PHISH & SHIPS

BIGGER AND BETTER FOR 2018!

#14
JAN: 2018

BE CYBER AWARE AT SEA

HIGHLY COMMENDED, SAFETY AT SEA AWARDS 2017
BEST CYBER AWARENESS CAMPAIGN, INTERNATIONAL CYBER SECURITY AWARDS 2017

Kindly sponsored by

CSO ALLIANCE
MARITIME
Welcome to a new year and a new issue of “Phish & Ships”, the maritime cyber security newsletter, keeping you up to date with the maritime and offshore industry initiative, “Be Cyber Aware At Sea”.

Inside issue 14, we look at the issues which will likely be shaping the shipping industry's response to maritime cyber security risks in 2018. One of the key problems has long been reporting - so we are pleased to share news of a major new development from our supporters at CSO Alliance.

Like many governments, the UK has seen the potential that cyber risks posed to national security, and across various departments they have been ensuring that the mantra of “defend, deter and develop” has been heard and enacted. Inside you can read more of what has been done, and what will be happening in the future.

Another concern for companies in 2018 is the arrival of new European Union data protection legislation. In a major shake-up, companies need to ensure they are doing what is required, or they could face huge penalties. Our good friends at Axis provide some valuable guidance in this issue.

With so much to share, we just want to wish you a safe and secure cyber year ahead. Thank you for your continued support.

See https://www.becyberawareatsea.com/ for more details.

CSO ALLIANCE: INTRODUCING THE MARITIME CYBERCRIME REPORTING PORTAL

We know there are significant problems with the reporting of maritime crime, and that a mechanism for the effective and rapid sharing of global cybercrime information does not exist. It can take as little as four days for a virus to spread across computer networks throughout the world. How can we begin to combat the rapidly evolving threats if we don’t have a maritime focused cybercrime reporting portal able to provide timely alerts.

CSO Alliance has partnered with Airbus to provide just such a Maritime Cyber Alliance to meet this need (https://www.maritimecyberalliance.com). In addition to cyber incident reporting and alerts, it offers free to use malware checking with articles, information on best practice, insights, and impact statements. It is currently in the pilot phase for the next few months so we welcome ideas and feedback as we continue to invest in demand led functionality.

CSO Alliance brings years of experience in running online security communities and Airbus have a team of over 600 FTE in their cyber division who protect their supply chain, thousands of fly by wire airplanes and over 134,000 group employees. It is this insight and experience that Airbus are keen to share with the maritime community.

The portal is designed for reporting all cybercrime, be it on ships or shore, and is dedicated to the global maritime supply chain. CSO Alliance has run 25 workshops around the world and in the last 6 weeks held workshops in London, Paris, Rotterdam, Antwerp and Hamburg as well as a port workshop in Holland to introduce the platform, where it was well received. A global roadshow will bring this to a city near you in 2018.

We are proud to have sponsored the Be Cyber Aware at Sea newsletter, Phish & Ships for its first year and fully support the vision that it remains free and so accessible to all. We wish it continued success in 2018.
The UK Department for Transport has been looking back at the new initiatives which have been introduced by the Government as it demonstrates how seriously it takes the risk of cyber attacks.

Back in 2015 the National Security Strategy reaffirmed cyber as a "Tier One risk" to UK interests. Then in 2016 the National Cyber Security Centre was established, and within its first year, prevented over a thousand cyber attacks on UK interests, and managed the response to hundreds of individual incidents.

One of the most important developments for the shipping industry is a joint government and industry group reporting directly to the National Maritime Security Committee (Industry). This group has representation from all the major ports within the UK, the UK Major Ports Group and the British Ports Association, and the UK Harbour Masters Association which also represents our smaller ports concerns.


The Code is aimed at ship operators, owners and crew members. It is designed to help businesses of all sizes to assess risks, devise the most appropriate reactive measures, and manage security in the event of an attack. The code explains why cyber security should be an integral part of maritime management through a ship’s lifecycle, and delivered cost effectively as part of mainstream business.

