#11

OCT:2017

PHISH & SHIPS

BE CYBER AWARE AT SEA

Kindly sponsored by

CSO ALLIANCE MARITIME

WELCOME

BE CYBER AWARE AT SEA

Welcome to issue 11 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".

The campaign continues to make head way. Just last month during the London International Shipping Week 2017, the issue of cyber security was repeatedly brought to the fore, and our efforts to ensure that seafarers and the wider shipping industry are engaged with cyber security were praised.

This even saw us receive a High Commendation as an Unsung Hero for Commitment to Raising Cyber Security Awareness in Global Shipping Worldwide at the IHS Safety at Sea Awards,

Campaign Director, Jordan Wylie who attended the event, commented: "It is a real honour to be recognised in front of the IMO Secretary General here in London. Nothing great in life is ever achieved alone, this was a team effort but I would like to highlight the special contributions of Lizzy Foster (Campaign Manager), Steven Jones (Newsletter Editor) and CSO Alliance for their continued sponsorship of the Be Cyber Aware At Sea campaign, which allows us to keep educating seafarers and raising awareness. Thank you also to all the maritime stakeholders that continue to support this free initiative."

The work is only just beginning, and inside this latest issue we look at the stories, threats, projects and people who are bringing maritime cyber issues to the fore. See https://www.becyberawareatsea.com/ for more details.

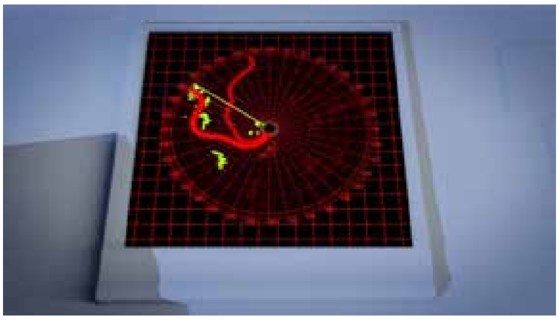
LAWYERS ONBOARD WITH CYBER

HFW

International law firm HFW takes seriously the cyber threat faced by ship owners and their employees. According to HFW, it is essential that all seafarers are given the training and support they need, both to reduce their own personal exposure to the cyber threat and to mitigate the chances of a successful cyber attack being perpetrated on their employer. As part of these continuing efforts, the law firm is supporting the development of short films to educate seafarers further.

Having supported the Be Cyber Aware at Sea Campaign since its earliest days, HFW is delighted to have been able to partner on the production of these 8 innovative and exciting videos. William MacLachlan, Senior Associate (pictured above) at HFW noted "By being culturally neutral and utilising the minimum of written English, the hope is that the videos and their message will spread to the farthest reaches of the ship owning and seafaring community". Find out more at www.hfw.com

LOOSE
CLICKS
SINK
SHIPS!
BE WARY OF POP UPS, EMAILS AND WEBSITES ASKING FOR SENSITIVE INFORMATION



The Cyprus Shipping Chamber (CSC) has been working with its members to assess the problems of cyber security. According to the Chamber, "Digitalized ships, increasing interconnectedness, the extended use of electronic data exchange and electronic navigation increases the likelihood of cyber attacks".

As such CSC has issued cyber security guidance in the form of a case study interview with a member-company: one able to play the part of shipowner, technical-operations manager and crew manager. Across a range of key questions, the company justifies its decision making, the safeguards in place and the way in which threats are assessed and responded to.

The case study hinges on a company that is undergoing a transition from the current Fleet Broadband communication services to a higher broadband capable VSAT system. So, much hinges on the fact that suddenly their ships will be "open to the internet", and of how they intend to deal with that.

For the company in question, the fact that VSAT broadband brings opportunities and threats is well understood, and they are seemingly responding appropriately. They recognise that cyber threats will most likely come from within the ships' network, from a vendor, or the crews' use of personal computers, from virus emails, phishing, improper content downloads, to name just few threats.

They also recognise that the ships' network needs to be mapped and all critical systems need to be assessed for vulnerabilities. Penetration tests are a good check on the existence of vulnerabilities so that corrective actions can be prioritised.

