#10

SEP:2017

PHISH & SHIPS

BE CYBER AWARE
AT SEA

Kindly sponsored by

CSO ALLIANCE
MARITIME

WELCOME

BE CYBER AWARE AT SEA

Welcome to issue 10 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".

Given that we are working in the cyber and digital domain, the fact that we have reached issue 10 of Phish & Ships is a real landmark. It's a binary thing.

Anyway, in this issue we are pleased to have packed in as much information as possible. We look back on the pain and costs associated with cyber losses. We also explore the old technologies which could re-emerge as vessels seek to protect themselves against GPS weaknesses.

In addition, inside we explore the development of best practices when it comes to cyber security, and the ways in which the shipping industry needs to be more resilient in the face of the risks facing it.

Once more, our good friends at Novae Group have provided us with another incredibly thought provoking piece, where they urge shipping companies not to wait for patches, but to act proactively.

We also look at the basic steps to deal with cyber risks and threats, and explore the panic that can spread when these impact safety of navigation. Are we seeing an age of cyber assisted collisions?

There is also a look at the mitigation strategies that are used in other industries, and the models that could be transposed effectively onto the maritime domain.

We hope this latest issue of Phish & Ships provides further insight into the issues, and helps you and your staff to become cyber aware. Share this newsletter, talk about the issues and stay safe.

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

MAJOR LOSSES

Soren Skou, the CEO of AP Moller – Maersk, has, for the first time approximated the hit in revenues they suffered in the wake of Not Petya at $300m.

"In the last week of the quarter we were hit by a cyber-attack, which mainly impacted Maersk Line, APM Terminals and DAMCO. Business volumes were negatively affected for a couple of weeks in July and as a consequence, our Q3 results will be impacted. We expect the cyber-attack will impact results negatively by $200m to £300m," Skou said. However, the Danish company has not changed its full year results guidance.

Underlying profit for the group in Q2 improved from $134m to $389m with Maersk Line contributing with an underlying profit of $327m. However, as a result of post-tax impairments of $732m related to Maersk Tankers and APM Terminals, the reported result was a loss of $264m.

"Maersk Line is again profitable delivering in line with guidance, with revenue growing by $1bn year on year in the second quarter. The profit was $490m higher than the same quarter last year, based on higher rates," Skou commented.

The cyber-attack on Maersk marked the most high-profile online hit of a shipping firm to date.

CYBER RETHINK

The maritime industry appears to be specifically vulnerable to cyber attacks due to several factors including the fact that IT systems onboard were designed with the concept, 'the system must work under all conditions' instead of 'the system must work securely' mind set. That is according to Markus Schmitz, the managing director of Cyprus-based IT provider SOFTimpact, who recently gave an interview on the matter.

Other factors that make it tricky to secure shipping from hackers are the wide chain of people involved in day-to-day operations. Several parties – crew, managers, service personnel, pilots, auditors, inspectors, charterers – cooperate in operating the vessel.

Other issues to be aware of include the common use of voyage contracts which potentially affects employee loyalty and training investments. Moreover, the international character of shipping facilitates certain common cyber threats, like phishing attacks and fraud.

In order to overcome the challenges posed, the industry needs to go through a change of mindset to one where technology is used more consciously, and where technology purchasing decisions take cyber security into consideration. Schmitz questions whether, for example, it is really advisable to purchase an ECDIS system, which relies on USB sticks, in order to distribute updates?

DEVELOPING CYBER BEST PRACTICES

Commissioner William P Doyle of the US Federal Maritime Commission perhaps summed up the impact of the recent cyber attack on Maersk better than anyone. "If it can happen to them, it can happen to anyone", was his view, and he is right.

The response of the industry is still unsettled, flitting between evolving further technologically and being held back by issues such as financing, lack of understanding and general fear of hacking. There have been a number of key areas where the industry needs to redefine best practice, as identified in KNect365's recent blog:

TECHNOLOGICAL GROWTH

In the wake of the Maersk cyber-attack, some parts of the industry are questioning the benefits of progression and returning to or adapting older technology that is seen as 'hack-free'. However, as Gareth Williams, a Partner at Holman Fenwick Willan states: "Constant growth requires constant striving for better and more efficient ways to do things. Connectivity provides that and reliance on networks is not going to slam into reverse. This kind of event usually acts as a spur to do better on the security front."

Andre Simha, Global Chief Information Officer of MSC Mediterranean Shipping Company, didn't think that a single event could override the developments: if anything, it should encourage those who underinvested to try to expand more.

SAFETY PROCEDURES AND MANAGEMENT

Given that developments in technology are here to stay, the onus should be on improving safety procedures and management. Indeed Phil Tinsley, Manager of Maritime Security at BIMCO noted that "it is important that safety procedures are developed concurrently" with technological advancement.

