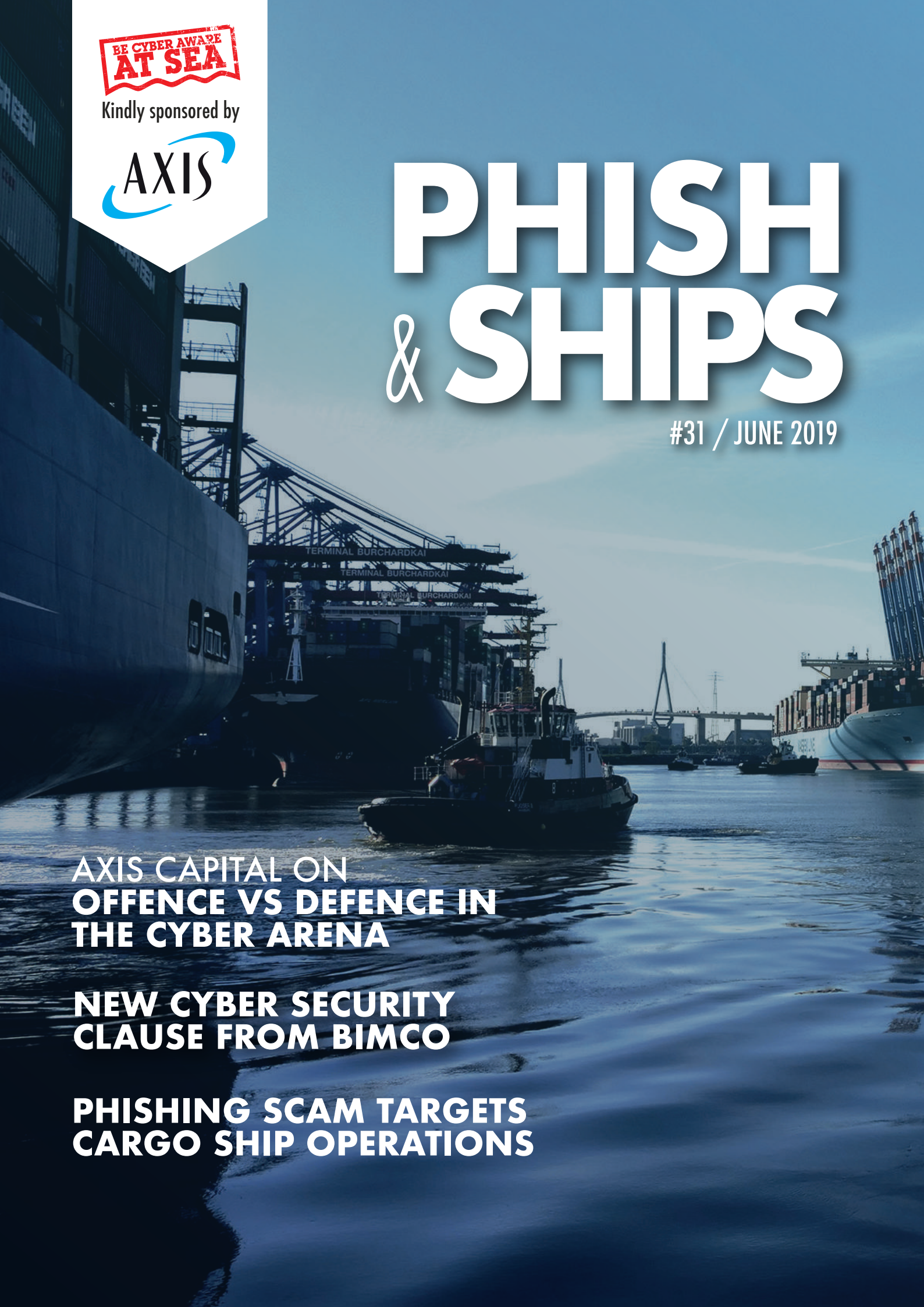
BE CYBER AWARE AT SEA

Kindly sponsored by

AXIS

PHISH & SHIPS

#31 / JUNE 2019



AXIS CAPITAL ON
OFFENCE VS DEFENCE IN THE CYBER ARENA

NEW CYBER SECURITY CLAUSE FROM BIMCO

PHISHING SCAM TARGETS CARGO SHIP OPERATIONS

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.