While it is interesting and encouraging to note that CSC and its members are looking at such matters, there should also be some caution. Shipping companies have been adept for years at saying what they would do, but have often not been so effective at actually doing it. Let's hope that we are not hearing the art of the possible, but instead the stories of the actual.

Paying lip service to cyber security is perhaps the worst thing any company can do. The full case study can be found on the CSC website and makes fascinating reading:

https://maritimecyprus.com/2017/09/25/cyprus-shipping-chamber-cyber-security-case-study/

Code of Practice
Cyber Security for **Ships**

Official new UK Government guidance has warned of the need to improve protection for vessels from online attacks. Ships could be vulnerable to "kidnap, piracy, fraud [and] theft of cargo" if their computer systems were compromised, the Department for Transport (DfT) said.

In a new Code of Practice, the DfT stresses that security is not just about preventing hackers from gaining access to systems and information, potentially resulting in loss of confidentiality and/or control. It also addresses the maintenance of integrity and availability of information and systems, ensuring business continuity and the continuing utility of digital assets and systems.

To achieve this, consideration needs to be given to not only protecting ship systems from physical attack, force majeure events, etc., but also to ensuring the design of the systems and supporting processes is resilient and that appropriate reversionary modes are available in the event of compromise.

Personnel security aspects are also important. The insider threat from shore-based or shipboard individuals who decide to behave in a malicious or non-malicious manner cannot be ignored. Ship owners and operators need to understand cyber security and promote awareness of this subject to their stakeholders, including their shipboard personnel.

The new Code of Practice explains why it is essential that cyber security be considered as part of a holistic approach throughout a ship's lifecycle, as well as setting out the potential impact if threats are ignored. The Code of Practice is intended to be used as an integral part of a company's or ship's overall risk management system and subsequent business planning, so as to ensure that the cyber security of the ship, or fleet, is managed cost effectively as part of mainstream business. It should also be read by board members of organisations with one or more ships, insurers, ships' senior officers (for example, the Captain/Master, First Officer and Chief Engineer) and those responsible for the day-to-day operation of maritime information technology (IT), operational technology (OT) and communications systems.

Download the code here: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/642598/cyber-security-code-of-practice-for-ships.pdf

THE WAY WE TELL 'EM...

Anthony Daly, a senior Cyber Security Consultant is guilty of the following crime against humour...If you happen to have any cyber security jokes which can compete at this kind of level, we'd love to hear from you.

A Captain asked the head of IT if they could change the ECDIS password to Beefstew1

No, came the stern reply, it's not stroganoff!

INDIAN REGISTER NEW CYBER RULES

In a bid to address the cyber risks of emerging technologies that are being introduced to the Indian maritime industry, the Indian Register of Shipping (IRClass) has developed class rules based on guidelines set by the IMO, as well as appropriate standards, such as the National Institute of Standards and Technology – US Department of Commerce (NIST).

With the rise of cyber attacks on information and operational technology systems, cyber security is critical not only for data protection but also for safe and reliable operations, the classification society noted.

Cyber attacks on ship's control systems, IT, navigational and other critical systems can result in damage or even losing course of the ship, which can have a negative impact on the safety of the ship, port facilities and marine property, explained Executive Chairman, Mr. Arun Sharma.

"As the industry continues to introduce new technologies, IRClass as a classification society, plays a significant role in ensuring that the safety of a vessel and its crew are not compromised by such attacks," he added.

The implementation of these rules help IRClass to identify the cyber risk issues from as early as the design stage of the vessel. A final verification then takes place once the vessel is built, and periodically during annual surveys. A vessel, together with its shipping back office, that is certified for cyber safety is one that complies to the class rules, as well as additional class notation.

In addition to the class rules, IRClass has also developed the first edition of 'Cyber Safety Guidelines for Port and Shipping Company Facilities', a guide to safeguarding technology systems from internal and external cyber threats. These guidelines would help a company to identify gaps and mitigate risks and IRClass is in a position to offer end to end solutions.

INMARSAT NEW CYBER SERVICE LAUNCHED

Inmarsat has released its new Fleet Secure service, the industry's first fully-managed service to detect cyber vulnerabilities, respond to threats and protect ships from widespread cyberattack.

