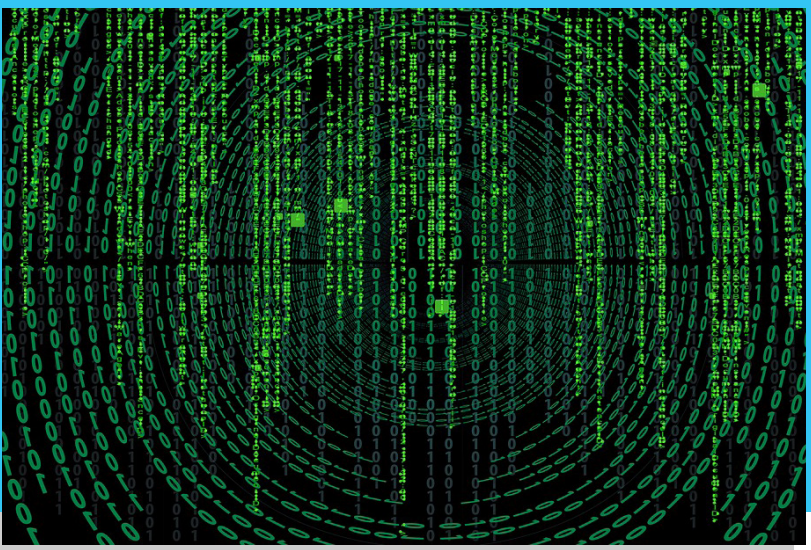

#13

DEC:2017

PHISH & SHIPS

BE CYBER AWARE AT SEA

Kindly sponsored by

CSO ALLIANCE MARITIME

WELCOME

Welcome to issue 13 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".

As ever, there is so much to pack into our monthly newsletter. There is more advice and guidance, and the thoughts of industry leaders. There is also new guidance on how to head off maritime cyber risks.

While the Be Cyber Aware at Sea campaign is working well, the challenges of cyber security are still with us. We are so pleased that our posters are popping up on more walls and bulkheads, the training film, by Fidra Films, has been seen by tens of thousands of viewers, and Phish & Ships now goes to over 30,000 readers. However, there is still so much more to do.

With breaking news that broking giant Clarksons has been hacked, and with the fallout of previous attacks being felt on the bottom line, shipping is in a real battle to stay safe and secure. Together we can make a difference, so take a look inside and find out what you can do to get cyber aware.

We have a favour to ask too. As yet more awards beckon, we are asking for your support in voting for us at the Safety4Sea 2017 awards. More details inside.

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

THE MARITIME CYBER EQUATION

$$S = H + P + E$$

Writing in the US publication MarineLink recently, cyber security experts Scott Blough of Tiffin University and Kyle Johnson of Indiana Tech sought to explain how the maritime industry needs to think about dealing with cyber security.

They stress that for many industries, cyber security is about target hardening and perimeter defence. This makes sense, as cyber security is implemented in much the same way that physical security is implemented. Like a medieval castle design, there is defence in depth and one simple equation sets it out:

Security = Hardened Target + Perimeter Defence

Security assets such as fencing, ingress and egress areas (think doors, drives, sidewalks), guard stations and cameras. These are the things that can be seen and touched – they provide reassurance. In the cyber security world, this translates into firewalls, intrusion prevention systems, intrusion detection systems and antivirus software. The reassurances aren't physical, but they are in place and can work.

So, what of shipping? Well, the maritime system has long been a place where physical security has taken a very high priority. Now, though, it is time to take that approach and apply it to the new threats which are emerging.

According to Vircom (2017), human error was responsible for 52 percent of data and security breaches. Thus, humans are the weakest link in any organisation's defence-in-depth strategy. Meanwhile, according to the 2017 Verizon Data Breach report, more than 800 breaches that occurred in 2016 were the result of a social attack, such as phishing.

The human security risk is very real, in part because of the lack of education and training about cyber security. This is exacerbated by the lack of perceived consequences for violating cyber security. For shipping, the phrase "out of sight, out of mind" can ring true and have serious consequences if end users are not well educated.

It is evident that the current security formula is inadequate for the future of maritime cyber security. Perhaps a strong cyber security awareness training programme that links behaviour to consequences might prevent the next NotPetya cyberattack or drug smuggling operation in your organisation. Adding that education piece to the definition of security will only strengthen the overall security posture of maritime organisations. In the end, the fence is only useful if people know its purpose.

