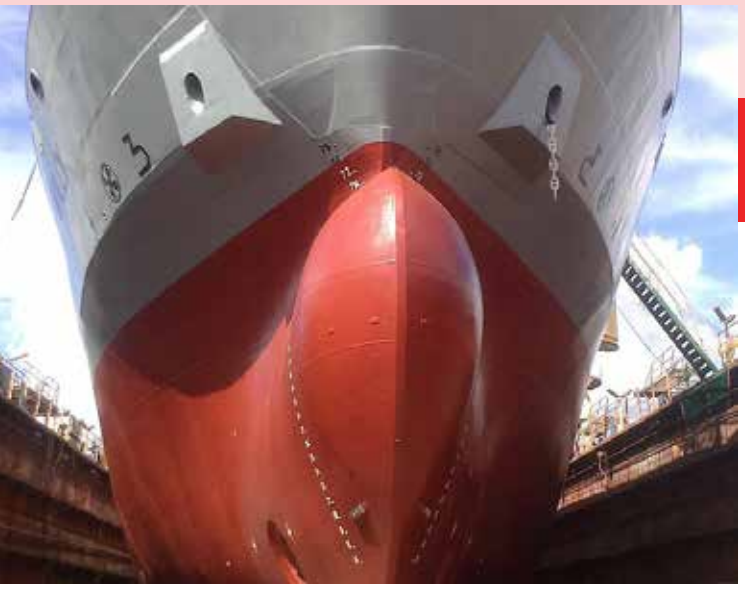
#22
SEP: 2018

PHISH & SHIPS

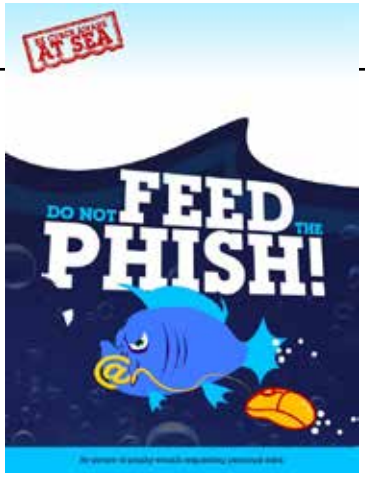


Kindly sponsored by

TDG
Cyber Marine

SMART4SEA TRAINING AND EDUCATION AWARD 2018
UNSUNG HERO OF INDUSTRY: HIGHLY COMMENDED, SAFETY AT SEA AWARDS 2017
BEST CYBER AWARENESS CAMPAIGN, INTERNATIONAL CYBER SECURITY AWARDS 2017

2018 Training Award SMART4SEA



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

Issue 22 is generously sponsored by TDG Cyber Marine, an expert player in the cybersecurity industry. The company offers leading edge and patented technologies to provide a more robust defence against the escalating threat from cybercriminal activity.

This month we look at the importance of planning when it comes to cyber security. When attacks come, and they will come, it is vital that companies have the ways and means to deal with the problems. New evidence in the wake of high profile maritime industry attacks has also shown how important it is for companies to ensure they keep their businesses running.

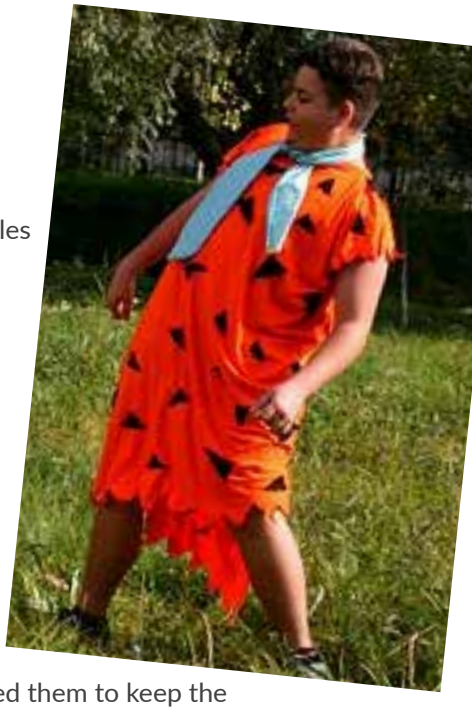
Another key debate this month is the importance of reporting incidents. One of our regular contributors shows just how much we have to gain from sharing and helping others to avoid cyber problems and security risks.

We look at an assessment of the industry's preparedness for cyber attack - spoiler alert - it's not good. While we also explore how problems can affect the very value of a company.

The aim of Phish and Ships is to ensure that cyber awareness at sea is taking hold, and we are very proud to play our part. See https://www.becyberawareatsea.com/ for more details and please support our campaign and don't forget to download our free resources, including our award winning (and free) posters.

Visit https://www.becyberawareatsea.com to learn more.

ATTACKS SEND FIRMS BACK TO STONE AGE



If you want an image of what it may be like to be an Executive within a shipping company hit by a cyber attack, perhaps imagine Fred Flintstone running in his car.