Fleet Secure is a Unified Threat Management (UTM) and monitoring service that will offer owners and managers a continuous view of the status of their digital security. It detects external attacks via high-speed satellite broadband, and it protects vessel networks from intrusion via infected USB sticks and crew devices. Three different levels of the Fleet Secure service will be available for customers of Inmarsat's popular Fleet Xpress satellite broadband. The UTM is powered by Trustwave, a world-leading provider of information security solutions, and is available in three service levels.

"Cybercrime is an inevitable downside of the digital economy, on land or at sea," said Peter Broadhurst, Senior Vice President Safety and Security. "Other maritime cybersecurity offerings we have seen address only part of the threat or some of the management issues. Inmarsat's new Fleet Secure service provides an all-inclusive, real-time managed monitoring service . . . The threats from cyberattack demand robust technical solutions, network integrity, operational and training support, and raised awareness across the maritime sector."

The firm says that Fleet Secure complements the strengths of its own satellite and ground network. Inmarsat is also involved in setting global standards for cybersecurity at sea through its support for a working group set up by the International Association of Classification Societies (IACS). www.inmarsat.com

SPEND BIG AND STILL GET HACKED

Epsco–Ra launched in February 2016 to answer the emerging maritime cyber security threat. Here Gideon Lenkey, their Technology Director, shares his thoughts on why big companies who spend a lot of money on cybersecurity still get hacked?

I get asked this question often and the answer is complex because there are actually many different reasons this happens. First, you have to understand that if you work for the type of company that takes the time to understand and manage cybersecurity risk, you'll know that being hacked isn't a matter of if but when and how bad. The difference between a company which properly manages cybersecurity risk and a company that doesn't, is the company that does detect they've been hacked will react accordingly. Companies that choose not to manage risk or perhaps focus entirely on compliance still get hacked, perhaps even more so, but they usually only become aware of it when informed by a third party, such as a law enforcement agency. They are often reacting to a situation they have not properly planned for.

Let's compare two recent examples of high profile hacks, Maersk and Equifax. Maersk was hit with some fairly sophisticated malware in June of 2017. It seriously impacted operations as it spread, forcing Maersk to close customer facing order taking systems. Given an absolutely nightmarish scenario, it appears Maersk had a good incident response plan in place and executed it. Yes it took time, yes it cost them money but it all seemed to go according to a plan. In a statement their CEO briefly described the attack, acknowledged their losses and issued assurances that additional measures had been enacted. Acting on the lessons learned in an attack is just part of good cybersecurity management. That pretty much was the end of it. To a security man like myself the Maersk attack looked well handled.

Contrast that with Equifax, not one but two recent attacks, neither of which was sophisticated but both were devastatingly effective. The Equifax response was described by in security circles as 'a dumpster fire'. The attacks seem to have caught them completely off guard and without a plan. Differing messages on their websites, Twitter sending people to a fake phishing site and executives caught dumping stock in the run up to the breach announcement, left people not only confused and misinformed but feeling really angry.

Both companies undoubtedly spend considerable money on Cybersecurity products, services and personnel but obviously operate on two different levels when it comes to risk management. The moral of the story is Cybersecurity management is hard and your success relies on a deep understanding of the risks involved. Understanding and planning for the inevitable 'bad day' will make the difference between calmly managing the events and a dumpster fire burning wildly out of control.

www.epsco-ra.com

EPSCO-Ra

THE COST OF CYBER FAILURE...

Novæ
LOOKING FORWARD

In Novae's "Talking Cyber Sense" column, this month Stuart Quick, Breach Response and Cyber Operations Manager talks about the costs of failure, and how to avoid it.

When it comes to cyber attacks, we have to think of "Not if, but when". In my role as a cyber security consultant I used to see companies focusing huge amounts of resources on controls to prevent security incidents from happening. However, this often came at a cost to the investment in systems and processes for responding to, and managing incidents when they occurred. For those with the responsibility for securing their systems the distribution of resources between these two areas this was a perennial challenge but one that, if addressed appropriately, really differentiated one organisation from another.

As insurers we see the benefits of being prepared. Companies with robust and well tested BC and DR plans recover quicker both in the short term (operationally) and long term (strategically). The hidden or intangible costs of an incident such as; reputation, morale, consumer confidence, suffer less when companies are able to respond openly, swiftly and competently. Sadly we also see those that have not prepared adequately always recover operationally but typically suffer strategically.

