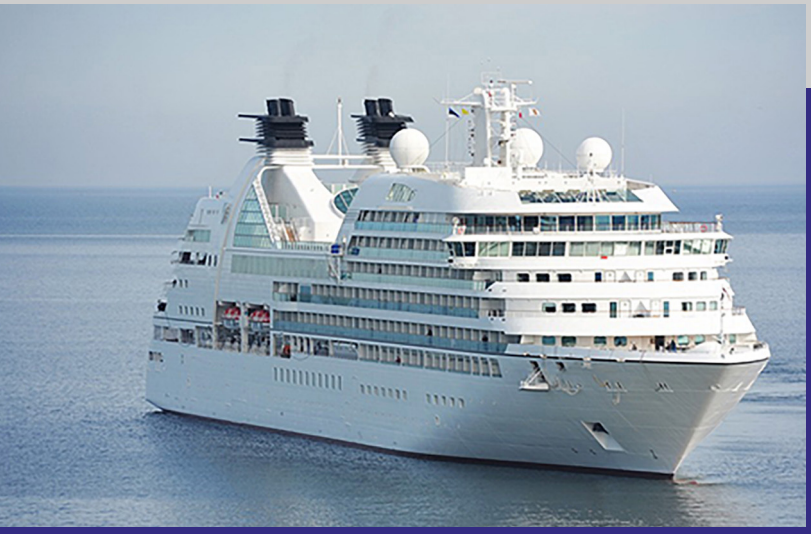
BIGGER AND BETTER FOR 2018!

#15

FEB:2018

PHISH & SHIPS

BE CYBER AWARE AT SEA



Kindly sponsored by

CSO ALLIANCE MARITIME

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 maritime and offshore industry initiative, "Be Cyber Aware At Sea".

Inside issue 15, we welcome back a number of friends of our campaign - with Epsco-Ra and Axis providing expert commentary. Their wise words on learning from other industries and of the power of segmenting networks could make all the difference to your cyber efforts. We have a host of other articles on a wide range of cyber topics, and we hope you find them useful.

We are also immensely proud to have been announced as winners at the SMART4SEA awards held in Athens. Be Cyber Aware At Sea won the 2018 Training Award, voted for by people across the shipping industry. We are so grateful to everyone who voted - thank you! You can see how much receiving the award meant to Campaign Director Jordan Wylie. Your support means the campaign goes from strength to strength, so we can we can make even more people at sea, and within shipping companies, cyber aware.

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

MARITIME CYBER SECURITY: WHAT CAN WE LEARN FROM OTHER INDUSTRIES?

As someone who has been involved in information security, now "cyber security", for over twenty years I've had the opportunity to observe multiple industries as they adopted and in some cases been transformed by information technology. I've worked with infrastructure, banking, insurance, healthcare and others as Internet centric technologies transformed them. Although each industry is unique, uptake of information technology generally results in at least some unanticipated consequences, not the least of which is risk, where little or none may have existed before. Unfortunately for many of the early adopters the intersection of a new risk, a vulnerability and a credible threat come together with devastating effect, prior to the risk even being initially identified. But that was then, this is now… right?

In an ideal world we would immediately learn from the mistakes of others and move forward with that knowledge intact and in hand. In the real world it seems like history just repeats itself in an endless cycle of carefully documented, clearly avoidable yet predictably made mistakes. In the Maritime industry I see some familiar patterns of an industry in the midst of a transformation at the centre of which is the proliferation of Internet connectivity and connected devices aboard vessels. If there are advantages there are going to be disadvantages also requiring consideration. On the one hand are the purveyors of products and services designed to increase the operational efficiency of vessels, fleets and the maritime industry in general demonstrating skyrocketing capabilities. The benefits are certainly seductive. On the other hand are the purveyors of infrastructure, information technology and cyber security saying hold on guys this comes with risks we have to consider. The risks are certainly demonstrable.

