BE CYBER AWARE AT SEA

Kindly sponsored by AXIS

NEW FOR 2019

PHISH & SHIPS



AXIS DELIVER... UNDERSTANDING CYBER SECURITY & INSURANCE

EPSCO-RA: WHY COMPANIES RESIST PENETRATION TESTING



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.

There have been some exciting developments in the industry, not least our headline sponsor AXIS delivering the first Maritime specific Understanding Cybersecurity & Insurance course, aimed at insurance brokers and risk managers.

We all have a duty to understand cybersecurity better and the sure fire way to do that is by communicating and sharing information – which is expressed by the US Coast Guard for the need for an Information Sharing and Analysis Centre (ISAC). It is a debate that we have been keen supporters of for a long time and one that our supporters, the CSO Alliance continue to lead the industry to date with their cybercrime reporting portal.

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

AXIS DELIVER ITS FIRST UNDERSTANDING CYBER SECURITY & INSURANCE COURSE FOR SHIPPING

BE CYBER AWARE AT SEA

Kindly sponsored by AXIS

Marine insurance brokers are asked increasingly by their shipping clients to explore the options that are available to them to help mitigate the impact of cyber attacks. With the IMO encouraging administrations to ensure that cyber risks are appropriately addressed by the 1st January 2021, mariners are especially keen to know exactly what the cyber threats are, how their business could be affected and how they can mitigate these risks.

From an insurance point of view, the two main areas of risk to consider are onshore and offshore:

ONSHORE risk is similar to the cyber threat facing any business. The primary concerns include the loss of income from business interruption, as well as the logistics of, and the expense incurred in, restoring affected systems and paying any extortion demands.

OFFSHORE risk is any risk occurring onboard the vessel that leads to a physical damage loss, from pilots using an infected USB stick which takes the system down leading to the vessel grounding, to the vessel system being maliciously attacked by a third party resulting in a collision. Of course, any cyber threat that could lead to physical damage to the vessel could also lead to costly business interruption and system restoration cost as well.

Over recent years, the marine insurance market has mainly been concerned with the offshore risk, and hence the CL380 Cyber Exclusion Clause has been added to Hull and Machinery Insurance policies in order to exclude the risk of physical damage caused by a malicious cyber attack. However, as paper charts have given way to technical onboard systems, thereby increasing the cyber risk, concerns have grown over the gap in insurance coverage created by the CL380 Exclusion. Equally, the cost of business interruption caused by a cyber attack is being increasingly felt in the maritime industry, and with tight business margins, owners want the reassurance of being insured.

Thought should go, therefore, to identifying and addressing the following three factors: the onshore and offshore risks facing maritime companies, the cyber security measures that can be taken to protect them from these risks and the potential use of risk transfer to minimize the cost of an attack.

In February, AXIS hosted our first maritime-focused 'Understanding Cybersecurity and Insurance' course in our London office. The aim of these courses is to educate marine hull brokers about the cyber-related risks that the maritime industry is facing which, in turn, will help them to be better placed to advise their clients. We shall continue to host such educational classes on marine cyber throughout 2019, and encourage you to reach out if you are interested in learning about upcoming course dates.



Sharif Gardner AXIS at Lloyds

If risk transfer is one of your intended strategies, your insurance broker should be able to advise you on the most suitable cover for your needs.



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	✓

Coverage is provided by an insurance company subsidiary of AXIS Capital Holdings Limited or by AXIS Syndicate 1686. AXIS Specialty Europe SE is regulated by the Central Bank of Ireland. AXIS Insurance Company, an Illinois property and casualty insurer, is licensed in all 50 states of the United States and the District of Columbia. AXIS Syndicate 1686 is managed at Lloyd's by AXIS Managing Agency Ltd. AXIS Managing Agency Ltd is authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority (Firm Reference Number 754962). AXIS Managing Agency Ltd is registered at Willkie Farr & Gallagher (UK) LLP, 'Citypoint', 1 Ropemaker Street, London EC2Y 9AW (company number 08702952). Coverage may not be available in all jurisdictions and may be available only through licensed producers.