Are you prepared? When was the last time you practiced you BC and DR plans for your company, office, vessel, department, or critical systems? What follows is a basic checklist of the key components to a BC/DR plan:

- Risk Assessment – needed to feed the BIA.
- Business Impact Analysis (BIA) – what is important and what is not and what impact will this have on your business in monetary terms.
- Trigger Definitions – what scenarios and specific circumstances will trigger your BC or DR plan?
- Documentation – needs to be up to date, simple and accessible i.e. stored on and off site and accessible to more than one person.
- Maintenance Plan – who is responsible for maintaining and improving your plans and when does this happen?
- Education and Training – does everyone need to know everything? Decide which groups need to know what.
- Role & Responsibilities – senior stakeholder buy in is critical, then decide who is accountable for the programme and who is responsible for making it work.
- Testing – how frequently do you plan to test your plans, which locations, which systems, what type of test? There are 3 types of test; desk top test, walk through, live test.
- Incident Management – if you need to maintain a chain of custody during an investigation, how does this impact BC and DR plans and objectives?

A fully worked up BC and DR plan does not happen overnight. It takes time. If BC and DR are managed by different teams then bring them together and pool resources. Review your risk assessments and BIA and then identify and prioritise work based on risk and business objectives. Walk before you can run, your plans will never be 100% complete and in the world of BC and DR it is better to have plans 70% complete 'on time' rather than 100% complete 'after the event'.

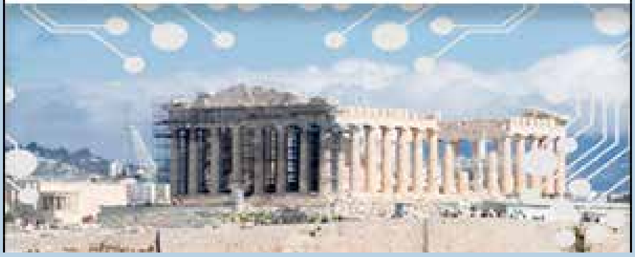
There is always a cost to failure but the cost of success far outweighs the losses poorly managed BC and DR events cause. A well thought out and well-rehearsed continuity and recovery plan help to mitigate costs and get you back up and running sooner and usually stronger.

https://www.novae.com/

Digital Ship

CONFERENCE & EXHIBITION

Athens, 1 & 2 November 2017



Digital Ship is pleased to be returning to Greece for our longest running event, with the 15th Annual Digital Ship Conference & Exhibition in Athens on 1 & 2 November.

Industry experts will take to the podium during the conference which will include plenary and interactive panel sessions over the two days, and there will be an exhibition showcasing leading suppliers and vendors to the sector.

The 5 key focus sessions throughout the 2 days will include:

- Harnessing Maritime's Digital Future
- Developing Big Data Ecosystems
- Building Cyber and Security Resilience – with a Special Focus on GDPR
- Blockchain in Practice – Creating Trust in the Maritime Supply Chain
- Vessel Performance Optimisation

New for 2017 – Digital Ship's Start-up Showcase

The Start-up Showcase is a new addition to this year's Digital Ship Athens. The Showcase will bring together exciting new talent - developing products, services and platforms; implementing and harnessing digitalisation of the shipping industry.

From visibility to credibility, partaking in the Start-up Showcase will provide a platform to bring innovative solutions to our audience, and receive constructive feedback from peers and industry leaders. For more information on how to join this session contact youngsuk@thedigitalship.com.

PLUS: EXCLUSIVE WORKSHOP, OPEN ROUNDTABLES AND NETWORKING FUNCTIONS,

INCLUDING A GALA DINNER ON 1 NOVEMBER

We are currently preparing the agenda, with speakers and panellists announced soon. For more information, contact cathy@thedigitalship.com.

Event: Digital Ship Athens 2017

Date: 1 & 2 November 2017

Venue: Metropolitan Hotel, Athens, Greece

Website: https://www.athens.thedigitalship.com/

BE CYBER AWARE AT SEA

Sponsored by:

CSO ALLIANCE MARITIME

www.becyberawareatsea.com

think@becyberawareatsea.com

With thanks to our many industry supporters....