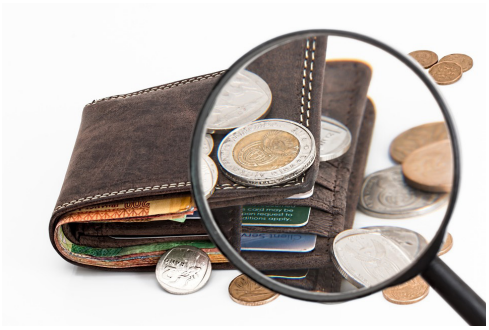
So how much risk comes along with this adoption and transformation, how do we manage it and the big question… who pays to mitigate it? These are not new questions as every other industry has gone through adoption either as a class of industries or individually. One of the reasons this is even a question for Maritime is because Ship Owners and Ship Managers, the decision makers, receive wildly differing opinions on how serious the risk is and how immediate the threat is from their influencers (staff, vendors and industry experts). Vendors and the experts working for them tend to overstate the risk and for obvious reasons. They're trying to sell you a solution so the problem has to be immediate and severe enough to prompt you to act upon it. In addition, experts never want to be put in a position of being asked "why didn't you warn me this could happen" after an incident occurs. Internal staff on the other hand often understate the risk because mitigating it means adding more work to their already full schedule and besides… nothing bad has happened yet. Or maybe it has but it was swept under the carpet as an anomaly.

So remember that part about learning from other's mistakes? Here is what Maritime can do that other industries haven't successfully done early in the Internet adoption process; share incident data. I'm not talking about vague anecdotes whispered around at conferences, I'm talking about detailed incident reports. Without a reasonable idea of what incidents are actually occurring and their frequency, how can we as an industry make good decisions about mitigating risk? Without details of an actual breach, how can we react and make the right choices? We are left to speculate on what could happen rather than extrapolate on things which have actually occurred. If maritime can become comfortable sharing incident data, even anonymously, the industry as a whole would benefit greatly and the ROI on cyber security would be easier to quantify and budget for.

About the author: Mr. Gideon Lenkey, Director of Technology at Epsco-Ra. As President of Ra Security Systems he has consulted on information security matters since 1989. He specialises in assessing and testing the security posture of enterprise IT infrastructures and managing enterprise cyber security initiatives. He has provided advanced training to the FBI and has been consulted by both foreign and domestic government agencies. Mr. Lenkey is a past president of the FBI's InfraGard program in New Jersey and has been recognized by FBI Director Robert Muller on multiple occasions for his accomplishments. He regularly lectures, writes and grants interviews on cyber security topics. In 2011 Mr. Lenkey coauthored "Gray Hat Hacking" third edition for McGraw Hill and is featured in the film documentary "Code 2600".

EPSCO - RA
Maritime Cyber Security Solutions

CHECK CHECK AND CHECK AGAIN...RISE IN PAYMENT FRAUDS



Security researchers have found that freight messaging systems can be subverted to send money to criminals via an electronic messaging system used to send payment for cargo.

According to security researchers at Pen Test Partners, the IFTFCC (International Forwarding and Transport message – Freight Costs and other Charges) could be subverted by hackers to steal money.

An IFTFCC has specific formats that are very interesting to those trying to steal money. A message typically sent from a shipping company to the receiver (or at least whoever is paying for the shipment) allows for various compulsory and optional fields. Most of the message covers information about currencies, values, tax etc.

Researchers said there should be a cross-check that limits the ability to carry out fraud. Hopefully, the shipping company and consignee will ensure that the details match the Bill of Lading. Especially as there have been many occasions where security breaches have happened as a result of assumptions made by various parties about security.

Often, users make assumptions about security with no knowledge of message transport security, authentication and integrity processes. "Irrespective, any user of EDI messaging for anything financial, maritime or not, would do well to check that their systems are secured from message manipulation and related invoice fraud," said Munro.

So be sure to check and check again - otherwise, the money could be landing in the hands of fraudsters and criminals.

UPCOMING EVENTS

Digital Ship – Maritime Cyber Resilience Forum
15 February 2018 Rotterdam, The Netherlands
https://www.rotterdam.thedigitalship.com/

Digital Ship – iShipping Conference
27 February 2018
Copenhagen, Denmark
https://www.copenhagen.thedigitalship.com/

Lloyd's Maritime - Cyber Security Seminar
18 -19 April 2018, London
https://goo.gl/SnK2U1

MARITIME CYBER ALLIANCE: SHAKE DOWN FOR FEEDBACK

CSO ALLIANCE MARITIME

The support from all the ship owners and ports we have met to date has been inspirational. As we listen we are learning and it is clear shipping is under significant hostile probing from cyber criminals.