The product information is for descriptive purposes only and does not provide a complete summary of coverage. Consult the applicable policy for specific terms, conditions, limits, limitations and exclusions to coverage.

DNV GL COMPLETES TYPE-APPROVAL OF NAVAL DOME'S CYBER PROTECTION SYSTEM



DNV GL CP-0231 is a type-approval programme developed using the international standard ISA/IEC 62443, security for industrial automation and control systems.

Type-approval consisted of verifying the security capabilities of the Naval Dome solution, including stringent penetration testing at DNV GL's laboratory in Trondheim, Norway.

Naval Dome is currently the only provider of cyber defence solutions to the maritime industry to have achieved Security Level 4 (SL4), the highest level of certification that can be awarded under the DNV GL rules.

DNV GL's global service line leader for cyber security Mate J Csorba said "We are very pleased to be able to award Naval Dome (ND) this certification. Our team supported them throughout the certification process, culminating in a four-day long test period, where ND demonstrated the cyber robustness of systems protected by their Secure Endpoint against a variety of methods commonly used by cyber attackers. This is the first time we have worked with a customer on SL4 and after a very intensive and co-operative process, we can verify that they meet the requirements set forth in the standard and our class programme."

Naval Dome chief technical officer Asaf Shefi said "DNV GL type-approval of the ND Secure Endpoint cyber security system is an important development for both Naval Dome and the global shipowning community. As the only cyber security provider to have achieved this level of certification, it delivers further confidence to shipowners that our system is verified to offer ships' systems a very high level of defence against cyber attacks."

> **"DNV GL type-approval of the ND Secure End-point cyber security system is an important development for both Naval Dome and the global shipowning community."**
>
> **- Naval Dome chief technical officer Asaf Shefi**

The Naval Dome Secure Endpoint system is a cyber defence system that encapsulates existing maritime OEM vendor software while adding a variety of advanced cyber security mechanisms.

The solution requires no changes to the original software, nor does it change the operation of the original equipment manufacturers' software.

This is a powerful advancement in helping shipowners separate the wheat from the chaff in terms of cybersecurity products. All too often the industry has become skeptical of vendors selling fear, uncertainty and doubt which has delayed the adoption of credible action amongst many in the industry.

https://www.marinemec.com/news/view,dnv-gl-completes-typeapproval-of-naval-domes-cyber-protection-system_56841.htm

DENMARK CRACKS DOWN ON MARITIME HACKERS

The Danish Maritime Authority (DMA) has unveiled a series of new navigation and cybersecurity regulations to protect its shipping and port operations, according to a statement.

The announcement follows the Cyber and Information Security Strategy for the Maritime Sector released by the Danish government in January 2019.

The DMA says its new Order will strengthen already existing legislation and that its principal purpose will be to protect the industry at large from cyber attacks.

A recent Port Technology technical paper looked at managing digital supply chain risk.

It will also comply with and implement the EU's Network and Information Security (NIS) directive, which came into force in 2018.