Vigilance is key, as Williams points out: "You should be constantly reviewing and testing the capabilities of your cyber security technology, because the threat changes constantly, and so too must the response...The attack in Maersk is believed to have owed its devastating effect to the fact that a vulnerability for which a patch was available had not been put in place. So sometimes it is as much a matter of doing the simple things as the bigger higher level ones."

Be Cyber Aware At Sea's Jordan Wylie saw effective cyber risk management lying with good governance, supporting processes, and training along with the right technology. But first, shipowners need to assess the risks to their organisation and understand the threats before deciding to invest in technologies.

HUMAN ELEMENT AND TRAINING

In shipping, there is always a human element to consider, even with something so technical as cyber security. Crew training, therefore, is essential in implementing good cyber hygiene.

"We can have the best technical solutions, policies and procedures in the world but if people aren't trained properly and don't understand what the threat is, then all the above are not wise investments at all", Wylie warned.

"Training needs to cover prevention, detection and cure", Williams suggests. "Cyber risk awareness needs to be raised at all levels in the organisation:

- **drilling into people the risks of opening suspicious email attachments,**
- **teaching how to determine what is suspicious, and**
- **how to recognise when there might have been a security breach."**

In addition, he suggested discipline in backing up data and cyber drill to practice the regime to kick in during the event of an attack.

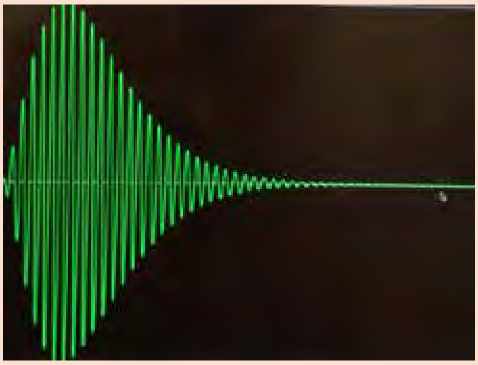
HANDLING A CYBER ATTACK

Finally, companies should be aware that global cyber attacks have far reaching impact upon operations, finances and even human health and safety. Customer service is also a key consideration.

For the industry, reforming what constitutes best practice will be an important part of protecting themselves from and reacting correctly to any cyber attack.

BACK TO THE FUTURE FOR NAVIGATION

Concerns about the impact of cyber attacks on satellite navigation are reportedly prompting a return to legacy systems, many of which date back to WWII radio technology. Experts say that modern GPS devices reliant upon satellite signals, are vulnerable to jamming by hackers, and ships lack back-up navigation systems.



One such answer is the earth-based navigation technology known as eLoran. The ELoran technology is being pushed as a means of protecting security despite it requiring significant investment. The network will need new transmitter stations to give signal coverage, or old facilities will need to be upgraded, which could prove expensive, as many of these date back decades to when radio navigation was standard. Many towers have actually been demolished over the past years, so there would have to be major investment.

US engineer and retired US airforce Colonel Brad Parkinson, known as the 'father of GPS' is among those supporting the development of eLoran, as it offers a powerful signal at an entirely different frequency."

Four Steps to Cyber Security

Tackling cyber threats from a standing start can be intimidating for many reasons. Security systems can seem daunting and confusing, while the costs can appear overwhelming and operation technology data heavy and vulnerable.

However, it is imperative that a robust cyber security system is built sooner rather than later. But where to start? Your first four steps could be:

1. **Assess your current cyber state**
2. **Review your policies and procedures**
3. **Create a data map of the network and how your data interacts**
4. **Review the systems to help identify priorities – are they outdated/unsupported and configured correctly?**

Cyber risk can sometimes be difficult to quantify or assess but it needn't be. Risk management is nothing new to the maritime industry and cyber is just another form of risk to be assessed and managed.

Once assessed, it is immeasurably easier to incorporate the recommendations into your business plan, particularly when you consider cyber risk as part and parcel of your annual budget.

Be aware that much of the technology in shipping is legacy based – older systems no longer supported by the software provider – or haven't had security built in on installation – these are inherently vulnerable.

In terms of expense, the best way to consider the costs is to prioritise the basics to cover your greatest needs, working outwards.

With the IMO's new guidelines, now is the time to take action and strategically plan your approach to becoming cyber secure.

MAJOR CYBER REPORTING BOOST

Airbus Defence and Space has partnered with our sponsor, CSO Alliance, a maritime community of company security officers (CSOs). The agreement covers the building of a tailor-made, secure online reporting platform to help counter maritime crime across the world.

The platform will be ready for launch in early October and will provide the CSOs and company information security officers (CISOs) with a worldwide, voluntary and anonymous incident reporting portal for assessing physical, as well as cyber, threat activities and the respective risk levels as the basis for appropriate decision-making and action-taking. October version is a Pilot that will be adapted based on user feedback.

Phish & Ship readers have been urged to think about the importance of reporting, and as part of this campaign, CSO Alliance has extended an invitation to come along to discuss the subject during London International Shipping Week 2017.