We now have several impact reports. We anonomise key identifying criteria, but importantly we can share the tactics. The carefully planned and executed fraud attempts range from ship broker commission payments (PDF's payment details altered), Superyacht bunker stem payments, Port Agency Disbursement account frauds, a Port suffering a long term and carefully planned social engineering fraud and a breach at a P&I Club. These are all in the process of being loaded on the platform.

It is clear that once the criminals discover a tactic they then work hard to try it out in several maritime locations, as our members learned by phoning round similar companies in the same city. In our industry, with 100,000 ships of 100 GT and above making 1,600,000 million port calls per annum, there is plenty of opportunity. As we evolve we can see that we can identify and share the criminal email addresses used and start to identify the originators. As we shake down something of a manual process, we can see our philosophy of "Security through Community" begin to deliver.

With Airbus we will be running cyber workshops throughout the UK. We will be inviting Ports and Ship Owners to the same cyber workshops in Southampton (5 Feb), Aberdeen (12 Feb) and Glasgow (14 Feb). We will also run further workshops in Liverpool and Belgium later in February and early March.

The aim of the workshops is not only to help companies in the maritime supply chain understand the cyber threats, government and EU regulation, but also to share ideas on how to cyber (self) audit and what tools and services may be required. All workshop attendees leave with an aide memoire to share with their management.

We will share the learning on https://www.maritimecyberalliance.com and in upcoming issues of Phish & Ships.

NEW US CYBER FRAMEWORK

The US Coast Guard Office of Port and Facility Compliance recently announced the release of new cybersecurity framework profiles for the Offshore Operations and Passenger Vessel industries, providing a pathway for these industries to implement the National Institute of Standards and Technology (NIST) Cybersecurity Framework.

As informed, the NIST Cybersecurity Framework was developed in 2014 to address cybersecurity risk in a cost-effective way, based on business needs and without placing additional regulatory requirements on businesses.

These profiles reflect how organisations align the NIST framework's cyber security activities, outcomes, and informative references to organisational business requirements, risk tolerances, and resources. They outline a desired minimum state of cybersecurity and cyber risk management, and provide the opportunity to plan for future business decisions.

These two new profiles follow the November 2016 release of the Maritime Bulk Liquid Transfer cybersecurity framework profile, a voluntary cyber risk assessment tool developed in conjunction with the NIST as well as industry stakeholders. The series of industry profiles are the first of their kind for the marine transportation system sector, and they are the result of the coordination between the USCG Office of Port and Facility Compliance, the NIST's National Cybersecurity Center of Excellence (NCCoE), key industry stakeholders, and trade associations.

One of the primary focuses of the Coast Guard and NCCoE during the development of these profiles was to ensure they were industry-focused and leveraged existing standards and recommended practices.

"The cybersecurity framework profiles are designed to assist organisations in assessing cyber risks, and offer guidance on how to allocate limited resources in order to improve their cyber resiliency. The Coast Guard hopes these profiles will assist organisations in answering these questions and help with mitigating concerns," said Lt. Cmdr. Brandon Link, a marine safety expert in the Critical Infrastructure Branch within the Coast Guard's Office of Port and Facility Compliance.

The Coast Guard anticipates working with the NCCoE on at least one additional profile addressing navigation and automated systems onboard vessels as well as facilities.

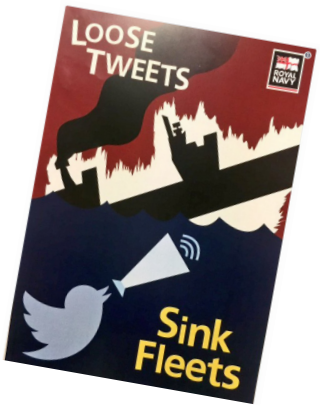
RN WARNS ON LOOSE TWEETS

The Royal Navy has revamped one of the most famous Second World War propaganda slogans to warn its sailors to be careful what they tweet.