As you will read in AXIS' article this month, cybersecurity has many parallels with a warzone, with firms building their defences to repel the attacking invaders.

How nice then, to report simultaneously of several positive developments that will help reinforce the barricades in such different ways. BIMCO continue to lead the ground with their new Cyber Security Clause that will support organisations in their planning for security breaches. Meanwhile as Singapore's Maritime and Port Authority opens a Cybersecurity Operations Centre, we hope that this will show that collaboration between all aspects of shipping will be an integral part of global protection.

Cyber criminals are seeking to attack from any possible angle, so cybersecurity must be multifaceted to provide full cover from the incoming fire. Be Cyber Aware At Sea is with you, every step of the way.

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

NEW CYBER SECURITY CLAUSE FROM BIMCO

BIMCO's Documentary Committee has agreed a new standard Cyber Security Clause that 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.

In the wake of recent costly cyber security incidents involving large shipping companies, cyber security has become a major focus in the maritime industry.

BIMCO has taken a lead position on cyber security issues through its active role at the International Maritime Organization and by co-authoring the "Industry Guidelines on cyber security onboard ships". The development of the BIMCO Cyber Security Clause has been an important part of this initiative.

The clause has been written by a small drafting team, led by Inga Frøysa of Klaveness, with representatives from shipowners, P&I clubs and a law firm, and was published towards the end of May.

"I am very pleased to see BIMCO as the first mover on this important topic. Recent years have shown that there is a clear need for a clause addressing the contractual issues that can arise from a cyber security incident," says Inga Frøysa.

SHARING RELEVANT INFORMATION

The clause is drafted in broad and generic language which allows for it to be used in a wide range of contracts and in a string of contracts for easy back-to-back application. It is hoped that the clause will assist parties in obtaining affordable insurance for their cyber security exposure, as the clause introduces a cap on the liability for breaches.

"It was very important to the subcommittee to impose an obligation on the parties to keep each other informed if a cyber security incident should occur, and to share any relevant information, which could assist the other party in mitigating and resolving an incident as quickly as possible," Frøysa says.

This is done through a two-fold notification process. Firstly, through an immediate notification from the party who becomes aware of an incident to the other party. Secondly, through a more detailed notification once the affected party has had the chance to investigate the incident.

The clause also requires the parties to always share subsequent information, which could assist the other party in mitigating or preventing any effects from the incident.

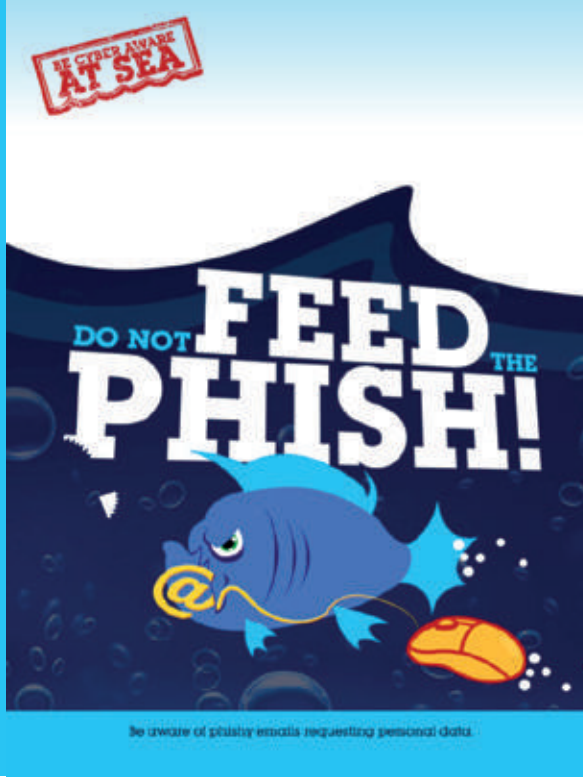
The level of required cyber security will depend on many elements such as the size of the company, its geographical location and nature of business.

