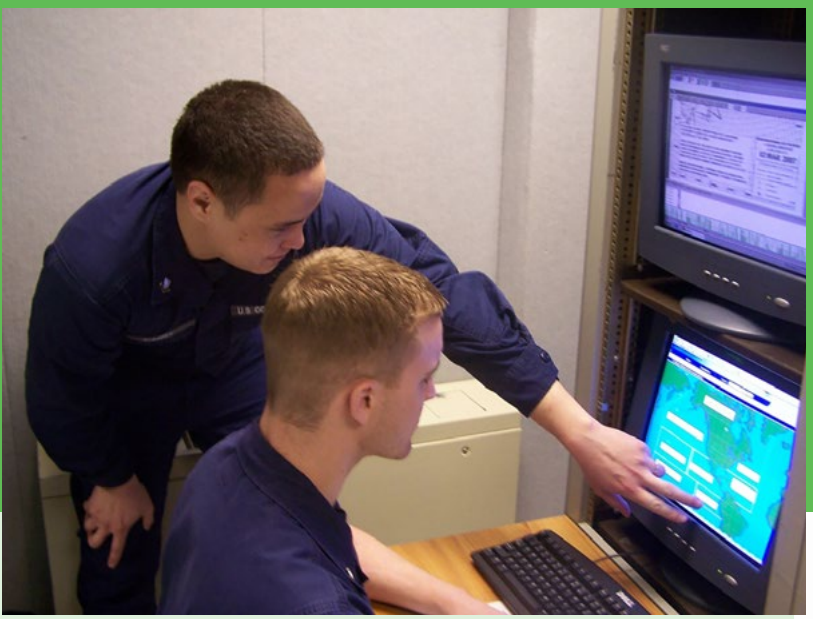

#12

NOV:2017

PHISH & SHIPS

BE CYBER AWARE AT SEA

Kindly sponsored by

CSO ALLIANCE MARITIME

WELCOME

Welcome to issue 12 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".

When the UK's National Health Service (NHS) was attacked and succumbed to the WannaCry ransomware attack it caught headlines around the world. Now a report into the attack and response has (unsurprisingly) found that NHS computers were not being updated. Without the necessary patches, they were incredibly vulnerable to cyber attacks. This is a chance for shipping to learn a key, and simple, message.

In the past month more attacks have been reported, and so too have worrying security weaknesses. So, we need to do more. There is a need for training - 84% of seafarers in a recent survey said they lack training. This has to change. We also need to tackle the use of USB sticks onboard.

Our campaign director Jordan Wylie has been out and about speaking at events, and it is clear that our work is only just beginning. 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.

DOES SHIPPING CARE ENOUGH?

Does shipping care enough about cyber security? That was the question posed by Moore Stephens cyber security partner Steve Williams recently. Williams, speaking at the launch of a new cyber training initiative, said "It's the same with every industry. Nobody cares until there's a problem. It's not a criticism of the [shipping] industry, it's just a fact."

The launch of a new cyber security training programme developed by Videotel in partnership with BIMCO, was a chance for the industry to ask some tough and searching questions about the current response to cyber security.

Members of a panel speaking at the launch event cited a general lack of concern across the wider shipping industry as a key obstacle to improving cyber security. Williams added that cyber attacks were pervasive throughout all business, government and NGO sectors. "50-90% of organisations will get hit by a cyber attack. Why should [shipping] think that we're any different?"

The panel – which, in addition to Moore Stephens' Steve Williams, consisted of Cribb cyber security technical director Patrick Carolan and BIMCO manager Lars Gullackson - discussed the importance of 'cyber hygiene' on board, the importance of further cyber security regulation and the need for shipowners and managers to invest more in cyber security. It is clear there is much work to be done.

They stressed that a cyber attack can severely impact and impair vessel performance. Many cyber incidents on board are triggered accidentally by seafarers opening phishing email attachments or hyperlinks, or using infected removable media. The newly launched training programme explores how to minimise the risks by making personnel more aware of their cyber role and responsibilities.

ANOTHER SHIPOWNER CYBER ATTACK

Another month, another cyber attack; this time BW Group was targeted by computer hackers.

The Singapore-based shipowner confirmed that they had suffered an "unauthorised access" though they stressed that actions were taken to rectify the matter so that internal and external communications to customers and stakeholders were not impacted, stressing that it was "business as usual".

However, as with a swan, underneath the surface a great deal more was going on: the company had to implement a security response and work around system down times. Their IT department, with the assistance of external consultants, then worked to reinforce their cybersecurity infrastructure.

BW Group said the cyber attack was not ransomware and gave no further information on any financial or data loss due to the unauthorised external access. There was also no indication of whether the culprits had been identified or traced.

This is likely to be an ever more common news story unless changes are implemented.