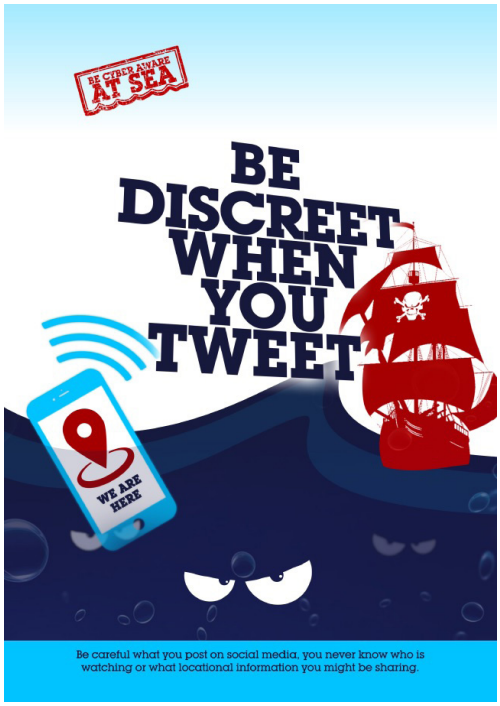
It issued an updated version of the 1943 "loose lips sink ships" poster, tweaked to refer to social media instead, and featuring the new HMS Queen Elizabeth aircraft carrier going down in flames.

There is real concern that sensitive information could inadvertently be posted in public by somebody on board who did not realise the significance of what they were sharing.

The message from the official account of HMS Queen Elizabeth, along with a reminder that "OPSEC [operational security] isn't a dirty word!" is an homage to a well-known 1943 propaganda poster distributed by the United States Office of War Information.



The Royal Navy were one of the Be Cyber Aware at Sea campaign's earliest supporters - and backed our poster campaign. You can download free poster resources like the one here at https://www.becybera-wareatsea.com/awareness



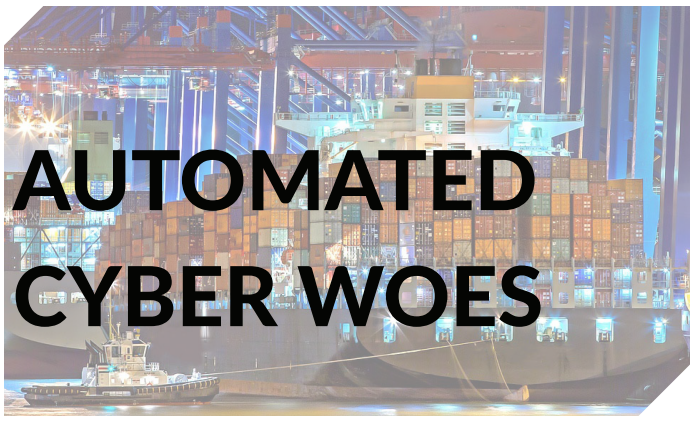
CYBER IN WORLD RISK REPORT

Each year the World Economic Forum's "Global Risks Report", works with experts and decision-makers across the world to identify and analyse the most pressing risks that we face. As the pace of change accelerates, and as risk interconnections deepen, this year's report highlights the growing strain we are placing on many of the global systems we rely on.

In this year's Global Risks Report cyber-crime now joins environmental disasters, largescale involuntary migration and illicit trade as one of the most notable risks in the world.

Almost 1,000 global experts are surveyed on their views in order to create the list and they rank cyber-attacks as the third most likely event to happen globally in 2018, only sitting behind extreme weather events and natural disasters.

With this fair warning companies should pay attention and secure their systems so they do not fall victim to attacks. You can access the report here: https://www.weforum.org/reports/the-global-risks-report-2018



AUTOMATED CYBER WOES

To stay ahead of competing ports and technological developments, automation has been heralded as inevitable. Major transshipment hubs and aspiring ports bet their future on automation, which raises the impact cyber risks could have in the long-run.

While full automation gives large ports the advantage of reliable, full-time operations at low operating costs, full automation also increases the vulnerability to cyber risks. This is due to the use of technologically advanced and networked systems.

These terminals use industrial control systems that translate sensorial data and commands into mechanical actions. The network links between mechanical equipment and sensors are exposed to the same threats as data networks. The complexity is further increased by the months and years it can take to figure out and fix bugs and weaknesses in automated systems. In an automated system, different system components have to effectively work together as one, stretching the time needed to figure out and fix bugs. This involves mainly software issues that have to be fixed while also moving boxes of cargo at the terminal.

According to a new report from CIMSEC (Center for International Maritime Security), cyber risks require adequate awareness and planning to strengthen a port's resilience. Training employees is vital and ports need to engage in contingency and scenario planning to be better prepared should an attack occur.