The clause takes this into account by stipulating that the parties must implement "appropriate" cyber security. The clause also requires each party to use reasonable endeavors to ensure that any third-party providing services on its behalf in connection with the contract, has appropriate cyber security.

https://www.hellenicshippingnews.com/new-cyber-security-clause-from-bimco

PHISHING SCAM TARGETS CARGO SHIP OPERATIONS

Email phishing tactics have been added to the list of methods being used by outsiders to hack into commercial cargo vessel operations and navigation information, maritime regulators report.



According to a safety bulletin published by the U.S. Coast Guard (USCG) on May 24, "adversaries are attempting to gain sensitive information including the content of an official Notice of Arrival (NOA)" in requests that use email addresses posing as official Port State Control (PSC) authorities. Foreign vessel operators are required to file NOAs at least four days in advance of arrival at a U.S. port to allow the USCG to prioritize vessel inspections.

In addition, the agency said it also recently received reports of malware "designed to disrupt shipboard computer systems." A malware attack was used by hackers to infiltrate the operations of container shipping giant Maersk two years ago, which ended up indirectly affecting FedEx [NYSE: FDX].

Vessel operators and land-side ship company managers should be verifying the validity of email senders before responding to unsolicited emails, the USCG asserted in the bulletin. "If there is uncertainty regarding the legitimacy of the email request, vessel representatives should try contacting the PSC authority directly by using verified contact information," it recommended. "Additionally, vessel owners and operators should continue to evaluate their cyber defense measures to reduce the effect of a cyber-attack."

Despite the latest attacks, the USCG noted that vessel masters have been reporting suspicious activity to its National Response Center, in accordance with federal regulations, which is helping the agency to identify and counter cyber threats around the world. Coast Guard officials were not immediately available to provide more details on the latest cybersecurity attacks.

U.S. Representative John Garamendi (D-California), a member of a subcommittee that oversees the U.S. Coast Guard, said at a public forum in April that there is not enough attention being paid to the growing cyber risks in the maritime sector, including the spoofing of vessel GPS devices.

The USCG warned in October and November of 2018 that "significant" GPS interference continues to be reported by vessels operating in the eastern Mediterranean Sea, concentrated near Port Said, Egypt; the Suez Canal; and near Jeddah Port, Saudi Arabia. "This interference is resulting in lost or otherwise altered GPS signals affecting bridge navigation, GPS-based timing and communications equipment," the agency stated at the time.

Apart from the most recent safety bulletin warning of the renewed threats, the USCG is attempting to address cybersecurity vulnerability by sharing prevention procedures with maritime companies, as outlined its four-year (2018-2022) strategic plan. As part of a directive from the International Maritime Organization, it will also ensure that shipowners address cyber risks within their vessels' safety management systems by 2021.

https://www.freightwaves.com/news/phishing-scam-targets-cargo-ship-operations

BE CYBER AWARE AT SEA

Kindly sponsored by AXIS

OFFENCE VS DEFENCE IN THE CYBER ARENA

Cyberspace. Who holds the upper hand - defenders or attackers?

Consider this context: a rough rule of thumb in military circles is that an attacker needs a 3 to 1 advantage in manpower and firepower in order to successfully defeat a defender. Defenders, not attackers, typically have an advantage because it is normally easier to protect and hold than it is to move forward, to destroy and to take.

Yet, in cyberspace, the consensus view is that attackers have an enormous advantage, maybe by a factor of as much as 10 to 1 according to some. There are several reasons for this advantage. The internet was primarily designed to be easy to use - with security very much an afterthought. The initial objective was to share information, not to prevent its flow. As a result, malicious actors can exploit a tremendous number of vulnerabilities.

Today, large institutions such as banks must defend against thousands of attacks daily. Only one needs to get through for an attacker to succeed. Generally speaking, offensive cyber attacks are low cost and high payoff, a key reason for the extraordinary growth in cybercrime.

Further, the complexity of modern software and IT systems hands the advantage to the attacker. Both the attacker and the defender are in a race to find vulnerabilities; the attacker to exploit them and the defender to patch them. But, the number of vulnerabilities grows exponentially with the size and complexity of the system. The defender has little chance of finding every single vulnerability and patching it before the attacker finds one to exploit.