That is the message from the journalist Martyn Wingrove, who sees cyber attacks as being able to take shipping companies and ports back to the "Stone Age" almost instantly.

We will explore the lessons learned in more depth later in this issue of Phish & Ships, but thankfully we are all seemingly beginning to learn and appreciate how important it is to protect against cyber attacks, but sometimes it is only by seeing the real damage that we can appreciate the impact cyber attacks can have on a business.

According to Wingrove, "Cyber attacks can take shipping companies back to the digital Stone Age in one fell swoop. The recovery, however may not be so swift."

So, it is perhaps good for those who haven't knowingly been infected yet to use shipping's increasingly high-profile cyber attacks to learn lessons and to appreciate what preparation is necessary to head off cyber woes.

The recent cyber attack on COSCO Shipping Lines' North American operations is being held up as an example of what can go wrong, and of how companies are forced to adapt to keep business flowing.

The COSCO attack reportedly brought down its email system and disrupted telephone communications at its customer service centre near Los Angeles. This meant that urgent action was needed to somehow keep the business going.

One of the oft forgotten rules of crisis management is to keep the business running while bad things are going on all around. This can be especially hard when any emergency response is naturally focused on the extraordinary, while the rest of the company has to somehow retain its equilibrium.

For COSCO it was vital to find out what had gone wrong, and the origin of the attack. This then allowed them to keep the malware that caused the attack physically isolated. In doing so, they managed to prevent the malware from spreading, which would have been disastrous. The prompt action meant that in just four days the company could claim to be back to normal.

During the peak of the COSCO problem, employees were forced to turn to private Yahoo email accounts for processing shipments. When the Not-Petya virus hit container shipping giant AP Møller-Maersk employees were forced to resort to pen and paper to keep the business afloat after their attack.

The lessons are that business continuity is key, and resilience means being able to keep moving forward - even if you do look like Fred Flintstone in the process.

TEN BASIC CYBER TIPS

1. ***You Are A Target*** - Act accordingly
2. ***Eight Characters Is Not Enough*** - Practice good password management
3. ***Lock It Up*** - Never leave your devices unattended.
4. ***Practice Safe Clicking*** - Always be careful when clicking on attachments or links in email.
5. ***Beware Of Browsing*** - Browsing banking or shopping, should only be done on a device that belongs to you, on a network that you trust.
6. ***Back It Up*** - Back up your data regularly, and make sure your anti-virus software is always up to date.
7. ***Physical Cyber Safety*** - Be conscientious of what you plug in to your computer.
8. ***Share Less Sensitive Information*** - Watch what you're sharing on social networks.
9. ***Cut Out The "Middle Man"*** - Offline, be wary of social engineering.
10. ***Stay On Top Of Your Accounts*** - Be sure to monitor your accounts for any suspicious activity.

CYBER ATTTACK THEORY BECOMES REALITY

At The Black Hat conference in Las Vegas, a researcher has claimed that a theoretical threat to ships, planes and military through hacked satellite antennas is 'no longer theoretical'.

As discussed at the event, satellite communications could be hacked to carry out "cyber-physical attacks", turning satellite antennas into weapons that operate, essentially, like microwave ovens.

It seems a number of popular satellite communication systems are vulnerable to the attacks, which could also leak information and hack connected devices.

Ruben Santamarta, a researcher for the information security firm IOActive, carried out the study, building on research he presented in 2014. "The consequences of these vulnerabilities are shocking," Santamarta said. "Essentially, the theoretical cases I developed four years ago are no longer theoretical."

The attack works by connecting to the satellite antenna from ashore through the internet, and then using security weaknesses in the software that operates the antenna to seize control.

From there, the potential damage varies. Santamarta described one "cyber-physical" attack: repositioning the antenna and setting its output as high as it will go, to launch a "high intensity radio frequency (HIRF) attack".

"We're basically turning Satcom devices into radio frequency weapons," Santamarta said. "It's pretty much the same principle behind the microwave oven." Even if the antenna can't be used to physically injure soldiers, passengers or crew, a HIRF attack can also cause physical damage to electrical systems.

US TACKLES CYBER THREATS

In an initiative that perhaps the shipping industry can learn from, the United States Marine Corps a couple of years ago launched a hacking support unit.

The Marine Corps Cyberspace Warfare Group (MCCYWG) has now ramped up to full operational capacity and supports the US Marine Corps Forces Cyberspace (MARFORCYBER) established 2010.

The move follows the launch of other hacking units and implementation of new cyber doctrine in recent years. It also matches the movements of Russia and China which have entire branches of their military dedicated to cyber attacks.

MCCYWG provides staff, training, and equips Marine hacker teams for their offensive and defensive operations.

"We're still evolving, but I think five years from now, as the Marine Corps comes online and understands more and more what is happening in this space, the Cyberspace Warfare Group will look much different than it does today." It is described as the "Marine Corps' firewall" to prevent attacks.

