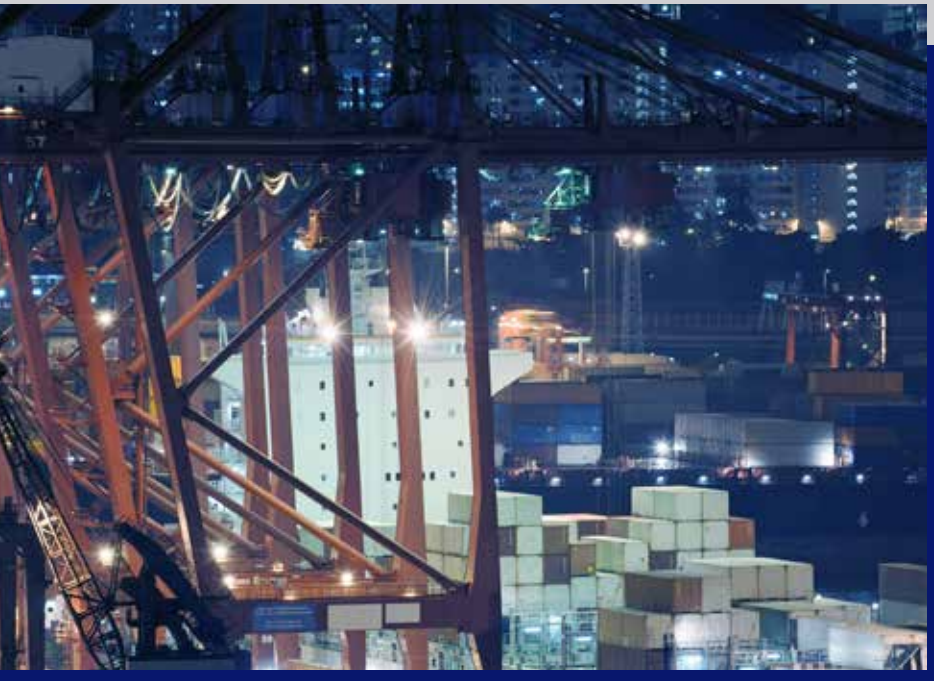
#5

APR:2017

PHISH & SHIPS

BE CYBER AWARE AT SEA



Kindly sponsored by

CSO ALLIANCE MARITIME

TIME FOR CYBER AWARENESS

Welcome to issue 5 of "Phish & Ships", the maritime cyber security newsletter, keeping you up to date with the shipping industry initiative, "Be Cyber Aware At Sea".

That leading technology commentator Daniel Allen has recently been looking at the growing number of key shipboard systems, demonstrates that cyber security is an increasingly important part of maritime risk management.

While to date the number of recorded maritime cyber attacks may be minimal, the risk of threats will grow. The very real concern is that critical systems could be prevented from functioning, resulting in collision, pollution and environmental damage, and possibly ships being redirected.

Robust cyber security—both in terms of technological systems and human behaviour—will therefore be critical. This is even more so as autonomous ships sail closer to reality.

One of the biggest concerns is that such vessels will use off-the-shelf components and big data within autonomous systems. This means that hackers can leverage their familiarity with the technology, with potentially dire consequences.

Going forward, it is clear that the shipping industry must do more to pre-empt the inevitable security issues associated with autonomous systems. But it will need assistance.

Moves toward connected shipboard systems are already increasing cyber risk. By July 2018, all ships will be required by the International Maritime Organization (IMO) to use the Electronic Chart Display and Information System. Relying on internet-based software and updates, this GPS-based system is clearly open to digital corruption, and there are many concerns and much anecdotal evidence that problems could be around the corner. It is more important than ever to act on cyber security.

Recent guidelines from entities such as Lloyd's Register and the ABS are helpful, but clear and discrete solutions to specific cyber security challenges are still thin on the ground. In an industry which operates on tight margins, those solutions will need to be affordable and user-friendly, as well as timely.

Digitalisation and automation in commercial shipping is a reality, so the time to think about cyber security is now. By acting today we can ensure existing systems are protected and new ones are even safer. So let's all Be Cyber Aware At Sea!

BEWARE OF RANSOMWARE

Among today's fastest-growing cyber crime epidemics is "ransomware" - malicious software that encrypts your computer files, photos, music and documents and then demands payment in Bitcoin to recover access to the files.

A big reason for the steep increase in ransomware attacks in recent years comes from the proliferation of point-and-click tools sold in the cyber crime underground network, making it simple for anyone to begin extorting others for money.

There are actual online tools which enable anyone to become a cyber pirate, kidnapping data for a ransom, so you need to be on your guard. Experts believe that protection is vital, but so too is awareness. After all, you can have the best security systems, but if you circumvent them yourself, then of course, you will be at the mercy of those who would seek to extort you.

TOP ANTI-RANSOMWARE TIPS

Ransomware encrypts the files on a computer, essentially scrambling the contents of the file so that you can't access it without a decryption key, in exchange for which is demanded a ransom. Once the malware has infected one computer, it can spread to others in the network, making it impossible to carry out normal operations.