CYBER EVENTS FOR YOUR DIARY

15th-16th November 2017, Shipping2030 North America, New York USA

https://maritime.knect365.com/shipping2030-northamerica/

6th-7th December 2017, Maritime Information Warfare 2017, London UK

https://www.smi-online.co.uk/defence/uk/conference/Maritime-Information-Warfare

EXPERT WAKE UP CALL FOR SHIPPING

As the industry rouses itself to the threats of cyber incidents, they turn to the expertise of cybersecurity sector leaders. These companies are enlightening us all with the full scope of what a hacker can do with the vulnerabilities presented to them.

Recently a cyber researcher's blog post raised the spectre of weak passwords, easily exploitable satellite antennae and other misconfigurations that could be easily identified by conducting a simple search on Shodan (a search engine for internet-connected devices).

The blogger, has shaken the industry with examples of private network terminals that are all too easily accessed, and which contain details and data which are potential gold dust for fraudsters who could access this information easily by hovering over the page.

With such information they can facilitate phishing attacks on individual employees. Bloggers have also raised concerns as to the threat employees present themselves by accidentally giving threat actors access to corporate networks and how other security flaws via satellite communications equipment open the doors for hackers to location and cargo data.

A key issue is in how industrial control systems were designed long before organisations understood cybersecurity yet they are now increasingly reliant upon more varied technology. In a 24/7 environment where the internet never sleeps, we need to plug the gaps and protect from all known vulnerabilities.

CYBER REPORTING RESPONSIBILITIES

Knowledge is power; and the more the shipping industry knows of its vulnerabilities the better it can protect itself from threats. However, as the media is saturated in reporting of cyber incidents, we all need to be aware of how we discuss security issues so as to not simply better prepare the hackers.

Public discussion of potential vulnerabilities that face shipping is an important part of opening the dialogue between cybersecurity experts and the industry, but we must remember the most beneficial work for an organisation will be done behind-closed doors, one-to-one with their expert help.

COASTGUARD CYBER COLLABORATION

The United States Coast Guard is increasingly concerned that ships can all too easily fall victim to "bad actors, hackers, and nuisance cyber agents". However, they have been quick to stress that many of these incidents can be prevented or mitigated by embracing a culture of cyber risk management.

The USCG wants to see technical solutions like virus protection software and firewalls become second nature - but they also stress that these are ineffective if they do not sit alongside robust training and professional skills.

Working in partnership with industry associations, Class Societies, and other Flag States, they are pleased to have produced the International Maritime Organization (IMO) Guidelines on Maritime Cyber Risk Management, and a subsequent Resolution Maritime Cyber Risk Management in Safety Management Systems.

The USCG states that these documents affirm that safety management systems should take cyber related risks into account, in accordance with the objectives and requirements of the International Safety Management Code.

In the same way the maritime industry developed a robust safety culture, we must now focus on the development of a culture of cyber risk management. In much the same way as crews train for fire and flooding emergencies, crews should also train for cyber incidents.

The IMO Guidelines on Maritime Cyber Risk Management stress the importance of a continuous and cyclical process of identifying risks, protecting from those risks, detecting incidents, responding to incidents, and recovery to normal operations. It is vital that shipping companies embrace a culture of cyber risk management at all levels of their organization in order to achieve a robust cyber posture. Training, exercises and drills are a critical component of a cyber risk management regime and should be adopted into Safety Management Systems.

The Coast Guard Office of Design and Engineering Standards is working to develop additional best-practice guides and industry standards which can be used to assist companies with implementing cyber risk management policies. While they are also collaborating with the National Institute of Standards and Technology, National Cyber Center of Excellence to develop sector-specific profiles which adapt the NIST Cybersecurity Framework to specific asset classes. This collaboration has already produced profiles for bulk liquid transfer facilities and offshore platforms, and will soon be kicking-off a profile on electronic navigation and automation systems.

THE USB CURSE...

USB drives are everywhere. However, for all the convenience and power of the USB drive, there are some serious dangers to be wary of. Almost everyone carries them and this has perhaps made us overly trusting of the technology. We plug them in, pull them out, and plug them in again without a second thought to issues of security and protection.

There should be no overlooking or forgetting USB security. We often hear tips and tricks related to online cybersecurity: Don't click random email links. Don't visit shady websites. Keep your firewalls up and your antivirus databases updated. Use safe passwords and stay vigilant against keylogger infections. Yet, an infected USB can cut straight to the chase...

In fact, USB drives are like mosquitoes. They have the potential to pick up infections when plugged into an infected computer and they can spread those infections almost instantaneously as they're plugged into other devices. This is why it's so important that you keep not only your computers clean but your USB devices as well using regular scans and antivirus programs.

USB drive dangers require constant vigilance. You might use the same USB drive for years without a hitch, then one day you could grab a file off of your friend's computer and end up infecting your home network with something serious. USB security is not often on the minds of computer users, even the tech-savvy ones, but as long as you are aware and take proactive steps against the potential spread of viruses that piggyback on USB devices, you'll be all right.

