#6

MAY:2017

PHISH & SHIPS

BE CYBER AWARE AT SEA

Kindly sponsored by

CSO ALLIANCE MARITIME

SUPPORTING SEAFARERS ON CYBER

Welcome to issue 6 of "Phish & Ships", the maritime cyber security newsletter, keeping you up to date with the shipping industry initiative, "Be Cyber Aware At Sea".

Seldom does a meeting, conference or exhibition in the maritime industry pass without mention of the cyber threat to shipping and the need for greater levels of security. Our campaign director, Jordan Wylie, has been vocal on the issue, taking to the stage last month at The Digital Ship conference in Athens (pictured above).

That cyber is the buzzword of our time demonstrates that our campaign to promote and encourage cyber awareness is hitting the mark. As Be Cyber Aware At Sea has long purported, discussion of the problem of cyber crime is an important step towards tackling it. However, it is just the first step of the marathon that the industry now faces.We would be wise to not become complacent; there is a danger is considering the discussion of the issue as tantamount to fixing it. To paraphrase Winston Churchill, perhaps this is simply the end of the beginning. Now we are aware of the issues and what is at risk, the next stage for the maritime and shipping industry is to operate under a new mind set, learn from the past and innovate its way to safer cyber seas.

Our mindset should be absolute: cyber crime exploits the gaps in security to devastating effect so the industry must remain vigilant and on its guard from top to bottom, boardroom to boiler room. Losing battles to win the war is not a solution in tackling the cyber threat.

We need to learn from the lessons within dynamic positioning systems. We need sufficient redundancy, to avoid single points of failure and to isolate systems from threats.

We need to be innovative. The shipping industry is beholden to the systems designers who develop our power management, navigation controls and mechanisms. We need these to be fit for purpose and able to head off cyber problems as a matter of priority.

We also need to be aware that protecting our maritime and shipping industries against cyber crime will involve company-wide solutions. Just as the crews at sea need to be vigilant, companies should be working to support them, reducing their risk exposure and narrowing the gaps in security and opportunity of cyber criminals.

As for Be Cyber Aware At Sea: we look forward to running step by step with the industry in this marathon against cyber crime. Learn more at www.becyberawareatsea.com

LEARN TO TRUST BUT VERIFY

A popular tactic hackers employ is social engineering, which means pretending to be someone they are not. For example, they may pretend to be an employee at your company to get you to click on a link in an email, or pretend to be an interview candidate and ask you to retrieve a resume from a USB stick.

Blindly complying with these requests could enable malicious software to spread throughout your computer or network, allowing the hacker to either absorb company or personal information or data, or take control of the system.

As a best practice, always ask questions before doing something for someone you don't know, and know its okay to decline a request in an effort to stay secure.

WORRYING SHIPPING CYBER DATA

According to a new survey of the maritime industry:

90% of **MARITIME LEADERS** say more should be done to prevent cyber attacks

81% believe **REPORTING** should be mandatory

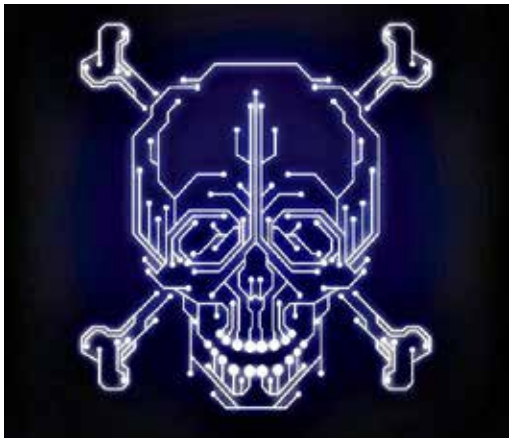
BUT...

56% have **NO PLAN** to tackle cyber security

10% think **CYBER ATTACKS** are most critical challenge today

Source: Sea Asia survey

Sponsored by: CSO ALLIANCE MARITIME



Inmarsat Views Cyber Risk

Ronald Spithout, the president of satellite communications giant Inmarsat Maritime has pulled no punches with his assessment of cyber risk management in shipping.

According to Spithout, most shipowners today have not conducted comprehensive risk analysis of cyber breaches, leaving the global merchant fleet very exposed to online attacks.

Speaking to respected industry journal, Maritime CEO, he stated his fears that as "ship/shore connectivity improves, ships become bigger targets for attack, more vulnerable to malware". He also fears that more mobile devices onboard will generate more opportunities to download infected files.

Inmarsat is keen to tackle these problems, and has responded by dedicating more resources to the issue of maritime security within its own Safety Services section. The organisation now has a team of cyber security specialists developing an end-to-end cyber security solution, which provides a technical answer to report and prevent attacks, plus a programme of awareness, risk assessments and training.