The aim of the Unit is to help prevent attacks while hindering the "enemy". Such cyberspace operations ensure that US systems are secure to stop hackers from getting into our systems where our personal identifiable information and everything else is stored.

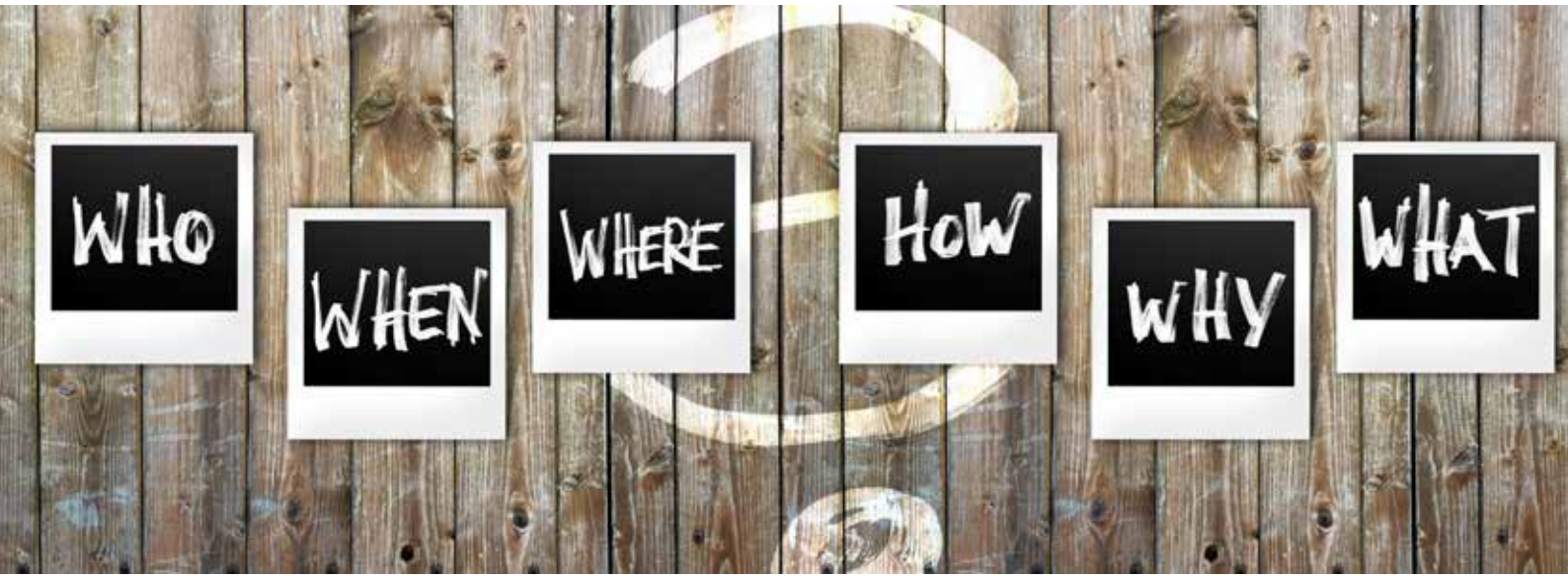
It is not all about defence, there is an offensive side too, and that focuses on what the US forces can do to hinder an enemy.

As part of the MCCYWG development, the United States Marines are even paying "friendly hackers" to cyber-attack them in an attempt to find out their vulnerabilities before an enemy can.

The Department of Defense recruited 100 of the world's top hackers to find security gaps in the military's public websites before enemies does. It's an event called a "bug bounty."

In one night, the friendly hackers found 75 vulnerabilities in the Marine's online defences. Some of these vulnerabilities include information such as where active duty military personnel are stationed.

Marines paid out $80,000 for the hackers' work, and they found out what they need to fix to keep America safe.



WHY IT IS VITAL TO REPORT CYBER ATTACKS...

Gideon Lenkey, Technology Director at EPSCO-Ra shares his thoughts on why it is vital to report cyber attacks and incidents...

Incidents happen every day. Some are not very notable or at least they seem minor. Others you can't miss, like a ransomware attack that stops everyone from using a critical server thus making work difficult or impossible. The vast majority of incidents which occur are never reported regardless of what size they are. Part of the problem is the victims want to keep the incident quiet, but another part of the problem is who do you report the incident to?

For example, just last week we handled a very minor financial incident. The bookkeeper at a company received a call from someone claiming to work for the maker of their bookkeeping software. The individual identified himself and informed the bookkeeper that they could see from their logs that the bookkeeping software was not updating itself. If you are thinking, wait RED FLAG, vendors of off-the-shelf software don't make calls like this, you would be correct! The caller then asked the bookkeeper to allow him access to the machine so he could diagnose the problem. The bookkeeper allowed this and within seconds two things happened, malware was loaded onto the machine and the caller informed the bookkeeper that it would cost $750 USD to fix the update problem. It was at this point the bookkeeper realized the caller might not be who he said he was. Too late, damage done, the company now had an incident.