TIME TO TALK CYBER IN THE BOARDROOM

When insurance giants such as Allianz report that cybersecurity is the second most important business risk, it is time to sit up and listen.

According to a new "Risk Barometer" report, the number and complexity of cyber attacks is growing. Which is to be expected, as it mirrors technology's increasing impact and complexity: the bad things are dark mirrors of the good.

New threats such as "cyber hurricanes", increasing reputational risk and tougher data rules mean businesses and risk experts are more concerned than ever. "Every company has been or will be impacted by cyber risk. It is not over-hyped. If anything it is under-appreciated because the threats are not always well understood," says Emy Donavan, Global Head of Cyber at AGCS, noting that over 50% of Risk Barometer responses rank cyber as the risk most underestimated by businesses.

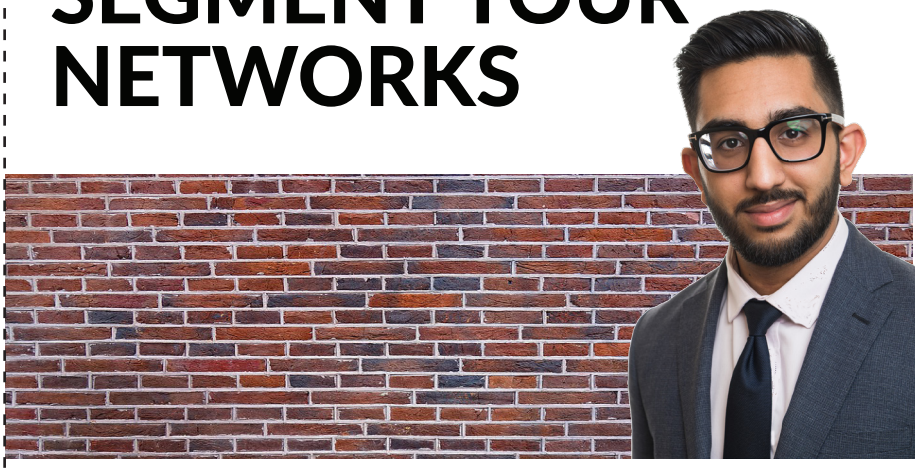
The report states that companies can't bury their heads in the sand. The sooner they respond the better the outcome. Companies that respond poorly to a cyber incident will see more of a long-term impact on their stock price than those that respond well.

So what is the number one business risk? Well that is business interruption (BI). "Whether it results from factory fires, destroyed shipping containers, or, increasingly, cyber incidents, BI can have a tremendous effect on a company's revenues."

In other words, while cyber incidents pose a significant challenge by themselves, their consequences can be even greater— it's difficult to escape the conclusion that cybersecurity should be a boardroom topic right now.

You can read more of the 2018 Risk Barometer here: http://www.agcs.allianz.com/assets/PDFs/Reports/Allianz_Risk_Barometer_2018_EN.pdf

WHY YOU SHOULD SEGMENT YOUR NETWORKS



Akash Bharadia, Technology Specialist – Cyber & Tech E&O at Axis shares his thoughts on the importance of segmenting your network:

Network segmentation is defined as splitting a computer network into subnetworks or 'segments' with the aim of boosting performance and improving security.

Whilst resource-heavy to implement, the benefits of network segmentation far outweigh the work it takes to put it into effect. There are many benefits to implementing network segmentation. One of those benefits is that it keeps any malicious software isolated to whichever network segment it has manifested itself into.

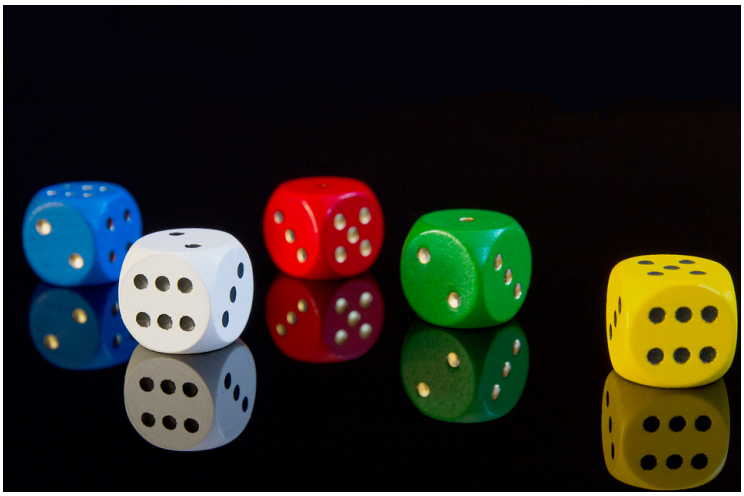
Let's say a shutdown virus has found its way onto the network of a vessel. The virus is going to propagate itself throughout the accessible network until it has run shutdown scripts on every machine it finds. This isn't too much of a problem if the network has been segmented and the virus is only running on, say, the crew welfare network. However, it becomes a much bigger issue if the network has not been segmented and the virus finds its way onto the cargo management system.