1. Make sure you're running a robust security solution which covers all your devices (PCs, Macs, smartphones, and tablets) and provides protection.

2. Regularly backup your data. Store the backups offline, and test they work.

3. Ensure the software on all your devices up to date.

4. Be extra careful with email attachments, especially with ZIP files and Office documents (Word, Excel, and PowerPoint). Don't open email attachments that are sent by someone you don't know.

5. Limit your use of internet browser plugins.

Sponsored by: CSO ALLIANCE MARITIME

GCHQ CYBER APPROVAL

Leading maritime security and safety provider JWC International, a UK Maritime & Coastguard Agency approved ISPS and ISM training consultancy based in Europe and Asia, has launched a Maritime Cyber Security Awareness (MCSA) platform to help inform and educate seafarers and offshore crews worldwide.

GCHQ, a security division within the UK government and a renowned world leader in information security and cyber resilience, has approved the JWC International course which represents a mark of excellence for shipowners and managers looking to find a specialist credible maritime cyber security education provider.

JWC International is the only GCHQ approved provider to the global Maritime and Offshore sector. See online for more details at https://www.jwcinternational.com/

Cyber Jargon Buster

ADWARE - A form of spyware that displays unwanted advertisements on a computer.

BACKUP - Copying data to ensure its availability in the case of computer failure or loss.

DOWNLOAD - To obtain content from the internet, as an email attachment or from a remote computer, to your own hard drive.

HONEY POT - A security feature built into a network, designed to lure hackers into meaningless locations to avoid harm to genuine, crucial data.

SMARTPHONE - A mobile phone built on a mobile computing platform, with more advanced computing ability and connectivity than a standard mobile phone.

JOIN INDUSTRY LEADERS IN ATHENS ON 25 APRIL AT DIGITAL SHIP'S MARITIME CYBER RESILIENCE FORUM

The cyber threat is growing across all sectors. In this information era of the connected ship, and with the shipping sector's increasing reliance on technology and remote monitoring, maritime cyber security is no longer optional, but is business-critical.

How many companies are ready to tackle the cyber challenge? And how resilient are they? How quickly and robustly a company can respond will depend on how ready and determined they are, and on whether they are planning to invest in cyber preparedness.

Are we witnessing a new security paradigm, where the focus is on prevention rather than simply relying on reaction? Ship operators need to be confident that their procedures can deal with ever bigger and more sophisticated cyber-attacks and that that they are developing a safe, dependable, cyber capability in shipping.

Digital Ship's Maritime Cyber Resilience Forum will bring advisors, end-users, technology providers and policy makers together, aiming to:

- Understand, define and assess the threats and risk of maritime cyber-attack.

- Raise awareness of cyber security and risk issues and identify increased cooperation and information sharing mechanisms.

- Discuss appropriate regulation and guidelines for clearer standards throughout the industry, and with authorities.

The Forum will contain 5 focused key sessions:

1. Facing the Cyber Threat: An Overview of Maritime Cyber Challenges and Focus on Building Resilience.

2. New Developments in Maritime Cyber Regulations and Guidelines.

3. Cyber Risks: Identification, Mitigation and Response.

4. Pan-Industry Platforms and Collaboration to Combat Cyber Challenges - Lessons for Maritime.

5. Viewpoint: Are We Cyber Ready? Conclusions and Actions.

Book now: http://www.athens.thedigitalship.com/

INDUSTRY BIG HITTERS AIM SIGHTS ON CYBER SECURITY ISSUES

ABS, a leading provider of classification and technical services to shipping, recently spoke out on cyber issues at the 32nd annual CMA Shipping Conference and Exhibition in Stamford, Connecticut.

ABS Chief Operating Officer Tony Nassif shared his insight on cyber-related challenges and the role of Classification Societies in tackling the problems currently facing shipping and those that are just around the corner. Nassif believes the main challenges being faced by shipping industry are due to the fact that "not all users of new technology understand the way the software they are using was built, how it operates, what happens when it fails and what mitigation they have."

It appears shipping companies are sat in something of a blackhole, many not seeming to understand what is being done, how and why, when it comes to technology. This is very worrying, particularly, as Nassif elaborated, given the scale of system integration: "Now, our ships and assets employ a 'system of systems' approach that combines operational and information technology".

Nassif saw exciting times ahead for Classification Societies as they adapt to address these new risks. "Looking at the future, we can see that cyber and software risk are overlapping and converging, and as a result, class and industry both have to adapt. With the expansion of the regulatory environment, class is widening its remit to include verification of compliance with regulations and new topics such as cyber security."

Nassif warned, "Cyber risk is a subject that is not going away." To tackle this massive subject, ABS has developed ABS CyberSafety®, a modular and measurable process that can evolve over time as threats and technologies emerge.

Describing ABS' approach to cyber security, Nassif said, "ABS CyberSafety brings together traditional IT and Operational Technology, moving from a set of basic procedures covering corporate organisation and governance, to a detailed capability and task-assessment cycle. Looking at it this way enables us to understand assets, gaps and vulnerabilities, develop a risk profile and execute a project plan with asset owners."