Spithout raises a key point that while most shipowners or operators now recognise that cyber breaches are occurring, most have not completed, or would even know how to go about, conducting a comprehensive risk analysis. It is high time to translate recognition of the problem into workable solutions.

Cyber Jargon Buster

ADMINISTRATOR: A user with sufficient access rights to allow them to manage the access rights of other users.

AUTHENTICATION: Process for verifying that someone or something is who or what it claims to be.

COOKIE: A small file which asks permission to be placed on your computer's hard drive. Cookies allow web applications to personalise your experience by gathering and remembering information about your preferences.

DIGITAL SIGNATURE: Data that is used to identify and authenticate the sender and integrity of the message data.

.EXE FILE: Executable file: used by programs to install and run on computers.

FIREWALL: Hardware or software designed to prevent unauthorised access to a computer or network over the internet.

Digital Ship

THE MARITIME BIG DATA FORUM @ NOR SHIPPING 2017

OSLO - MAY 30

Shipping is waking up to a new digital age, and two of the most important issues within the maritime transport system, where digitalisation is creating increased opportunity for development and innovation, are operational efficiency and safety.

Much has been made of new and improved integrated platforms designed to influence both key elements, and in the last 12 months we have seen various stakeholders launching "ecosystems" designed to improve integration and thus drive both efficiency and safety; between the various systems on-board, from ship to shore, as well as between different onshore devices.

Digital Ship's Maritime Big Data Forum @Nor-Shipping will investigate how data sharing and collaboration is evolving in the maritime sector and changing the way shipping companies operate, now and into the digital maritime future.

Three highly focussed sessions will include plenary and panel discussions:

Session 1: An Overview of New Integrated Data Sharing Platforms

- How have these ecosystems and platforms arisen and why does the maritime sector need these now?
- What are the drivers for developing these?
- What are the opportunities for new and existing stakeholders to offer innovative services by leveraging Big Data and Internet of Things technologies?

Session 2: Protection in the Big Data Era

- How is safety and security driving new platform developments?
- What role does/should regulation play in the future of open data exchange?
- How is the industry addressing the increased cyber threat Big Data initiatives represent?

Session 3: Survival of the Fittest: The Business Case and Future Legacy of Big Data Ecosystems

- How can shipping companies use these platforms to optimise their operations in a data-rich future?
- Where does the revenue come from in a future of open data exchange?
- How can the industry leverage this technology to build a more efficient future?
- How can data owners be incentivised to share information that has previously been considered a competitive advantage?

Digital Ship looks forward to welcoming you to the Digital Ship Maritime Big Data Forum in Oslo.

Date: Tuesday, 30 May 2017, 09:00 – 17: 00

Venue: Thon Hotel Area, adjacent to Norway Trade Fairs

https://www.norshipping.thedigitalship.com/

ECDIS AND CYBER SECURITY

There is much confusion about Electronic Chart Display and Information Systems (ECDIS) and the levels of cyber risk. Even we have become a little mixed up at times, so we are grateful to Chris Lowe, Senior Lecturer (Ship Simulation) and ECDIS Course Manager from Warsash Maritime Academy, for plotting the right course ahead for us all.

Electronic Chart Display and Information Systems (ECDIS) have now become common across all types of vessels with many being required to fit ECDIS, and others fitting it out of choice. ECDIS has completely replaced paper charts on hundreds, possibly thousands, of ships with many others in the process of becoming paperless.

ECDIS systems are computer based systems that display official electronic charts on a screen to allow a user to plan and monitor the vessel's movements. ECDIS systems must have position, heading and speed inputs and may have many more.

As with any computer based system, ECDIS systems are vulnerable to cyber security threats but routine cyber security procedures will prevent threats becoming problems.

Getting the basics right is fundamental, so here are some of the questions you need to be asking:

- How do I get updated chart data and permit files into the ECDIS? How safe and secure is the process?
- Who has access to the USB ports? Are USB sticks checked every time, before use? Are dedicated USB sticks provided and securely stored?
- Are there any software updates outstanding? Good communication with your ECDIS manufacturer is essential.
- How secure are all the other pieces of equipment connected to the ECDIS?
- Do all the deck officers know what to do when things go wrong?

If properly used and maintained, ECDIS has the potential to improve navigational safety, however the knowledge and skills of the user are key, whether in routine use, keeping the system secure or responding to problems.

Training for fires and sinking has long been part of life at sea, training for problems with essential computer based systems must become as integral to the shipboard routine if we are to operate modern, computerised vessels safely and efficiently.

Chris Lowe qualified as an OOW in 2000 after a Trinity House Cadetship then joined the RFA, leaving as Navigator to become the ECDIS Course Manager at Warsash Maritime Academy in 2010.