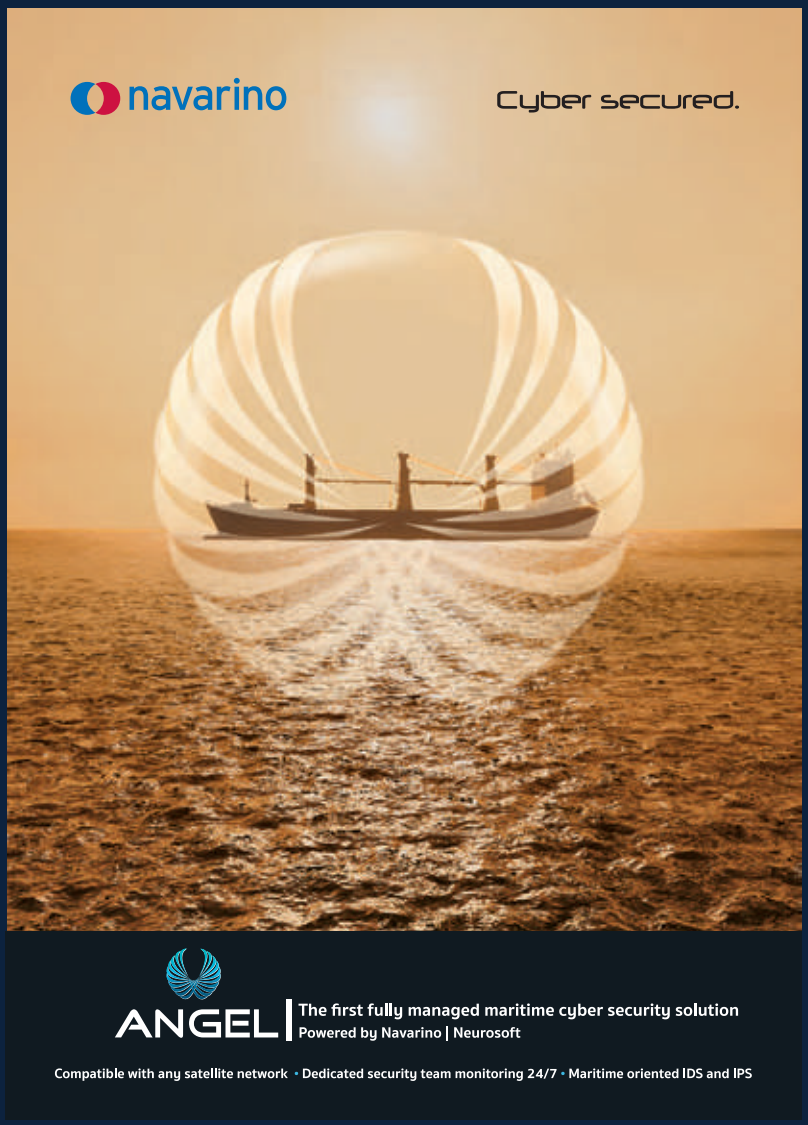
Furthermore, the new safety regulations will, according to the DMA, clarify EU and international cybersecurity regulations.

Part of the government's plan is to establish a Danish Maritime Cybersecurity Unit and create a single point of contact between maritime operators and the Centre for Cybersecurity.

As part of that, it hopes to spark increased awareness through collaboration and knowledge sharing in the maritime sector.

The team at the Be Cyber Aware at Sea Campaign will be keeping our eye on what Denmark are doing in this space.

It does appear that they are set to lead the way as a European nation in the fight against cybercrime. We have and will continue to advocate that awareness and collaboration is going to be vital in protecting the shipping and transportation industry.



https://www.porttechnology.org/news/denmark_cracks_down_on_maritime_hackers

MARITIME CYBERSECURITY
MORE IMPORTANT THAN EVER, BUT INDUSTRY ONLY TALKS ABOUT IT

Feds and private sector leaders in the maritime industry met recently to discuss cyber risks, but instead of making serious progress, the results were, as one expert put it, "like standing around a building that's on fire and talking about the infrastructure."

According to a new report provided to InsideSources, the National Maritime Intelligence-Integration Office (NMIIO) and the National Strategic Research Institute (NSRI) are in the middle of a study on cyber risks in the maritime industry, spanning February 2018 to August 2019, which will be presented to the Director of National Intelligence and the National Security Council.

Cybersecurity is a serious issue for maritime industries. Major ocean carriers like Maersk and COSCO and ports like the Port of Los Angeles and the Port of San Diego suffered severe cyberattacks over the last few years, temporarily crippling their supply chains and, in some cases, bringing the flow of goods to a halt.

The report from the workshop summarized by the NSRI shows participants skirted around the real issues and instead focused on coordinating responsibilities and information-sharing strategies.

In other words, they talked about getting work done, but didn't do any work.

It wasn't a total waste, however: Workshop participants agreed that the entire maritime supply chain should be up to date on cyber risks and cybersecurity initiatives, and determined that the biggest cyber risk within the maritime supply chain is third party vendors, like contractors and software providers.