In closing Nassif reiterated the importance of tackling cyber risks head on and doing so in a way that integrates operational and information technology platforms.

The annual CMA Shipping Conference and Exhibition brings together experts from around the world to speak on the issues that will shape the future of the maritime industry. Perhaps unsurprisingly the issue of cyber security and shipping came to the fore at the 2017 event, and hopefully the fact that so many experts were gathered to exchange views may advance the cause and desire for maritime industry stakeholders to be cyber aware at sea.

WHAT IS YOUR PASSWORD?

To stay safe online and keep your data secure, it is important to create robust passwords. The best and strongest passwords should:

1. Contain a lot of characters – use the maximum length available!

2. Contain a mixture of upper and lower case letters, numbers and symbols. Make substitutions, such as $ for S.

3. Not include keyboard patterns e.g. 'Qwerty12345'.

4. Not include something obvious or relevant to you, such as your name or first line of your address. Even better, choose a word not included in the dictionary at all. Consider using an acronym from a phrase.

5. Be unique to each site you log into. Using the same password to access multiple accounts means hackers could access all your accounts with a single password.

JOIN IN AND HAVE YOUR SAY ON CYBER...

To keep up with the cyber risks to your company, fleet and onboard your ships, make sure you visit our website and join the campaign to make maritime cyber security work.

www.becyberawareatsea.com

think@becyberawareatsea.com

Steven Jones, the editor of this monthly round-up of maritime cyber matters, would love to hear from you.

So please share your thoughts, views and experiences with the industry. We look forward to the next issue where we will once again analyse the current state of play in shipping and bring you some top tips for staying secure online. Together we can help the industry to Be Cyber Aware at Sea.

TALKING CYBER SENSE:

SMART PHONES AND MOBILE DEVICE SECURITY

Novae
LOOKING FORWARD

TALKING CYBER SENSE: James Creasy, Cyber Unit Class Underwriter at Novae Group shares his thoughts on mitigating cyber threats. This time we look at smart phones...and the effect on cyber security.

We live in a world where the predominant form of computing is mobile computing. There is more power in our phones than there was in the computers used to guide the Apollo 11 mission to the moon. As consumers of this level of computing power, we think nothing of downloading applications and inputting our personal data to sign up to the latest games, health and fitness, music and personal productivity apps. Mobile communication provides us with so much to make our lives more comfortable and instant connectivity has brought about greater efficiencies. However, criminals and other threat groups also understand this and seek to exploit the vulnerabilities from mobile computing.

The threat surface is vast as we are almost always connected online in one form or another. A seafarer may be physically isolated at sea but their online persona is live and accessible. The portable nature of smart devices and the types of applications used, means there is a greater risk of private information being stolen or leaked than ever before. There are also significant differences between mobile computing and more traditional computing environments such as:

- Location detection, cameras and microphones are frequently used in social media communication, and can potentially compromise sensitive information.
- Smart phones are connected to web services almost always over an unsecure wireless connection.
- New mobile apps are released daily and updated regularly leaving users exposed to continuous software updates.

To mitigate these risks and reduce our vulnerabilities, every smart phone user should:

- Always restrict access with a passcode and use biometrics where possible.
- Automate device back up – remember that when pictures are saved to the cloud they are not secure, but at least they are backed up!
- Always update applications and operating system when notified to do so.
- Always download apps from trusted app stores and do not jailbreak devices.
- Avoid suspicious emails and pop-up notifications requesting credentials.

https://www.novae.com/

NAVY SERIOUS ON CYBER ATTACKS

The Royal Navy is holding its first large scale cyber war games. "Information Warrior 17" will involve Artificial Intelligence (AI) and test the protection of warships and submarines against cyber attacks.

The training will be held during Joint Warrior, which involves thousands of army, navy and air force personnel. Information Warrior 17 sets the foundations for cyber warfare in the future as enemies will seek to target any weaknesses.

The exercise will involve:

- Using AI technology to develop a "ship's mind" at the centre of Royal Navy warships. The Navy said this would allow fast, complex decisions to be made automatically, making warships and submarines "safer and more effective in fast-moving, war-fighting situations".
- Cutting edge computing technology and unmanned aerial vehicles to help the Navy and Royal Marines to fight in information warfare.
- Using open source intelligence and satellite imagery to enrich the intelligence picture of a situation.
- Test the defences of ships and submarines against the risk of cyber attacks on the vessels' combat systems, communications systems, power and propulsion control systems.

The Royal Navy is not alone in seeking to tackle cyber threats. In its combat against cyber threats, the US Navy has hosted an open challenge, calling on expert hackers to crack a simulated computer system.

The Center for Cyber Warfare at the Naval Postgraduate School (NPS) hosted an event challenging hackers to test their skills against a "boat in a box," a simulated system built by contractor Booz Allen Hamilton of the NPS to resemble fleet systems.

A key objective beyond breach prevention is enhancing their ability to respond efficiently to a successful attack and promptly regain control over compromised elements.

The navies of the world are getting serious on cyber – it is important that commercial shipping is not left behind.

www.becyberawareatsea.com

think@becyberawareatsea.com

With thanks to our Supporters