They had a good incident response plan and remediation wasn't too bad. The malware was fairly benign, just a remote access Trojan that the attacker never got to use, and the company didn't pay the attacker. The whole incident lasted less than two hours end-to-end. So a big sigh of relief and go back to work? You could do that or you could do what we did. The attacker left a call back number which we were able to reach him at and by using our own social engineering skills we got more information out of him including the name and website of the company that was processing the victims credit card payments. We then reported the details to both the bookkeeping software company and the FBI Internet Crimes Complaint Centre. https://www.ic3.gov

Now you might be thinking, okay that's nice but why bother? The information from a single small incident might not seem like much use but when correlated with many other small incidents relevant patterns can emerge. Law enforcement and security researchers can use many small cases to form a larger picture of a malicious actor, their tools and techniques. In some cases the actor can be identified and because of accumulative cost of their many small crimes, can be pursued and criminally prosecuted. So even if it's a small incident you should report it because you might be providing an important piece of a puzzle that an analyst is working on.

So that's fine for everyday financial crime in the US but what about maritime? If you've heard me speak in the last year or so then you've almost certainly heard me stress the importance of an anonymous maritime industry incident reporting service.

While I'm aware of several initiatives, it is still early days. One that is up and running right now and offers a free, simple anonymous reporting web interface can be found here: https://www.maritimecyberalliance.com/.

It's managed by the Maritime Cyber Alliance and while they haven't issued any public reports based on collected data yet, again it's early days. I see the effort as a good step towards maturity for maritime in general. The more data the maritime industry feeds into reporting systems, the better the intelligence we'll get out of it. The bad guys are organized and motivated, we have to be just as organised and motivated ...or more so.

To learn more about EPSCO-Ra see https://www.epsco-ra.com

ACADEMIC MAKES GRIM ASSESSMENT OF CYBER READINESS

A paper published this month by Professor Vivian Louis Forbes makes a grim assessment of the industry's preparation for cyber threats. 'The Global Maritime Industry Remains Unprepared for Future Cybersecurity Challenges' is published by Future Directions International and it makes the following key points:

- The volume, impact and sophistication of cyberattacks have grown at an alarming rate. Worldwide, nearly 17 million attacks reportedly occur each week.
- With around 50,000 ships at sea or in port at any one time, the maritime transport industry is highly exposed to cyberattacks.
- Vessels do not need to be attacked directly. An attack can arrive via a company's shore-based Information Technology systems and very easily penetrate a ship's critical onboard Operational Technology systems.
- The International Maritime Organization (IMO) reacted quickly in introducing guidelines in response to terrorist attacks on shipping, but has arguably been slower in formulating appropriate cybersecurity regulations.
- The maritime industry appears still to be ill-equipped to deal with such future challenges as the cybersecurity of fully autonomous vessels.

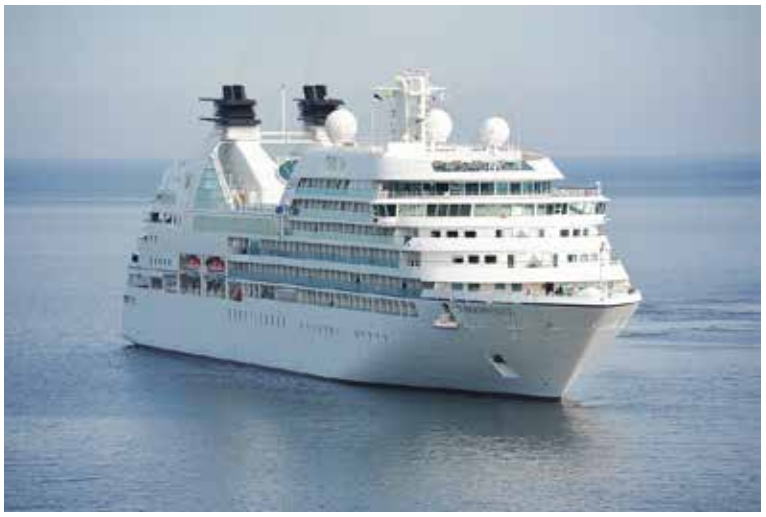
Citing a combination of the industry's heavy reliance on 'electronic commerce ("e-business") in many of its daily business transactions' and the large number of active vessels, at sea or in port, Professor Forbes believes that the maritime industry has a particularly wide exposure to cyberattack threats that can have severe repercussions.

In considering the potential of maritime cyberattacks, Professor Forbes looks closer at trends occurring in the wider non-maritime context of cybercrime. For example, that an estimated US$80 billion to US$120 billion of cyber crime cash is laundered annually shows the scale of the problem facing all industries globally. Much of that cash is laundered via cryptocurrencies and digital payment systems, showing how cutting-edge technology has been highjacked for darker purposes.