On the other hand, it is not all doom and gloom. The line between attack and defence is often a blurred one. Offensive techniques can be used for defensive purposes since the skill sets required are the same. Malware becomes obsolete quickly (hence the value of zero day exploits) and once it has been identified it can be rapidly defeated.

The evolutionary arms race between attackers and defenders is developing extremely fast with some notable successes on the defender's side. Progress in techniques like two factor authentication, password managers and keychains, disposable 'one-off' credit cards, cloud computing and faster patching cadences are beginning to redress the balance in favour of the defender.

While there can never be a system that is completely invulnerable to attack, organisations with good cyber hygiene, educated users and well-configured systems can increase an attacker's costs significantly.

Cyberspace is a shared space and the more that defenders co-operate with each other the safer the whole community will be. Traditional warfare is all about having the biggest gun or the fastest jet. In cyberspace, defence is more about best practice than best products.

Artcile by John Donald, Cyber Adviser as AXIS Capital.

AXIS Capital is a global provider of specialty lines insurance and treaty reinsurance and a Phish & Ships sponsor.

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

AON, HUDSON CYBER TEAM FOR MARITIME CYBER SECURITY

Aon and HudsonCyber are joining forces to provide enterprise-level cyber security capability assessment, integrated cyber breach response, and mitigation support to the global marine industry.

“We see a real need for collaborative thinking in respect of an enterprise level cyber security methodology for our clients," said Lee Meyrick, CEO of Global Marine at Aon. "It is important to understand cyber risk exposures, mitigation strategies and maximizing the effectiveness of their programs.”

Bringing together Hudson’s HACyberLogix cyber security assessment program and Aon’s cyber risk transfer, incident response, and mitigation services, this collaboration is designed for the unique requirements of the global marine industry.

The HACyberLogix platform provides decision-makers with an enterprise view of their organization’s cyber security capabilities and prioritized recommendations to support enterprise risk management investment planning and resource allocation.

“From a cybersecurity standpoint, the maritime industry is an underserved market," said Jason Hogg, CEO of Cyber Solutions at Aon. "Our collaboration with HudsonCyber will enable us to create a cohesive cyber security program for their clients around the globe. Together, we will help clients understand and mitigate their cyber risk, as well as act immediately to help them recover if an incident occurs.”

“We've been working closely with Aon's Global Marine Specialty and Cyber Solutions Group to deliver a maritime cyber offering which melds Hudson’s 35 years of maritime risk management expertise and performance with Aon’s cyber insights and capabilities," said Cynthia Hudson, CEO of HudsonAnalytix.

"Our integrated approach will provide the maritime industry with an unprecedented opportunity to implement a cyber response in an accelerated, disciplined, and comprehensive fashion, helping to mitigate damages arising from a cyber incident.”

https://www.maritimeprofessional.com/news/hudsoncyber-team-maritime-cybersecurity-345529

EVENT... MARITIME CYBER RISK MANAGEMENT FORUM 2019

Date And Time: Tue, 25 June 2019 / 08:00 – 19:30 BST

Location: Norton Rose Fulbright, 3 More London Riverside, London, SE1 2AF

Interactive maritime industry engagement on cyber risk management and security.

The Maritime Cyber Risk Management Forum engages those with frontline responsibility for maritime cyber security, from boardroom through to the back office, from superintendent to seafarer, from insurer to IT responsible, to update themselves on regulation, best practice and the latest products and processes in cyber security risk management.

PROGRAMME OUTLINE

Session One: Regulations, compliance and risk management.

Session Two: A view from shipowners and ship operators.

Session Three: Cybersecurity incident simulation exercise.

Session Four: Threats to cybersecurity in ports.

Session Five: How to prevent cyber attacks from happening?

Session Six: Riviera maritime media cyber security hub.

For further detail on the sessions and days agenda, please visit:

https://www.shipcybersecurity.com/programme.htm

TOP DOWN OR BOTTOM UP?

We need strong cyber resilience in the maritime sector, but where should we begin to make changes?