In order for the maritime industry to really crack down on cybercrime, every link of the supply chain must augment its cybersecurity. One way to mitigate cybercrime is via information-sharing between the attacked entities and others within its supply chain. Information-sharing is standard operating procedure from a cybersecurity standpoint, and while it may conflict with privacy initiatives for industries dealing directly with consumers, within the maritime industry it makes sense.

But there's currently no straightforward way to do that, the report noted.

According to the report, "there is general consensus on two main points: 1. An Information Sharing & Analysis Center (ISAC) dedicated to maritime issues is beneficial because an ISAC provides anonymity to reporting entities, provides analytic horsepower to correlate events across the industry, and coordinates with appropriate government organizations to provide a bridge between industry and government. 2. There is need for clear and consistent direction on dissemination and reporting requirements/capability."

It appears the maritime industry's view is that more bureaucracy could streamline cybersecurity efforts. In Rice's view, this just shows how badly prepared US infrastructure is for cybercrime.

"The state of cyber resilience is one where people are aware of the issues, but performance is, what should we do about it? And I think if they were further along we'd see more discussion about vulnerability assessment and how to deal with problems then, what's the environment?" he said.

https://www.insidesources.com/maritime-cybersecurity-more-important-than-ever-but-industry-only-talks-about-it/

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

RELAX, THIS WON'T HURT A BIT

Let's implement regular penetration testing...

How many times have you heard that from your dentist? And chances are if you go to the dentist regularly, she's right, it won't hurt.

However, if you're one of those people who avoids the dentist until there is a problem you might not hear those words and if you do it's a lie... it's going to hurt... maybe a lot. It's going to hurt because you let fear win over something you know is the right thing to do. You may even understand that the fear is irrational. The irony is the fear of bad news or pain has virtually assured you will wind up in a position where pain is now the likely outcome. But why are we talking about dentistry in a cyber security column? Well, because it's a good analogy for the two main ways I observe companies approach penetration testing. It's either something they do regularly as a best practice or something they dread and avoid. At least until they're in some sort of trouble.

Like going to the dentist, a penetration test is typically performed once per year. And to be clear, I'm referring to network penetration tests not application penetration tests which are more connected to devops than any set frequency. Unlike going to the dentist, a penetration test is usually a bit different each year, at least it should be. There's no point in testing something you know hasn't changed or has matured to the point where previous test methodologies are not going to tell you anything you don't know, or you haven't already documented.

By testing regularly, you gain valuable insight into what is working and what isn't, where you're succeeding and where you're failing, what your gaps are and in what order you should address them. You document your success and identify opportunities for improvement. Ideally, this leads to an increasing security posture and a documented suite of security controls that are proven to function. Even when you have been doing penetration testing for many years and there are no more big gains, you start to work on refining processes to make them more efficient. There really isn't a down side and companies that embrace the process actually look forward to the testing.



They are looking for the ideas for improvement or proof an improvement or control had the desired effect. Like people who regularly go the dentist they enjoy that clean teeth feeling you can only get after your checkup.

Now, you can't reason someone out of a position they weren't reasoned into in the first place, so there will always be people who just resist the idea of third-party penetration testing. I've never truly understood why as it seems illogical or at least counterproductive. In most cases I suspect it is fear of facing a weakness or looking "bad". This of course doesn't make sense, if you have a weakness you should want to identify it, acknowledge it and fix it. To pretend it doesn't exist or not test because you don't think you have any weaknesses is folly of the highest order. To suggest that testing or proving something works the way you think it does, is unnecessary in something as critical as cyber security is at least dangerous and perhaps incompetent. Like the person who won't go to the dentist for fear of pain, failing to test, to look and understand will ultimately result in a painfully expensive incident.

Fortunately, resistance to the concept of penetration testing, like the concept of going to the dentist, is usually overcome in the long run. Once you go through the process once or twice you realize that it's usually not painful and you learn a lot. Your cyber security posture, like your smile, will improve over time.

So stop putting it off, stop being afraid and relax... this won't hurt a bit.

