIDE INCLUDE:

* Developing a cyber security assessment and plan for important assets, processes and potential vulnerabilities
* Devising the most appropriate mitigation measures
* Having the correct governance structures, roles, responsibilities and processes
* Handling security breaches and incidents
* Highlighting national and international standards used and the relationship to existing regulation

The guide stresses that 'Cyber attacks on port systems are no longer considered hypothetical or simply the stuff of fictional narrative' and that the consequences of failure to address the cyber risks are serious, from injury or fatality to reputational damage, financial penalties or litigation.

The guide arrives in the wake of several reports of cyber attacks on port facilities including the Ports of San Diego and Barcelona, making this a timely update.

Ports and the wider maritime industry will have access to the new and improved guidance, helping these vital transport hubs remain secure from 21st century styles of attack.

You can view the UK's Port and port systems - cyber security code of practice here:

https://www.gov.uk/government/publications/ports-and-port-systems-cyber-security-code-of-practice

https://www.gov.uk/government/news/maritime-minister-undertakes-future-of-shipping-industry-tour-as-ports-cyber-security-guidance-is-updated

The guide stresses that 'Cyber attacks on port systems are no longer considered hypothetical or simply the stuff of fictional narrative.'

MARITIME INDUSTRY NOW A MAJOR TARGET FOR COMPUTER CYBER ATTACKS

Major advances in the rapidly changing maritime industry have made this area a top target for an increasing number of sophisticated cyber criminals. Their computer attacks are threatening vessels and ports that facilitate 95% of all UK trade – totalling around £500 billion.

Says Rick Flood, managing director of leading cybercrime firm Falanx Cyber, part of the Falanx Group: 'We are regularly seeing reports of ransomware attacks. These are where computer systems are compromised and payments – often extortionate – demanded to unlock them'.

Just over a year ago, for instance, shipping giant Maersk experienced such a breach and the damages were estimated at $250 – $300 million. Last year Norsk Hydro, one of the world's largest aluminium producers with a substantial shipping division, also fell victim to a new strain of ransomware. It's reported that this cost its business $52 million in the first quarter. There are many such recent examples across the world, including the USA and Australia, and these will only accelerate.

'The price of building an effective in-house cyber security solution is high and time-consuming – recruitment, staff retention and the costs related to locating those staff, the software and technologies they need to be effective are significant. Not everyone has that spending power. Operators are already conscious of the cost of both IT and Telecoms in the sector and would need to add a lot of specialist knowledge, which is currently a very scarce and expensive resource. More and more companies are falling victim to cyber-attacks so Falanx has introduced its shared Managed Detection and Response (MDR) Service for the maritime sector to help protect these targets.'

Basically, at an affordable price, this service works as an extension of a company's IT and Cyber teams. It provides highly skilled security experts, leading edge technology and rapid cyber incidence response, delivered from its UK-based Security Operations Centre. It works around the clock watching for signs of a cyber-attack before they occur. It employs advanced behavioural and endpoint analytics to hunt for unknown threats before they can gain a strong hold on a company's environment. It also ensures clients conform to NIS and GDPR regulations.

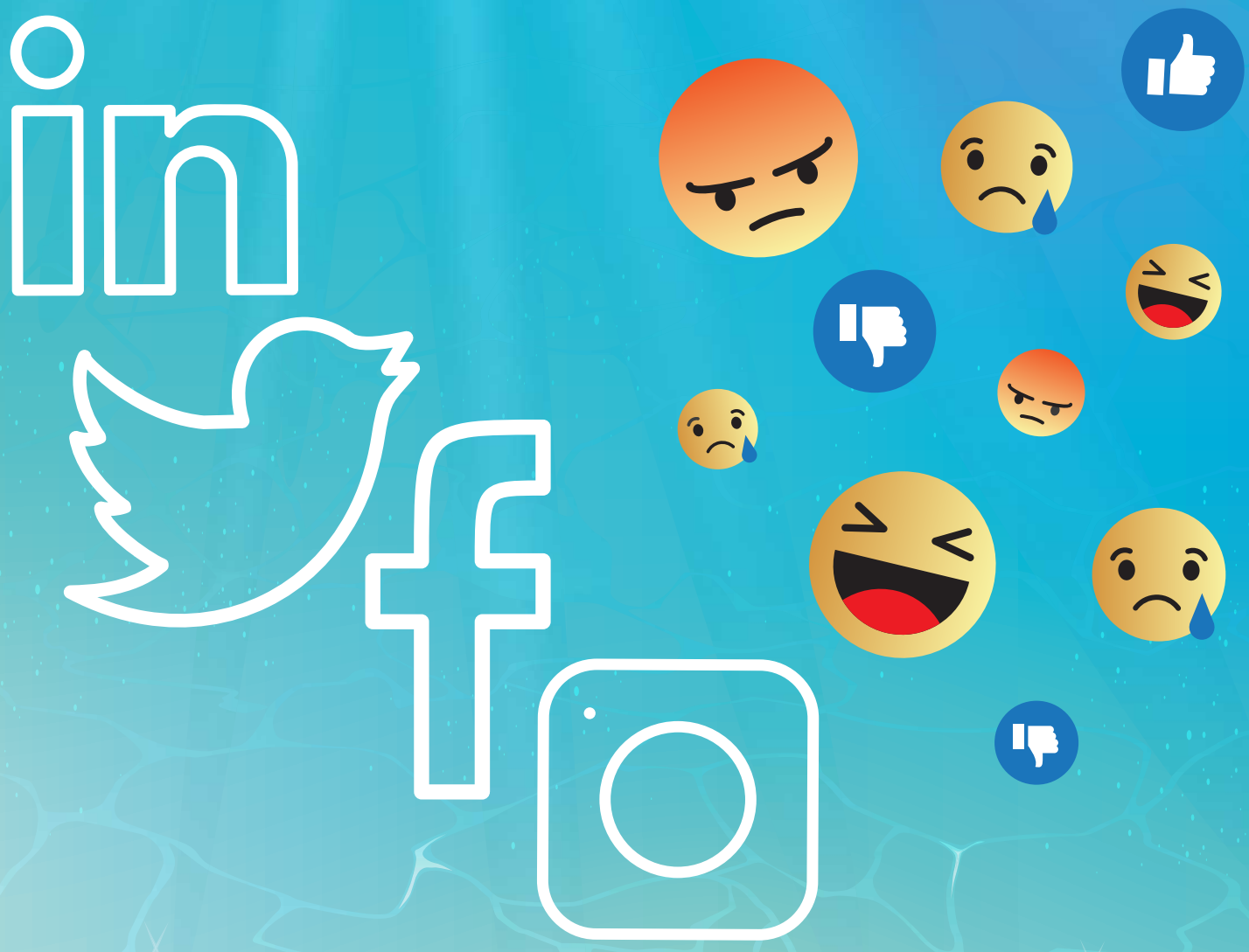
Says Flood: 'Cyber criminals are continually growing in sophistication – and in lucrative areas such as maritime they are becoming increasingly greedy. The industry should be aware of this – and take appropriate action.

https://www.directorstalkinterviews.com/maritime-industry-now-a-major-target-for-computer-cyber-attacks/412804217

BE CYBER AWARE AT SEA

SOCIAL MEDIA

ONCE SAID, THE WEB IS FED



EVERY THING YOU POST IMPACTS ON YOUR PERSONAL BRAND!

THINK. HOW DO YOU WANT TO BE KNOWN?