Security = Hardened Target + Perimeter Defence + Education

Read the full article at: https://goo.gl/sAVJf9

SAFETY4SEA has announced the 2018 SMART4SEA Awards, and there is a strong cyber security feel across a range of the categories. Even better news is that the winners are to be chosen by the voting public. So, you can have your say on the campaigns, training and innovations which have made a difference to your views on maritime cyber security.

The "BeCyberAware" film has been shortlisted in the 2018 SMART4SEA Awards in the Cyber Security category, which is to be awarded to any organisation that "provided a significant achievement, breakthrough or contribution in any aspect of Cyber Security in shipping". In an incredibly strong category, there are entries from companies who have also been working hard to assist shipping in dealing with the cyber risks facing it. The shortlist for the award is made up of Asket, Aspida, Hudson, Fidra Films, KVH Videotel and Steamship Mutual.

With your interest in the industry, we urge you to take a look and make your vote count by helping choose the SMART4SEA Cyber Security Award winner. See https://www.safety4sea.com/2018-smart4sea-awards/ for details.

It is not only the Be Cyber Aware film which has made the awards nominees list. Be Cyber Aware At Sea is delighted to have also been nominated for the SMART4SEA Training Award. This award recognises "any organisation that provided a significant achievement, breakthrough or contribution in any aspect of Training with respect to smart shipping".

Again, this is an extremely competitive category, with some wonderful companies, but please do vote for us. Winning isn't everything – but it does help to further the aims of the campaign and raise awareness. So click for Be Cyber Aware...

VOTE HERE: www.safety4sea.com/smart4sea-awards/

VISIT OUR SITE AND SHARE YOUR VIEWS

www.becyberawareatsea.com

think@becyberawareatsea.com

NEXT GENERATION MARITIME CYBER PROFESSIONALS

One of the primary roles of the Be Cyber Aware at Sea campaign is obviously to raise awareness. There is another element though, and that is to support those working, or wanting to work, in maritime cyber security. As such, we were so pleased to be contacted by Charlotte Morton, a Masters student at Liverpool John Moores University. Charlotte asked us for help in supporting her studies and rallying people to provide data for her dissertation.

Well, it seems that you responded to the call. Helped by the maritime community, Charlotte was able to complete her studies and has now graduated. She, has even taken the time to drop us a line and thank Be Cyber Aware at Sea for our support. Here are her words...

"I am so pleased and proud to say that I have passed the MSc Maritime Operations Management course through LJMU. After deciding cybersecurity was the focus of my dissertation, I was directed to the Be Cyber Aware at Sea website. The site provides a wealth of guidance and awareness advice and was truly instrumental in providing me with the background knowledge I needed to start my literature review research. As with any dissertation, primary data is gold, and I am very pleased to say that the people I contacted very kindly completed my primary data questionnaire, which made all the difference."

We are so pleased to have been able to support Charlotte - and look forward to helping more students become the next generation of maritime cyber professionals.

US CYBER BILL

The US has passed legislation aimed at addressing cyber security concerns at the country's ports, H.R.3101 - Strengthening Cyber security Information Sharing and Coordination in Our Ports Act of 2017.

It was spurred the global NotPetya ransomware outbreak, and the legislation's main goals are to improve information sharing and collaboration in facing up to cyber security risks at ports in the US.

It requires voluntary guidelines for cyber security risk reporting, to develop and put into practice a maritime cyber security risk model and to make recommendations on enhancing cyber information-sharing.

Read the Bill in full here: https://goo.gl/VqsxUZ

THE UNMANNED CYBER CONUNDRUM

As the International Maritime Organization (IMO) announced, it will begin to consider updating the International Convention for the Safety of Life at Sea (SOLAS) to allow cargo ships with no captain or crew to travel between countries. As the industry prepares for unmanned ships, there are still many remaining doubts, not least in the face of a cyber attack.

According to a new report from Clyde & Co and the Institute of Marine Engineering, Science & Technology (IMarEST), almost two-thirds (64%) of global marine industry executives believe there is uncertainty surrounding liability issues relating to unmanned ships should a vessel be involved in an incident as a result of a cyber attack.

A survey of 220 marine industry executives from across the world also found that there is a lack of clarity around collisions involving unmanned ships, with 59% of survey respondents agreeing there is confusion surrounding the regulations in this area.

IMarEST Chief Executive David Loosley said: "Technology is today advancing at an unprecedented rate and promises a host of new solutions for the maritime industry in terms of improved efficiency, safety and environmental performance. However, we should not be blinded by the benefits. We must also remain alert to the potential risks. This joint research report examines these vulnerabilities and how they might be addressed and is an important starting point for the industry to begin preparing for the future."