You may think, "No big deal, we can just power that system back on right?". That isn't the case if the virus keeps re-executing on boot up. This is going to involve re-imaging the whole system, with considerable downtime and possible loss of cargo logistic data while you restore the system to the last backup taken before the virus was discovered. Depending on backup cadence this could end up leading to multiple days' worth of misplaced cargo.

In addition to the downtime you are going to have whilst the system is rebuilt, you will have to deal with the misplaced cargo and any costs therein. It is, therefore, much less of a headache to ensure networks are properly segmented at the outset!

See www.axiscapital.com to learn more about the role of insurance in cyber security.

DON'T TAKE A CHANCE ON CYBER COVER



According to JLT Specialty, 2017 will perhaps be remembered for, among other things, being the year that awareness of cyber incidents in the shipping and maritime industry started barrelling forward at full pelt. Indeed, the pace of awareness and change, is picking up.

Companies across the sector, both large and small, need to work feverishly to get ahead of the cyber threats facing them. Currently the problems are likely to outpace the development of technology to combat them, so awareness and vigilance are vital.

Investment in cyber security clearly will have to be escalated and accelerated, and existing insurance policies and protections reviewed and scrutinised. Maritime firms are also warned that just because an insurance policy has 'cyber' in its name does not mean that it will fill all of the gaps in a standard insurance portfolio.

Cyber policies generally exclude physical damage to ships and cargo stemming from cyber incidents, so there is a real need to take a closer look at each organisation's existing insurance policies and work collaboratively across lines of business to meet a company's needs. Simply purchasing an 'off the shelf' cyber policy or negotiating to delete exclusions within non-cyber policies is unlikely to give risk managers the seamless coverage they desire.

In response, the insurance industry itself is evolving to meet these changing needs, with solutions and programmes via P&I Clubs now starting to emerge. As well as innovation in terms of products and solutions, it is essential that a much greater degree of collaboration across different areas of risk management becomes the norm and not the exception.

Marine specialists and cyber underwriters must put their heads together to ensure all areas of exposure have been addressed, and that maritime industry players have the best chance possible of avoiding or minimising the impact of costly – and potentially dangerous – cyber-related incidents.

WHALING SCAM: BANK NOT LIABLE

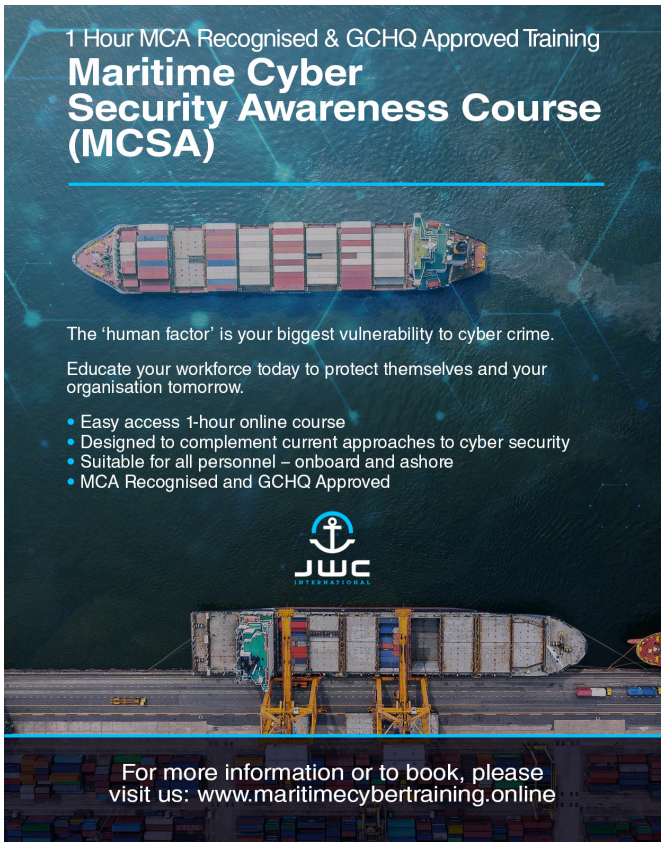
A shipping company has failed in an attempt to recover $1.8m from its bank after it was paid fraudulently to an unknown third party.