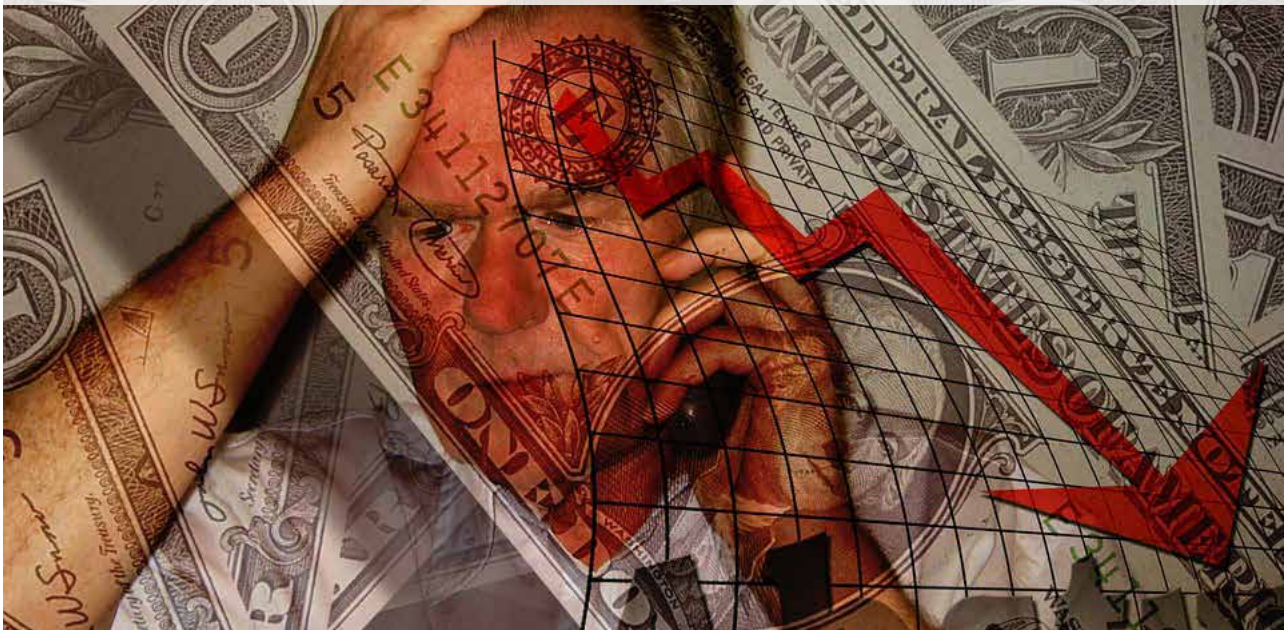
Professor Forbes proceeds to predict that reports of maritime cybersecurity threats and incidents will 'increase greatly', in tandem with more sophisticated technology. In that light, he believes that the industry 'has been relatively slow to realise that ships, just like everything else, are now intricately linked to cyberspace.'

Indeed, Professor Forbes' analysis of the industry's response so far is critical, saying that the IMO have been 'somewhat slow in formulating appropriate regulations' and that the cyber-specific amendments to the ISPS and ISM enter into force too late, leaving the industry vulnerable until 1 January 2021.

Download the full paper here http://bit.ly/2onjIlw



WHEN BUSINESSES FACE THEIR CYBER NIGHTMARE



One of the key messages of the Be Cyber Aware At Sea campaign revolves around the importance of ensuring top to bottom security; any single weakness in the system can be utilised by a cyber-criminal.

Back in November 2017, major shipbroker Clarksons revealed that they had been victim of a cyber attack, affecting the security of some personal information. They took steps to notify the individuals potentially affected and provide them with information and access to resources to ensure their future protection.

It has since been unveiled that the incident can be traced to an unauthorised third party accessing their computer system in the UK via a single and isolated user account. Through this they were able to copy data and demand a ransom for its safe return.

Clarksons were quick to respond to the incident, launching an immediate investigation into the event, notifying regulators and cooperating with investigators and law enforcement. They were fortunate to be able to trace and recover the copy of the data copied from its systems and have been working to determine what data may have been involved.

"While the potentially affected personal information varies by individual," says Clarksons, "this data may include a date of birth, contact information, criminal conviction information, ethnicity, medical information, religion, login information, signature, tax information, insurance information, informal reference, national insurance number, passport information, social security number, visa/travel information, CV / resume, driver's license/vehicle identification information, seafarer information, bank account information, payment card information, financial information, address information and/or information concerning minors."