Concerns about cyber risk also weighed heavily in the considerations of respondents. Over two thirds (68%) fear that unmanned ships present a greater cyber security risk than traditional ships.

Clyde & Co and IMarEST acknowledged that unmanned ships are likely to have a greater array of digital infrastructure than traditional ones, in order to ensure that shipowners and operators are able to control and track their ships remotely.

The law firm stressed that marine executives are right to be concerned about the potentially increased threat of cyber attack as a result of the use of unmanned ships. However, it is probably worth mentioning that the maritime industry as a whole has been criticised for being a bit slow in reacting to existing cyber threats, including fully crewed vessels and that the biggest threat to any organisation's cyber security posture is still, in fact, human error.

Read the full article here: https://goo.gl/XbuUD2

CYBER ANGEL EARNS WINGS

navarino

Developers of the first cyber security service designed and tested specifically for maritime use say their product has already prevented its first real-world cyber-security attack on a shipping target.

The new cyber security platform – called Angel – was developed by Navarino and formally launched at the end of October. Navarino's solutions architect Stratos Margaritis has spoken to the media about the attack it prevented.

"It was a denial of service attack that was immediately caught and blocked. The attack was isolated from the network. That's how Angel operates." Mr Margaritis was unwilling to specify which company had been targeted in the attack. He said that cyber attacks and security breaches of shipping systems are often kept secret and cited other unreported cyber incidents he is aware of within the shipping industry.

"I do know of two or three of them [unreported cyber attacks], yes. They [shipping companies] have been compromised from inside … but I don't know if they want to go public with it."

Mr Margaritis said that crew posed a threat to cyber security in shipping, and described an incident where a crew member infected a vessel's ECDIS system.

"I know of one [attack] where someone actually put his phone to charge on the ECDIS – and the ECDIS was compromised. Things like that can happen, and the crew is not exactly aware of … the mass damage they can do."

Find out more at http://navarino.gr/cyber-security/

FLAG ACTING ON CYBER

A recent maritime event hosted by the Marshall Islands Vessel Registry, has shone a spotlight on the threat to the shipping industry.

Expert speakers joined the world's second largest flag State in hammering home the message about maritime cyber risks. Speaking at the event, HudsonAnalytix founder and chief executive Cynthia Hudson said that "security measures are simply not keeping up with attacking measures". Stressing that cyber security often only becomes important when there is a loss.

Meanwhile, Paul Vlissidis, technical director and senior advisor to the NCC Group, believes that shipping is no longer dealing with just specialists. It seems the target profile of shipping has changed, as hackers are selling infiltration kits to criminals.

Phil Tinsley, head of maritime security at BIMCO, stated: "A ship, although an independent unit, can compromise a company's reputation. A survey shows that malware is the main threat; it can often come aboard carried on a USB stick loaded with movies, or via phishing emails."

Perhaps the most positive assessment was from the North of England P&I Association's deputy director for loss prevention Colin Gillespie. He believes the risk – like many others – just has to be managed, and says that the shipping industry is doing a good job on that front.

However, he did stress that awareness, must begin on board. So once more we come full circle back to the aims of Be Cyber Aware at Sea...people on ships need the training, tools, resources and awareness to act.

ROLE OF THE CYBER SECURITY OFFICER

In light of the recent DFT publication Code of Practice: Cyber Security for Ships, it is important to stress the need for having someone within the organisation who is responsible and accountable for managing cyber security.

The normal response to the question "who is responsible for cyber security?" is often "my IT department." IT departments are there to implement what the business needs – which is normally availability of information – they are not necessarily the information risk owners or policy setters.

When identifying the role of a Cyber Security Officer (CySO (DfT)) it is important that the role sits between the technical IT teams, the risk management function, the legal and regulatory stakeholders, and is aligned to business objectives. The CySO should have responsibility for implementing a cyber security plan that incorporates the following: Prevention of cyber incidents by educating senior and frontline management and end users, detection of incidents with a blend of technology and analysis of data, and execution of a response and recovery programme by implementing the business continuity and disaster recovery plans.

The dedicated person needs to have the seniority to manage supply chain cyber risk for secure procurement activities and be accountable to contracts set by clients in relation to their cyber exposure.

Whilst the DfT Code of Practice sits within the jurisdiction of the UK, it provides practical guidance that is applicable to the wider shipping industry. It is a useful tool for IT teams and senior officers, however it can also provide a valuable framework for ship owners wishing to understand how to assign budget and insurers for benchmarking risk.

Sponsored by:

CSO ALLIANCE MARITIME

www.becyberawareatsea.com

think@becyberawareatsea.com

With thanks to our many industry supporters....