It also highlights the national and international standards and regulations that should be followed. It will therefore complement the work being done by the International Maritime Organization (IMO) to raise awareness of cyber threats.

The UK National Cyber Security Strategy has identified maritime infrastructure and vessels, as a class of cyber-physical systems, to be potentially vulnerable to interference from cyber threats. This potential vulnerability stems from a combination of increased connectivity and reliance on digital components, increased levels of autonomous control, and globally accessible navigation systems.

According to a major new study, Future of the Sea: Cyber Security there are some key findings, which include:

• Three broad categories of maritime cyber attacks have been identified with a range of demonstrable impacts. These categories are defined by the target of the attack; enterprise and information assets, GPS and navigation systems, or critical control systems.

• Across these three types of attacks, a rise in criticality has been observed in terms of threat motivation, technical competence of attackers and complexity of employed attacks. The published evidence for the maritime threat landscape is sparse beyond the reported attacks.

• Some potential technological developments for the maritime industry merit special attention as they are expected to occur during the next 3–5 years. These include advances in communication, improved sensing, and intelligent and autonomous control systems.

• Traditional engineering has focused on safety-critical design and development. Safety, however, is distinct from cyber security.

• Enterprise IT systems used for typical office functions within the maritime sector need to be better protected.

• Navigation systems, which are critical to the maritime sector, should be paid particular attention in order to protect against skilled and targeted attacks.

• Advanced and sophisticated attacks may target a range of electronic and control systems for ships, vessels, offshore units and port systems.

• Other responses to mitigate against cyber security risks are also required to be cross-sector, including threat sharing and attack reporting systems, coordinated incident response.

Cyber security specialist, Naval Dome, have completed a series of tests on systems in common usage aboard vessels from tankers to superyachts, to ascertain their security against active attack.

Naval Dome’s cyber team hacked into live in-operation systems used to control a ship’s navigation, radar, engines, pumps and machinery. They could shift their reported position, mislead the radar display and disable machinery, over-riding signals to fuel and ballast pumps and manipulating steering.

Asaf Shefi, Naval Dome’s CTO explained how one test was to penetrate the ECDIS, which they gained access to by emailing the captain’s computer. The attacking file was uploaded into the system via an automatic ECDIS chart update.

A separate attack focused on the radar, which they gained control of via a local ethernet switch interface that connected the radar to the ECDIS, Bridge Alert System and Voyage Data Recorder.

The third attack was on the Machinery Control System, via an infected USB stick that, once in place, started the virus file automatically.

From removing radar targets to changing the vessel’s crucial parameters such as position, heading, depth and speed, Naval Dome’s scenarios showed severe consequences for the target.

They showed that they were able to take control of the vessel without notifying the officers on watch. Effectively, every piece of information used by the bridge to monitor the vessel, could be compromised without raising suspicion until it was too late.

As Shefi pointed out, they attacked the vessel “at a critical point during an intended voyage – during night-time passage through a narrow canal. During the attack, the system’s display looked normal, but it was deceiving the Officer of the Watch. The actual situation was completely different to the one on screen. If the vessel had been operational, it would have almost certainly run aground.”

Naval Dome summarised their efforts by pointing out that it is not just the vessels which are at risk of cyber attack but the manufacturers themselves, as they can be targeted so that when they carry out diagnostics or perform software upgrades they inadvertently expose the vessel to cyber attack.

Naval Dome’s experiments do show the potential breadth of a cyber attacker within a specific scenario. The industry must take on board the lessons and advice raised by Naval Dome and see them as an opportunity to ensure they are a step ahead of cyber attackers to start the new year on the front foot.