By Gideon Lenkey

BE CYBER AWARE AT SEA

MALVERTISING

"MALICIOUS ADVERTISING"

Typically involves injecting malicious or malware-laden advertisements into legitimate online advertising networks, pop-ups and webpages



USCG INFORMS MARINERS HOW TO REACT ON CYBER ATTACKS

US Coast Guard published a Bulletin concerning a cyber incident that occurred on a commercial vessel. The paper aims to inform possible victims how to prevent cyber attacks and also provides additional information on who to inform if one is under attack.

On January 26, 2019 the vessel received an e-mail according to which an individual or entity would present an official port state control body. Specifically, the e-mail originated from an email address 'port@pscgov.org' and was sent to the Captain of the vessel asking for detailed information for the vessel, its cargo and its crew.

The master of the vessel was doubtful of the email and activated elements of the vessel security plan related to suspicious cyber attacks.

Moreover, the Captain forwarded the email to the USCG Captain of the port for investigation and feedback.

Mainly, USCG states that "Reporting Suspicious Activity and Breaches of Security" outlines the criteria and processes for Maritime Transportation Security Act (MTSA) in order to report suspicious activity (SA) and breaches of security (BoS).

Also, USCG's National Response Centre (NRC) remains the primary contact for notifications concerning SAs and BoSs, including cyber.

Concluding, members can report possible attacks at National Cybersecurity and Communications Integration Centre (NCCIC).

Information sharing through platforms such as the CSO Alliance Maritime Cybercrime Reporting Portal is a great step for a non-governmental approach to reporting cybercrime globally.

The reality is now that as an industry shipping must stand on its own two feet and develop processes to effectively train up employees onshore and at sea to report incidents and escalate them. This is why the Be Cyber Aware at Sea campaign is obsessive about training and awareness.

REMEMBER DO NOT 'FEED THE PHISH'



https://safety4sea.com/uscg-informs-mariners-how-to-react-on-cyber-attacks/

PHISH & SHIPS

TOP OF THE CLASS:
HOW CLASSIFICATION SOCIETIES ARE ADAPTING TO CYBER

As the industry continues on its fast-paced journey to embrace cyber technology, what about the guiding hands of the classification societies?

Recently, these bodies have been detailing how they are also having to change in order to better serve the increasingly digital maritime industry, and how they are expanding their services to take into account the security concerns of cyber technology.

The role of the classification society is to ensure 'continued safety and security of the maritime domain with respect to the vessels and the various marine aiding constructions'.

As the landscape of the maritime domain alters, the safety and security parameters alter too, most notably with regards to cyber technology, highlighted by Knut Orbeck-Nilssen of DNV GL as one of the three key factors affecting the industry today.

For Knut, the classification societies have a key role here. DNV GL released 'Cyber Secure' class notations in 2018, and dispense practical advice aimed at 'demystifying the subject'.

They offer classes on cyber threats and even retain 'certified ethical hackers' to find weaknesses in systems in order to protect them longer term.

DNV GL have also adapted to serve their digitally minded clients by using technology themselves, such as with Veracity, launched in 2017. This is a digitised, automated system which collects and verifies data for the EU MRV scheme. For DNV GL, digital technology can support the industry, reducing the potential for human error, while extracting the maximum value from data to improve safety, performance and efficiency.

DNV GL is not the only society ahead of the curve; recently Matthieu de Tugny, Bureau Veritas' new executive vice president for maritime and offshore, declared that "if we don't invest in digitalisation we will not survive as this is part of the industry's transformation".

Accordingly, Bureau Veritas has also been leading the way, offering a number of services digitally, including requesting class surveys, accessing smart checklists for preparing vessels and managing fleet readiness and compliance. Like DNV GL, they also take seriously the potential for cyber threats, hiring fresh teams of IT and cyber security experts as well as offering notations for cyber secure ships.



Links and further reading:
https://www.marineinsight.com/maritime-law/the-importance-of-classification-societies-in-the-maritime-industry/
https://www.marinemec.com/news/view,class-must-invest-in-digitalisation-to-survive_56534.htm
https://www.hellenicshippingnews.com/knut-orbeck-nilssen-dnv-gl-ceo-maritime-maps-out-how-class-can-help-maritime-navigate-the-new-digital-reality/