Professor Keith Martin from Royal Holloway, University of London recently proclaimed ahead of the Maritime Cyber Risk Management Forum, in which he will sit on the panel, that: "Cyber security needs both a 'bottom up' and 'top down' approach".

He could not be more right; achieving strong cyber resilience throughout the industry requires a pincer movement in the creation of a knowledgeable and savvy workforce operating in companies more attuned to the risks and invested in prevention, striving to meet tighter and more realistic worldwide regulations.

Central to the bottom up approach is that personnel present the greatest risk to cyber security. This is the opinion of Be Cyber Aware At Sea yet, most crucially, we also see personnel as the easiest risk to remedy through education to improve cyber hygiene. Changing simple habits, being ever aware of the risks and knowing the procedures to react correctly and safely will help to limit the careless mistakes that account for so many cyber incidents.

For Professor Martin, this is not the whole picture: "I think the bigger mistake is to design a system that does not take the likelihood of human error into account." He is correct of course; if personnel are considered the greatest threat to cyber security then protection should be in place from top down to account for this. This may include cyber training for staff, investing in more secure IT systems, software and hardware, or establishing dedicated cyber teams to take responsibility.

Professor Martin also makes the case for the maritime sector being a fundamentally difficult sector to cyber-proof. By its nature maritime cyber security has many fronts in which to maintain a defensive position. From onboard the ship, across a fleet, the offices ashore, the data-networks in between and the companies they interact with on a daily basis, each presents a different perspective and opportunity for a cyber criminal to attack. Prof Martin also highlights "widespread use of legacy equipment and the dynamic nature of staffing on board vessels" as being inherent weaknesses in the industry.

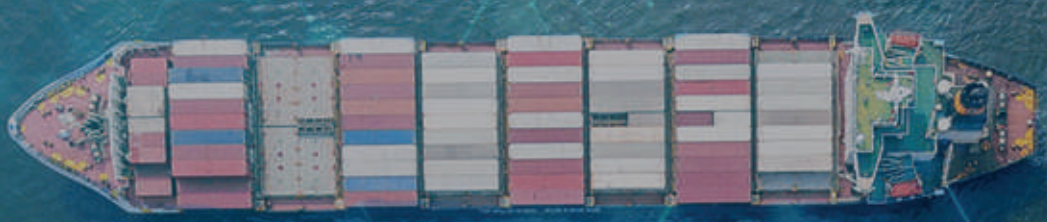
All this means that the maritime industry has to have a dynamic multifaceted approach to cyber security. Regulatory bodies should be upholding tighter standards that enforce cyber resilience while companies should be examining every potential weak surface point and investing in their preventative security and backup procedures should they suffer a breach.

What is most notable for the industry to realise is that they cannot pick one approach but must commit to several to ensure effective security. Everyone is a stakeholder in this industry, it must matter to all that security is upheld.

https://www.marinemec.com/news/view,original-insights-on-maritime-cyber-security_57822.htm

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

MPA OPENS MARITIME CYBERSECURITY CENTRE

The Maritime and Port Authority of Singapore (MPA) has opened a Maritime Cybersecurity Operations Centre (MSOC). Operated by ST Engineering in its hub, MSOC will conduct 24/7 monitoring and correlate data activities across all maritime Critical Information Infrastructure (CII).

It can also analyse activities in the IT environment and detect and monitor cyber-attacks. By detecting anomalies and threats, the centre can also respond to the cybersecurity incidents using available technology solutions.

and port critical infrastructure to prevent a major disruption to port operations and delivery of services. MPA has introduced other initiatives to strengthen the cybersecurity readiness of the maritime sector."

In addition to MSOC, MPA has introduced other initiatives to strengthen the cybersecurity readiness of the maritime sector.

MPA developed a new one-day Maritime Cybersecurity (Intermediate) Training Course in collaboration with Singapore Shipping Association and Singapore Polytechnic for maritime personnel to enhance their knowledge in managing cyber threats and challenges.

"As the world's busiest transhipment hub, it is important that we safeguard our maritime and port critical infrastructure."

- Niam Chiang Meng, Chairman, Maritime & Port Authority of Singapore

MSOC is aimed at strengthening the maritime cybersecurity posture in Singapore through early detection, monitoring, analysis and response to potential cyber-attacks on maritime CIIs.