TOP USB DRIVE SECURITY TIPS

1. **Block Physical Access**
2. **Use passwords or actual locks**
3. **Create policies and training programs**
4. **Scan devices for virus or malware infections**
5. **Warn crew of dangers**

CYBER SECURITY FOR THE MARITIME SECTOR

Are regulations necessary to counter the cyber threat in the maritime sector? That is the leading question to be asked at a major upcoming conference on cyber security. While it is true that some advances have been made and the maritime sector is waking up to the cyber threat. The question remains, is this enough? Is there a need for regulations? What role do international organisations such as the IMO and the European Maritime Safety Agency (EMSA) play on enforcing international regulations?

This year has seen cyber security incorporated in the US Maritime Transportation Security Act of 2002. While the British government is looking to impose fines of up to £20 million to companies if there is proof that they have not taken effective cyber security measures. Key to this is the fact that it only applies to companies who do not assess their risks appropriately, and who have not taken relevant measures nor communicated with authorities. Although the draconian Directive is not specific to the maritime sector, it will include ships, port facilities, ports and vessel traffic services.

So all parts of the transport chain will have an obligation to report any cyber occurrence that has disrupted the continuity and privacy of their services without any delay. With this forced disclosure, companies will be indirectly bound to protect their data more efficiently and reduce the impact of cyber threats, protecting both their clients and their own reputation.

The European Union is set to act too. and the European Maritime Safety Agency (EMSA), is supporting EU Member States by providing best practices and helping them with two aspects: promoting a general cooperation and harmonisation of cyber security strategy and improving incident and resilience reporting.

The former is done by identifying and developing incentives to adopt good practices, promoting the development and adoption of Information and Communication Technology solutions and drawing suitable standards from the most relevant working practices. The latter involves sharing of relevant information to the concerned parties, developing a coordinated response to incidents through the help of expertise, in order for the authorities to follow up with regulations, threat analysis and identifying good practices.

If you want to find out more, join the inaugural Cyber Security for the Maritime Sector conference to learn more about the latest industry best practices from a panel of senior speakers.

The inaugural Cyber Security for the Maritime Sector conference will be held in December 2018

https://cybermaritime.iqpc.co.uk/

ASTONISHING LACK OF TRAINING

A survey by independent satellite communications provider, NSSLGlobal, has revealed that, although crewmembers understand that they are partially responsible for maintaining cybersecurity on board their vessels, an astonishing 84 percent claim to have received limited, or no cybersecurity training from their employers.

NSSLGlobal's survey of crew reveals that although 64 percent of crews accept responsibility for security of onboard IT systems, the vast majority of maritime employers are not doing enough to help crews understand the risks they face, and how to avoid them.

With the majority of attacks being targeted at people rather than IT infrastructure, the 'human factor' is widely considered to be the biggest risk in cybersecurity at sea. The maritime industry needs to provide thorough cybersecurity training and education to its crews to keep these risks to a minimum.

"The lack of cybersecurity training is a real concern, but largely tallies with what we're seeing in the industry", commented Nigel Quinn, IT Security and Enterprise Manager, NSSLGlobal. "With threat vectors and the nature of security threats constantly evolving, the maritime industry needs to be just as prepared as any other industry to tackle the issue head on. NSSLGlobal has been stressing the importance of education for cyber security, and they state that even with the best technical solutions and tools in place, if people aren't trained to a satisfactory standard and don't understand what the threat is, then customers put their systems at risk."

SECURITY IN THE SUPPLY CHAIN

By Sharif Gardner: our regular "Talking Sense" cyber columnist from our good friends at AXIS, formerly known as Novae. Details can be found on their website https://www.axiscapital.com/

Shipping operations are under various threats at different levels – much like any other sector with large and varied suppliers. There are numerous different methods and approaches that cyber criminals will adopt to make money and attacking a company through its suppliers is not uncommon.

Firstly, not all threats are sophisticated. In fact, the majority are still commoditised untargeted attacks that prove successful because of poor practices and accidental introduction of malware or handling of information. Simple phishing or whaling attacks that aim to extract information or apply pressure on a victim to transfer funds in a time pressured scenario are the most common incidents that suppliers will encounter.

Moving up the threat level is a more targeted criminal approach such as spear phishing which targets specific employee(s) in the business in order to gain access to the suppliers systems. This approach is used to infiltrate the system and allows criminals to gain access to information that could lead to more damaging consequences, such as the transference of larger sums of money – commonly known as e-theft.

To mitigate against these types of attacks, it is important to have well trained employees that can firstly identify bogus emails. Identifying these emails prevents the introduction of malware or transference of funds because employees are more aware of the problem.

Secondly, a properly configured intrusion detection system (IDS) would pick up that an intrusion has happened and if known, this would lead to an effective response that deals directly with the threat. However, should this not be prevented or detected, it is critical that before any transfer of large funds that robust checking processes and separation of duties are in place to ensure that no one employee is able to sign off on transfers of a certain amount.

Sponsored by:

CSO ALLIANCE MARITIME

www.becyberawareatsea.com

think@becyberawareatsea.com

With thanks to our many industry supporters....