NIGHTMARE CYBER SCENARIOS

Leading the way in maritime cyber security

Powered by

AVG/NEUROSOFT
2018 sees the new OCIMF pre-fixture tanker vetting cyber requirement shaping the response of owners. While the IMO has given shipowners and managers until 2021 to incorporate cyber risk into ships’ safety management systems, tanker owners and operators that are subject to vetting under OCIMF’s SIRE Programme are now addressing cyber security risks in their policies and procedures.

In April 2017, the OCIMF issued TMSA Version 3. In addition to the inclusion of ballast water management, fuel management and other items, Version 3 also contains a new Chapter 13 entitled “Maritime Security” with extensive on board and in the office cyber security vetting requirements. For the pre-fixture vetting review, Chapter 13 is dedicated to on board and office marine cyber security with OCIMF recommendations. Chapter 13 requires that the company must have a written plan identifying security threats. The cyber plan must include procedures to identify, mitigate and respond to security threats, i.e., drills/training/briefing and security patrols/searches. The cyber-plan elements may be included as amendments to existing SMS and ISPS plans.

Chapter 13 also attempts to promote on board cyber security awareness, i.e. it encourages people to lock unattended workstations, safeguard passwords, use social media responsibly and prevent the misuse of memory sticks/flash drives by ships’ personnel.

OCIMF recommends:

- An internal cyber audit program,
- Owners retain independent cyber specialist support, and
- Updating vessel ISM System/SMS and ISPS ship security plans to address cyber security risks.

As a pre-fixture vetting review is very subjective and varies between charterers, time will tell how each oil major/minor company implements the new Chapter 13. However, as of 1 January 2018, owners should be making best efforts to comply, especially to ensure that cyber risks are appropriately addressed in vessels’ safety management systems and ship security plans.

For more details see ocimf.org

Classification Society Lloyd’s Register has introduced a newly revised ShipRight procedure to address the challenges posed by new uses of data, new platforms and new types of services, ways of working and vessels.

The new procedure has been developed based on the experiences of the classification society in live projects with clients such as Rolls-Royce, CSSC and Synergy Marine, as well as through lessons learnt by working with academic and industry partners at QinetiQ, the University of Southampton and the National Oceanography Centre.

The update includes three new descriptive notes. These include: Cyber MAINTAIN, for recognition of digitally enabled condition based maintenance systems; Cyber PERFORM, for recognition of performance optimisation systems; and Cyber SECURE, recognising that cyber security has been assessed in the context of design and build.

Descriptions of autonomy levels have also been refined, with differences between vessel automation, remote monitoring and control, and fully autonomous operation and associated accessibility from onboard or ashore having been clarified. The LR ShipRight procedure can be accessed through the Be Cyber Aware at Sea guidance section, with a host of other leading industry texts www.becyberawareatsea.com/guidance
Two significant and widely publicised new pieces of EU legislation related to data protection and cybersecurity will impact most industry sectors - including shipping - beginning in May 2018: the EU General Data Protection Regulation (GDPR) and the Network Information Security (NIS) Directive.

The GDPR applies to organisations established in the EU and outside of the EU that provide goods and services to customers in the EU. The penalties for non-compliance are fierce and fines could be as much as €20 million or 4 per cent global annual turnover.

The impact of the NIS Directive is still less clear, when compared to GDPR, as it is down to individual member states to transpose the Directive into their national law. In the UK, the NIS Directive is going to be a key part of the country's national cybersecurity strategy and will apply to operators of essential services, which includes shipping. It will require these operators to take the necessary measures to protect their IT systems and will further require businesses to develop a strategy and policies to understand and manage their risks. In shipping this could include both land and sea operations. The strategies under development should include procedures for preventing incidents with awareness and training, detecting attacks and having the ability to respond, restore and recover. This could potentially create a legal minefield for shipping as the International Maritime Organisation suggests that 90% of the world’s trade is carried out by sea and it is highly probable that within this percentile, a high proportion will trade with and through Europe, making them subjective to the NIS Directive.