From boardroom to boat, management to crew, security protocols are integral to ensuring that this type of crime is prevented. Any crack or crevice left exposed is enough for a cybercriminal to take advantage and cause untold damage. http://bit.ly/2MZQptC

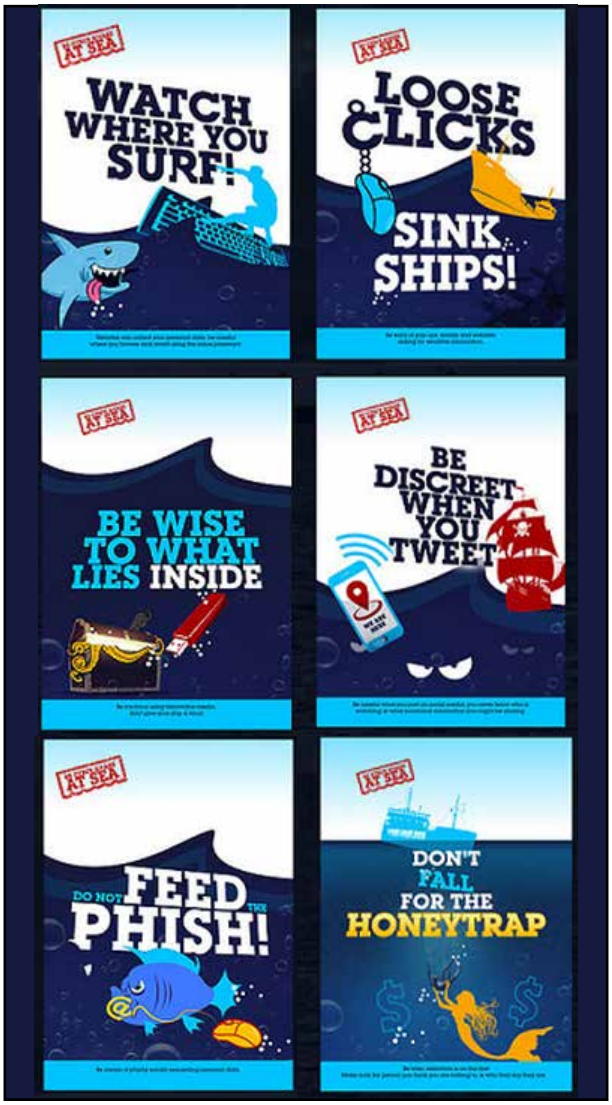
JOINED UP CYBER THINKING

Global cyber security and risk mitigation expert, NCC Group and Moran Shipping Agencies, Inc. have announced a new strategic alliance in maritime cyber security.

According to a press release, the alliance introduces a "holistic approach to maritime cyber security that combines both organisations' expertise to produce operationally relevant and realistic assessments and solutions that are sensible and uniquely tailored to the maritime industry".

There is a strong focus on Operational Technology (OT) with this new offering, and this deemed to be critical to understanding the complex systems and relationships of the maritime industry.

Moran is the largest independent steamship agency in North America with over 80 years of service to ship owners, charterers, and marine terminals. Moran has pioneered IT and security integration with quality standards in shipping and trade for over twenty years.



GRAB POSTERS FOR CYBER AWARENESS

One of the key pillars of the Be Cyber Aware at Sea campaign is our use of posters, and the fact that we provide them free to the industry.

The full series can be accessed and downloaded from our site for free, and we would urge all shipping companies to do so. All too often we hear of seafarers failing to get to grips with the firewalls, encryption, antivirus software and means of heading off cyber attacks.

Seafarers need to not just be aware of what they are fighting, but of the things which can help them. So, we hope the poster acts as a timely and useful reminder.

It is not just shipping companies, if you are a seafarer welfare or training centre, why not grab yours and make sure you are doing your bit to raise cyber security awareness at sea.

You can access high resolution versions of all our posters and resources at https://www.becyberawareatsea.com

Stay safe and cyber secure out there!

GOOD PREPARATION IS KEY TO CYBER RESPONSE

A year has passed since Maersk rang the cyber-sounding bell that caught the attention of the maritime and offshore industries. In the intervening time we have had yet more incidents to reflect upon, most recently that of Chinese shipping giant, COSCO.

Whereas Maersk's attack took several weeks to resolve and cost the company $300 million, COSCO was able to announce that they were back in business within days of the attack. Since the attack it has become clear that the preparations and reactions of the organisation to their cyberattack have paid dividends to lessening the impact of the incident. To the outsider, it appears that they were certainly paying attention to the warnings and advice that have flooded the industry since last August.

When it first realised it was being attacked, COSCO leapt into action, locating the origins of the attack so they could physically isolate it. They then took actions to contain the spread, for example cutting communications to other regions while maintaining operational ability. It is testament to their organisation and damage-limitation that even though the attack hit the Americas, the US, Canada and South American cargo handling at marine terminals was left largely unaffected.

Within four days, COSCO had the situation back under control and were able to report a full recovery from the cyber attack: no mean feat. According to Martyn Wingrove of Marine Electronics & Communications , this was "a good example of a quick recovery", and credit must fall on COSCO for their procedures and adherence to protocols. From the speedy isolation of the malware and reduction of communications to prevent spread of the virus to other branches of the company, both geographically and operationally, Cosco behaved smartly.