MPA will be able to work with CIIs to ensure their protection and investigate any cybersecurity threat or incident. In order to respond to cyber incidents in a timely manner, MPA will also build key data linkages between MSOC and Port Operations Control Centre.

Maritime and Port Authority of Singapore chairman Niam Chiang Meng said: "Cyber threats come in many forms and have been rising steadily across the globe. As the world's busiest transhipment hub, it is important that we safeguard our maritime

It also partnered with the Singapore Maritime Institute and local institutes of higher learning on a Maritime Cybersecurity Research programme that focuses on the protection of shipboard systems to mitigate cyber threats.

This is an excellent move forward in combating the threat of cyber risks in shipping. The MSOC will stand to help prevent, detect and respond to cyber attacks. Here at the Be Cyber Aware at Sea campaign, we're delighted to see that the MPA have developed training to support and enhance their overall cyber programme.
A great move!

https://www.ship-technology.com/news/mpa-maritime-cybersecurity-centre/

BE CYBER AWARE AT SEA

SAFE & SECURE WEB BROWSING

A GREEN locked padlock and the 'S' in HTTPS represents security. Its implementation by website owners is leading to a safer and more secure browsing experience.

WHAT IS BIG DATA?

Along with AI, big data is a key phrase bandied about in any discussion about how technology is changing the way we do business in the maritime sector. But what is big data and how is it vulnerable to cyber attack?

In a sense big data is literally a term to mean a large amount of data, although large to a degree that it is almost impossible to store and process by normal means. The collection of vast swathes of data is made possible by the growth of technology throughout all aspects of industry and so is set to escalate. The industry is already reported to generate 100- 120 million data points every day which includes information gathered from ports and vessels.

How is Big Data of value?

Most importantly, big data means big data analytics – this is the unlocking of the potential of data and is where its value lies to the industry. Its key utility is in identifying industry efficiencies to improve performance but it has widespread benefits from ship owners, ship charterers to ports.

For example, a ship owner may use big data to examine the efficiency of its schedules to fit in with supply lines, to consider what cargo to transport, when and how, and with what fuel consumption to keep costs down; and use big data to create better, more efficient ships for their needs in future.

A charter company may use big data to locate where relevant boats are at any time around the world and where they are going and with what cargo, in order to better select the right boat for the right price for their needs and timescale.

Ports also use big data. For example, Singapore Maritime and Port Authority uses big data to develop traffic protection tools, taking into consideration all the comings and goings of their port against weather data and incidents, allowing them to detect unusual behaviour and protect the fleet.

The potential value of data analytics is considerable: Eniram implemented data analytics in 12 cruise ships and found they could make 4% annual savings of $12 million.

Where do the problems lie?

The usage of big data has been tried and tested in other industries but has been slow to grow in maritime, even though a 2016 survey by Sea Asia reported 81% of respondents saw its importance to the industry. As it grows in importance and becomes increasingly relied upon throughout the industry, the time to consider its vulnerabilities is now.

The biggest issue with big data is in the quality of the data collected. According to DNV GL, in 2017 in the US alone, bad data cost businesses 3.1 trillion USD. From a cyber security perspective, when huge decisions are made based on the data collected, the worry is that a hacker could insert seemingly innocuous information to large detrimental effect, like the butterfly and the hurricane. The very process of collecting so much data also opens the industry to cyber-attack. Constantly monitoring all the critical infrastructure means constant connections, particularly between shore and sea, and the threat vectors rise proportionately. When we consider that big data has such open-ended value to the industry, the concern is that maintaining access to the data trumps security. That cannot be the case. We need to ensure network security on this vast scale before uploading, and prevent security problems at source.

When an industry comes to rely on data in the way in which shipping is predicted to, the integrity of that data and trust in it, is as important and valuable as the data itself.

https://www.patersonsimons.com/wp-content/uploads/2018/06/TMS_SmartPort_InsightBee_Report-to-GUIDE_01.02.18.pdf
http://orbit.dtu.dk/files/156025857/Lagouvardou_MScThesis_FINAL.pdf