The shipping industry is taking initiative to work more collaboratively with initiatives promoting cyber protection such as the “Be Cyber Aware at Sea” campaign and the CSO Alliance “Maritime Cyber Crime Reporting Portal”. In a murky and uncertain world of looming regulations, awareness is key!

See www.axiscapital.com for more details.

Penetration testing experts Pen Test Partners, have highlighted how hackers could "sink a bulk carrier". They state that this can be achieved by manipulating the loading data of its hull stress monitoring systems (HSMS) to deliberately cause an imbalance of cargo on the vessel without the crew being aware.

The consequences could be catastrophic with the vessel being put under intense strain leading to it breaking up and sinking. "The reason it is feasible is that when HSMS were first developed, there was no concept of a vessel being connected to the internet, allowing it to be accessed remotely. Therefore, many HSMS are just PCs connected to the ships’ network," said senior partner, Ken Munro.

"A hacker could interrupt the loading data being fed to and from the monitoring system, having previously compromised the network either via the satcom unit or a phishing e-mail.

"Once in control, hackers can manipulate the loading of cargo and turn off any stress monitoring alarms that would alert crew to any undue strain on the vessel," he continued.

HSMS vendors and all ship control and reporting system manufacturers need to take security very seriously indeed, otherwise their own systems could be used against the ship.

A Master puts his faith in the stress monitoring system to alert him to any load bearing issues so the last thing he expects is for it to misreport and threaten the very fabric of his ship.

Pen Test Partners recommend that all ship managers and operators ask probing questions of their technology and control systems suppliers and demand that they prove beyond reasonable doubt that their systems are secure and will remain secure throughout their operational lifespan.

Pen Test Partners recommend that all ship managers and operators ask probing questions of their technology and control systems suppliers and demand that they prove beyond reasonable doubt that their systems are secure and will remain secure throughout their operational lifespan.
There is a worrying dynamic developing in shipping, as shipowners and maritime professionals seemingly take exception to some of the cyber horror stories emanating from security companies and ethical hackers. There is concern that either the industry is being shaken by fake news and apocryphal stories, or they are true and cyber companies are providing those that would attack shipping with a blueprint to hit shipping.

As with so many things in life, the line probably sits some way between the two. When one commentator recently took to Splash24/7 to make his views known, it was clear that in order for cyber security companies to really resonate with shipowners, they need to have their facts nailed on.

There is fear in the air concerning cyber risks, and that means that the industry is jumpy. So “scary cyber stories” are seemingly not helping. However, that does not mean that companies and their staff can bury their collective heads in the cyber sand.

It seems there needs to be a more constructive dialogue, and perhaps instead of taking to the media when issues are found, perhaps a more formal, collegiate approach is needed. It does not really foster a positive relationship if experts who understand cyber security do not work hand in glove with the experts who understand shipping.

Fixing cyber security is a team pursuit, but it doesn’t feel that way when there are accusations that, “many of the cyber ‘experts’ currently peddling fear to sell their services don’t have any professional maritime experience or any real understanding of ship operations”. The criticism in Splash24/7 stated that all too many companies seem to be “increasingly desperate to gain some traction by trotting out increasingly risible stories. This is really harmful to an industry that does have an issue with the risks attached to increased automation and ships becoming always on line and is trying to find a sensible and practical approach to the real risks.”

So, there we are, the risks are real so there is no need to resort to fake news or overblown narratives. The problems facing shipping will need each side of the equation to understand the other. Cyber experts need to ensure they do truly know the ways in which ships work, and the shipping industry needs to be open to constructive criticism. Together we can find the answers to make seafarers, the environment, ships and trade safer, but only by understanding what safe behaviour looks like, and through finding the ways to promote that behaviour on board, in shipping board rooms and on naval architects’ drawing boards.

The Digital Ship Cyber Resilience programmes for 2018 have been announced. There will be events in Rotterdam 15 February 2018 and Digital Ship Cyber Resilience Singapore 15 March 2018, during APM have been announced.