There appear to have been preparations for such an attack, as concluded by Susan Kohn Ross, a Los Angeles attorney who specialises in cyber security, in discussion to Bill Mongelluzzo of IHS Markit : "There is reason to think that Cosco was aware of what happened to Maersk and they took steps to minimize their risk. They didn't have everything on one server."

To those looking in, actions such as distribution of a detailed Q&A document which outlined specific instructions such as submitting cargo booking requests, confirmations and amendments, shipping procedures and cargo tracking among others, showed preparedness for just such an incident.

Given the closely interlocking nature of transportation logistics, from vessel to vessel, land to sea and company to company, it is clear that the industry requires a comprehensive plan of action. As Susan Ross summarised "There has to be a more sophisticated approach". Yet, while we wait for a global action plan to arise, we need more responsible companies like COSCO.

MARITIME INFORMATION WARFARE

26TH NOVEMBER TO 27TH NOVEMBER 2018,
LONDON, UNITED KINGDOM

SMi
LINKING BUSINESS *with* INFORMATION

After the success of last year, SMi Group is proud to announce the return of Maritime information Warfare to London, UK on 26th and 27th November 2018. The two-day event will focus on information systems, machine learning, new methods of data analysis, the growing need for automation in naval assets, and strategies for naval cyber warfare and defence.

2018 Event Highlights:

- The concept of 'information warfare' in the maritime domain and the need to embrace information to enhance naval operational effectiveness.
- Comprehensive technical briefings from the Royal Navy and other leading maritime experts on Artificial Intelligence, big data analysis, open source intelligence gathering and C4i combat information systems.
- Detailed focus on naval cyber warfare and how major European naval forces are approaching cyber defence of maritime assets and networks.
- Meet cutting-edge technology providers at the forefront of delivering artificial intelligence, information technology, and cyber defence solutions.

This year's event will explore crucial topics in maritime information warfare and how harnessing the power of Artificial Intelligence, defending networks against complex cyber threats, and developing combat information systems to enhance command and control are all vital to increasing information superiority and gaining an operational advantage. Therefore, navies are recognising the need to prioritise 'Information Warfare' in order to maintain strength in the maritime sphere.

Attendees can expect to hear from many top-level speakers including:

- Rear Admiral (Ret'd) Anthony Rix, Former Flag Officer Sea Training, Royal Navy [CHAIRMAN]
- Vice Admiral Timothy White, Commander of 10th Fleet Cyber Command, US Navy (SFC)
- Vice Admiral Hervé Bléjean, Deputy Commander, NATO MARCOM
- Commodore Ian Annett, Assistant Chief of Staff Information Warfare and Chief Information Officer, Royal Navy

For more information visit the event website at www.maritimeinfowarfare.com/phish&ships

For those interested in attending, there is a £200 early bird discount which expires on 28th September 2018.

1110101 1 HACKED 1111011

UNTOLD STORY OF NOT-PETYA

"Crippled ports. Paralyzed corporation. Frozen government agencies. How a single piece of code crashed the world." So goes the tagline of a new piece covering the full story of the NotPetya attack that brought chaos to Maersk last year, written by Andy Greenberg and available in the September issue of Wired Magazine.

This thorough piece of journalism focuses on uncovering the human side of the incident, as much as explaining the physics of the attack and its reverberating repercussions. Andy spoke to employees of Maersk and beyond, enabling him to paint a vivid picture of the panic on the day when their computer screens went blank, the next few weeks as they fought to take back control of the situation, and months as they established themselves going forward.

It is easy to report that Maersk suffered a cyber attack without understanding what that experience would be to the hundreds or thousands of employees and clients who were also affected, and articles like this really help create the full and personal picture with which we can identify. Not least, from Norway, to Ukraine, to England and beyond, this article makes clear the true scope of our maritime key players and the global nature of incidents on this scale.

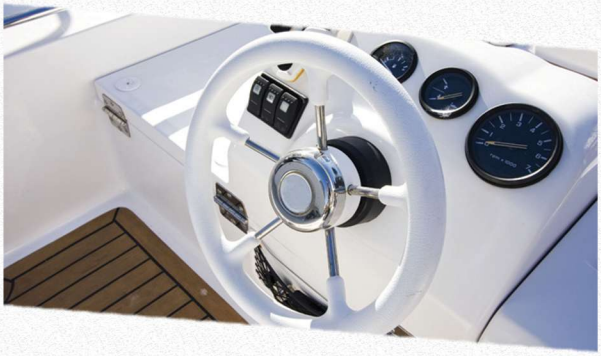
Andy Greenberg's piece also dwells on the scale of Not Petya beyond the maritime industry, although Maersk remains its focal point. He contextualises the attack against the backdrop of technological developments and political intrigue that enabled the malware.