The fraudsters had accessed the client's email account in an apparent "whaling" scam. This is a type of phishing email scam that targets high level executives such as CEOs, who have access to valuable information.

Four payments totalling $1.84m, were made by the bank following the receipt of email instructions, and the shipping company is now appealing the case.

It is alleged, the bank received six outward telegraphic transaction instructions from the owner of the company via email in the form of remittance application forms. The judge dismissed the claim finding that the bank was not negligent and therefore not liable for the claim. The judgment highlights issues with small to medium enterprises (SMEs) in terms of authorisation of payments and the use of webmail accounts.

Such cases reaffirm that vigilance concerning cyber-security should be present from top to bottom in all companies.



Lloyd's Maritime Academy presents Cyber Security Seminar – a two day training course on 18 -19 April 2018, in London designed to help the maritime industry understand the risks & threats, address weaknesses and implement fail-safe solutions against cyber security challenges: https://goo.gl/YgjZuH

Be Cyber Aware At Sea "Phish & Ships" readers save 20% using VIP code FKT3459BC or follow this link: https://goo.gl/YgjZuH

WHAT WILL YOU LEARN:

- Regulation updates - hear about the latest regulations from IMO and foreign policy on cyber security threats
- Risk management - learn about previous attacks and carry out risk management analysis to develop an effective mitigation policy
- Scenario planning - understand the threat, plan the strategy and implement an effective plan to combat an attack
- What does a cyber attack look like - identify tell-tale signs that signify a potential attack and weakness opportunities for criminals
- Legal and insurance implications - policy consequences, measuring liability and determining key parties involved
- Innovative technology solutions - understand the latest technologies and how they are tackling cyber security challenges

View full agenda: https://goo.gl/SnK2U1

WHY ATTEND:

- This is the only dedicated training course on cyber security for the maritime industry
- The whole supply chain will be present, giving you a chance to explore the threats from every angle
- Experts from the wider cyber world will be sharing their experience and relaying what this means for the maritime industry

Download full event agenda to explore what you will learn about and to view the latest speaker line-up: https://goo.gl/SnK2U1

Don't forget to use VIP code FKT3459BC or follow this link: https://goo.gl/YgjZuH to SAVE 20%

If you have any questions about the event, contact maritime@knect365.com or +44 (0) 20 7017 5511.

WEAPONS OF HACKING CHOICE

Despite the sudden spurt in malware and ransomware attacks across the globe, non-malware attacks were the weapons of choice for cyber criminals in 2017, researchers have revealed.

52% of all cyber attacks in 2017 were non-malware attacks despite ransomware attacks growing from being a £630 million industry in 2016 to a £3.7 billion one in 2017.

Researchers at the Carbon Black Threat Analysis Unit have revealed how ransomware attacks, along with malware and non-malware attacks, have created a 'vast attack surface' for hackers who are more creative and persistent than ever before.

The most common ransomware variants in use last year were Spora, CryptXXX/Exxroute, Locky, Cerber, and Genasom.

At the same time, hackers utilised destructive malware families like Kryptik, Strictor, Nemucod, Emotet, and Skeeyah last year to target financial organisations, healthcare providers and retail stores with great success.

Non-malware attacks are those in which an attacker uses existing software, allowed applications and authorised protocols. They can effectively gain access or take control of vulnerable enterprise software without having to inject malicious files which can be detected by anti-malware solutions.

TOP 6 CYBER THREATS FOR 2018

1. Huge data breaches
2. Ransomware in the cloud
3. The weaponisation of AI
4. Cyber-physical attacks
5. Mining cryptocurrencies
6. Hacking elections (again!)

source: Technologyreview.com

www.becyberawareatsea.com

think@becyberawareatsea.com

With thanks to our many industry supporters....