The events will explore how shipping embeds a host of new challenges into the maritime organisation, and how they can cyber security can be incorporated into systems and operations? The human factor is often claimed to be the weakest link. Ship operators need to increase cyber awareness both in the office and on-board. In this Forum, we will discuss ways to mobilise internal commitment, set up training and incorporate cyber awareness into daily procedures.

Cathy Hodge, Director, Digital Ship Events, says; “Cyber threat awareness is growing throughout the maritime sector – recent breaches have ensured that this is now high on the agenda. But there is still a lot of confusion and noise, and our aim through our Cyber Resilience agendas is to cut through this and provide our delegates with a clear view of the risk landscape, as well as the tools to harness resilience and security throughout their operations. APM in Singapore represents the ideal opportunity to share this message with a technically advanced and digital savvy audience of market leading shipping companies and other stakeholders in the supply chain.”

For more information on speakers and agendas at each event please contact cathy@thedigitalship.com or visit our website www.thedigitalship.com
As we head into 2018 the headlines have been full of the rise of cryptocurrencies. While they have been around for some time, digital currencies are now taking off as a mode of transaction within international commodity trading, and Ukrainian shipping firm Varamar Ltd is leading the way, currently in negotiations with a client to use bitcoin as a means of payment. They are sure to be the first of many.

Cryptocurrency is, at one level, just virtual cash exchanged through peer-to-peer payment technology, free from the restrictions and interventions of standard players of finance – central banks, mints, financial institutions and regulators for example. Operating in this unregulated environment means that cryptocurrencies like bitcoin offer unparalleled opportunity for wealth creation and, as founder of Varamar Shipping Alexander Varvarenko outlines, there are other benefits to an alternative payment system in such international businesses.

“Paperwork for transactions is a complicated issue with banks, and bitcoin payments will help solve that by being faster. It could also help solve payment problems in countries like Pakistan, Russia, Sudan, Yemen, and Qatar, which have safe companies but are victims of sanctions being imposed against their governments.”

The advantages cited by Varamar are echoed by others in the industry; Ivan Vikoulov, the managing director of a grain trader, emphasised the stress upon the industry by political decision making which means vessels registered offshore but whose owners have banks in the Baltics, are being pushed for payments in dollars.

For these companies, cryptocurrencies offer an attractive alternative system, ideally placed for international business. However, it does come with concerns that will require addressing, not least because as an intrinsically cyber-based system that means it is open to attack from cyber criminals.

In a recent article by BAE Systems, they outline how criminals are already adapting their attacks to include these cryptocurrency platforms, for example creating malware specifically to steal bitcoin as well as other cryptocurrencies, while focusing on bitcoin wallets and the compromise of private keys.

The potential of cryptocurrency is vast, particularly in the shipping industry where, as stated, its borderless nature is notable, and predictions of the market reaching trillions of dollars will make it even more tempting. This means that while the percentage of business currently accepting cryptocurrencies is small, it is likely to grow. The shipping industry will therefore need to weigh up the advantages and disadvantages carefully, particularly regarding the substantial cyber risk of this operation.

The UK Hydrographic Office (UKHO) published a revised edition of the ADMIRALTY ENC and ECDIS Maintenance Record (NP133C), which now for the first time provides guidance to help bridge crews record and manage cyber risks.

The quick reference folder is designed to help mariners demonstrate compliance with IMO regulations during Port State Control inspections, with easy-to-use checklists and templates to record ECDIS annual performance checks and software maintenance.

The update has been developed in line with guidance published by IMO, stating that approved safety management systems (SMS) should consider cyber risk management in line with the ISM code before January 2021. NP133C has been revised to help mariners achieve this by providing a checklist to document threats and procedures to mitigate risk to ships.


**TOP 6 WORST PASSWORDS**

1. 123456
2. password
3. qwerty
4. letmein
5. football
6. iloveyou

source: splashdata.com