WORK/LIFE DIVIDE

It can be tempting to use work computers for personal use, but DON'T.

To reduce risk, separate personal and work life. When using your work computer only for work purposes, you will likely visit fewer websites, install fewer applications, and generally reduce your overall attack surface.

To further protect the ship or company systems, the IT team should tightly control administrative credentials, and they should monitor and regularly review newly installed applications, and block categories of websites at our perimeter.

Onboard ship, seafarers should be encouraged to use personal devices, so the temptation or need to use the ship's PCs or systems are reduced. Human nature can cause problems, so it is important to limit the need or temptation for crews to cross the work/life divide.

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: MARITIME CYBER RISK INSURANCE

Novae
LOOKING FORWARD

TALKING CYBER SENSE: MICHAEL SHEN Head of Cyber Innovation at Novae Group shares his thoughts on the past, present and future of cyber insurance policies. In a market that grew out of the needs of different industries, the specific demands of maritime need addressing

The first cyber insurance policies were written back in the early 2000s out of the Lloyd's of London insurance market and this has since become an estimated $4bn global market.

Whilst the early adopters of this product lay predominantly in the retail, healthcare, hospitality and education sectors, it has since moved through into the manufacturers, utilities and lawyer segments, as coverage evolves and as awareness of the exposures and cyber coverage gaps within traditional insurance products increases.

Is maritime therefore the next cyber frontier? There seems a clear opportunity for cyber insurers to provide a valuable product that fills existing cyber coverage gaps.

Firstly, there will often be a cyber exclusion within many marine insurance policies, meaning any property damage, bodily injury or other loss triggered by a cyber event will be excluded. The cyber insurance market has provided gap coverage to address this and continues to do so.

Many of the existing standalone cyber insurance policies themselves also provide relevant coverage, but we need to do far more to build awareness of this and to create language that resonates with the maritime industry.

We already cover the costs of restoring damaged networks and cyber extortion, something that would be equally useful to a maritime risk as a land based risk. Equally we already cover business interruption and extra expense arising out of network interruption, and whilst this would extend to loss of hire, affirmative language to this effect would be better. Regulatory privacy fines are covered, but these are of less interest to a maritime risk than regulatory fines arising out of the inability to leave port due to a cyber event.

The use of electronic bills of lading and transition away from physical documentation creates a further exposure that a cyber policy could respond to, covering subsequent income loss and liabilities arising out of a cyber event, as well as IT forensic costs incurred in restoring this data. These are all focal maritime cyber risks that can be addressed by the cyber insurance market as we move through this next frontier.

https://www.novae.com/

CYBER MEETS SAFETY MANAGEMENT

The parallel issues of cyber-related and operational risks have been widely debated in the International Maritime Organization (IMO) recently. As such, it seems there are increasing signs that flag States are pushing for new rules that would see cyber threats being "appropriately assessed and managed".

These moves would bring cyber risks firmly in line with other threats at sea, which are dealt with through the International Safety Management Code (ISM Code).

The United States has been particularly vocal in this regard, leading calls to ensure that cyber issues are dealt with through the existing management processes. In a paper submitted to the IMO's Maritime Safety Committee (MSC 98/5/2), the US has analysed the direct link that cyber risk management and the ISM Code have.

As a result, the US has proposed the management of cyber risks aboard vessels to be accounted for through a vessel's existing Safety Management System.

The paper rests on these key issues:

- **Section 1.2.2.1 of the ISM Code** requires companies to "assess all identified risks to its ships, personnel and the environment and establish appropriate safeguards.

Cyber-related risks in shipping have been broadly identified and are commonly understood. As such, they need to be assessed and appropriately mitigated in accordance with the objectives and functional requirements of the ISM Code

- Given the widespread use of cyber systems across the industry, it is reasonable to expect that any present-day ship is vulnerable to cyber risks; therefore, it is reasonable to expect their Safety Management Systems will incorporate appropriate instructions, procedures, training requirements and lines of authority.

Evidence of this will be clear upon the review of the Safety Management System. This also satisfies the functional requirements in **section 1.4 of the ISM Code.**

- The ISM Code encourages companies to take into account any guidelines or standards recommended by the IMO, flag Administrations, classification societies or maritime industry organizations. In this regard, companies may find the interim, non-mandatory guidelines contained in **MSC.1/ Circ.1526** provide useful guidance when assessing risk and implementing risk mitigation measures.

If the MSC agrees to the submission, it would mean a draft resolution would require that cyber risks are appropriately incorporated in vessels' SMS no later than the first annual verification of the company's Document of Compliance after 1 January 2018.

This means some companies could have just a year to get their systems in place while all others would follow over the next five years.

www.becyberawareatsea.com

think@becyberawareatsea.com

With thanks to our Supporters