This article provides a fascinating fresh look at the Maersk incident and is a great read for anyone who wants to understand what happened and how it was resolved through a human experience.

You can find the article in the September issue of Wired magazine, or online here: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Superyacht Cyber Security – A Must-Have Solution

With the increase of digital technology and resources at sea it is now even easier for yacht crews, owners and guests to stay connected to our digital world.



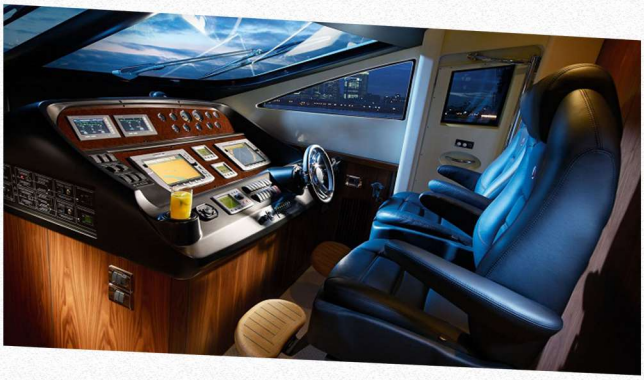
However, with the high profile nature of superyachts and their guests, it's no surprise that they are often targeted online more than many may expect. Superyachts have many things, but an anti-cybercriminal cloaking device isn't one of them!

A different kind of fishing

Hackers and those behind E-crime are constantly evolving. Every day networks around the world are thrown into complete chaos because someone clicked an unknown link, opened an unverified attachment or visited a compromised website, resulting in the system becoming infected, leading to loss of service, or worse still, data. The situation is no different for those living and working aboard a superyacht at sea.

Jordan Wylie of "Be Cyber Aware At Sea" comments that "Hackers don't care what it is they are attacking, In fact in most cases there unaware of their target, it could be an office a mobile phone, a superyacht or even a fridge! They attack without any thought as to the effects they may have on livelihoods, liabilities and in some cases peoples lives."

With ever-increasing budgets and awe-inspiring possibilities of superyacht design projects, more focus is placed on the yacht's performance, aesthetics, cinema systems and exterior speakers than its IT security system…..It is time to change.



Taking superyacht security seriously

Jordan suggests that the use of unsecured Wi-Fi networks, USB and endpoint devices when on board with the increase in hacking skills and complexity of Root Kits, phishing emails and malware should be taken into account when considering a complete security solution.

CONTACT US

Watchoak Business Centre, 5 Chain Lane, Battle, TN33 0GB

0330 043 1723

contact@turremgroup.com

www.turremgroup.com

COMING SOON: www.tdgcybermarine.com

CYBER ESSENTIALS

Information Security Management System ISO 27001 Certified

BE CYBER AWARE AT SEA

Onboard security for superyachts must be taken seriously if a yacht is hacked consider how this may affect the charter income and usability of the vessel. Who would want to charter a vessel that has been hacked knowing that there own private information, enterprise data, photos and mobile data could be next on the front page of the paparazzi's favourite magazine.

We already see a huge cyber risk increase within this sector, and it is now paramount for superyacht managers to consider mitigating such risks.

Jordan Wylie now recommends that all ocean-going vessels need to be aware of the risk of cyber incidents and that utilising maritime cyber specialists such as TDG Marine is a vital part of mitigating such risk.

No magic bullet solves such risks but as Jordan explained "Having a robust cyber-incident plan is paramount especially in the superyacht industry, understanding what the risks are is the first step. TDG Marine have proven time and time again that they can provide such capabilities with the monitoring and detection services to protect such vessels moving forward."

SOLUTION	BENEFITS	FEATURES
Managed Attack Prevention	• Fully Managed Solution • Reduct Operating Costs • Protect Your Assets • A Flexible Security Solution	• Enterprise Class Solution • Advanced Proactive Technology • Software Firewall • Comprehensive Reporting
Managed Exploit Protection	• Real-time view of risk • Automated assessment • Find the issues that matter • Prioritisation of exploitable issues • Vessel training & security status	• Enterprise Class Solution • Human Analysis • Comprehensive Reporting • Captains Dashboard*
Managed Risk Mitigation	• React to zero-day vulnerabilities • Leverages SOC* capabilities • Scalable patching service • Release schedule for each vessel	• Enterprise Class Solution • Hands on Assistance • Comprehensive Reporting
Consultancy & Security Audits	• Specific Maritime Knowledge • Onboard Cyber Audit • Worldwide Coverage • Tailored to clients needs	• Guest Sweep prior to arrival • Data sanitisation policy • Comprehensive Captains Report
Optional Add-Ons	• Latest Drone Technology • Physical Security	• Drone Detection • Special Forces Personal

All solutions are fully managed by our security team.

*Security Operations Center *Due for release Q4 2018