The CSO Alliance is hosting a joint event with BIMCO on Tuesday 12 September 9 am - 10.30, and it is really not to be missed.

Sign up via https://londoninternationalshippingweek.com/event/bimco-cso-alliance/

11-15 SEPTEMBER 2017
LONDON
INTERNATIONAL SHIPPING WEEK

FEAR OVER CYBER ASSISTED COLLISIONS

The tragic collision between a Liberian oil tanker and the USS John McCain is the fourth involving a vessel in the US Navy since January. This latest collision left death, casualties and confusion in its wake.

While not much is known about the incident, the coincidence of so many collisions in the Pacific area has generated speculation. Indeed, the question of a cyber attack on ship board navigation is one area of investigation at the US Navy's upcoming review. So experts have been left asking the very awkward question...could cyber hacks lead to collisions?

IN THEORY AND PRACTICE

In theory it would be possible for a cyber attack to be designed to confuse the crew on naval or merchant vessels, denying them access to critical systems in a moment of crisis or to lull them into dangers path. Researchers have delved into the range of software and hardware and found evidence of lax security practices, which could indeed see misleading information about a vessel's position and movements around it.

In recent months Phish & Ships featured an article about the US Maritime Administration safety alert regarding an incident in the Black Sea which saw an apparent "mass and blatant, GPS spoofing attack involving over 20 vessels". The vessels' GPS was displaying as 25 miles from their actual location although crew found no problem with the operation of the GPS devices.

Beyond spoofing, there is onboard software that is capable of being attacked. While security flaws in software including out-of-date applications and operating systems has been noticed even on new warships so vulnerabilities are abundant.

IMPROVE YOUR CYBER RESILIENCE – BEYOND THE PATCH

Novæ
LOOKING FORWARD

In our "Talking Cyber Sense"series, Sharif Gardner, Cyber Unit Training Manager at Novae Group looks at how to evolve your cyber resiliance, and move beyond just waiting for system

The world has seen a remarkable rise in the scale and seriousness of the impact a cyber-attack can have on a business. The shipping industry was one of many who bore the brunt of such an attack in June this year. 'NotPetya' infected thousands of businesses across the globe and resulted in hundreds of millions of dollars in damages. Many of those infected were still experiencing businesses interruption for weeks after the attack.

Most are aware of the need for patching in order to improve a computer's performance and fix security vulnerabilities. The importance of patching has been written on by many of the experts who contribute to Phish & Ships. But beyond the key mitigation strategies, what else can an organisation do to improve its cyber resilience?

HARDENING NETWORKS

By removing, disabling and separating networks, businesses can reduce the number of access points available to hackers and in turn limit their ability to infiltrate entire systems. Legacy protocols frequently serve as an entry point for hackers and should be disabled. This is arguably a critical control that would quickly halt the spread of malware such as 'NotPetya'.

EMAIL SECURITY

Businesses should configure their policies to scan and blacklist malicious inbound URLs, detect and prevent email spoofing and protect against suspicious attachments with email filtering. This will help protect users against phishing and spear phishing attacks.

DATA RECOVERY AND BUSINESS CONTINUITY

The 'Be Cyber Aware at Sea' is a preventative campaign, but what happens when an organisation is called into action? Preventative measures alone are not enough and the true test of an organisation's cyber resilience is its ability to bounce back – quickly.

Regularly backing up critical data and ensuring at least one copy is offline is vital to a business's ability to recover data rapidly. Malware, such as what was utilised in the 'Not Petya' attack, quickly encrypts large volumes of data. Having access to back-ups that began before the malware was introduced to the system will save businesses time and money. Additionally, having access to a specialist and dedicated incident response and business continuity service company who can provide strategic advice and expert assistance in the event of an attack has proven to be invaluable.

Cyber-attacks have emerged as one of the key risks of the 21st century. All businesses, big or small, should have a thorough risk management and incident response procedure in place and ensure that all staff have been trained on how to properly follow protocol.

https://www.novae.com/

FEAR OF CYBER RIPPLE EFFECT

Shipping is one of the most critical links in the global supply chain and a potential ripple effect of a cyber incident is what is most feared.

INTERCONNECTED INDUSTRIES

Like the technology itself, the shipping industry is becoming more and more closely interconnected, gaining efficiencies and creating more market opportunities along the way but also open to greater levels of disruption.

We are still finding more ways in which industries are connected, with more opportunities for interception and cyber crime. For example, researchers in Israel have identified that smartphone touchscreens and other hardware components such as orientation sensors and wireless charging controllers, are often produced by third party manufacturers, providing more attack vectors. They conclude that "attacks by malicious peripherals are feasible, scalable, and invisible to most detection techniques".

Shipping, as the ultimate in global supply chains, must be more aware of the possible attack vectors that pervade the industry and its many participating and interlocking parties and ensure they can trust in the provisions each sector has made for cyber threat.

BUT THERE IS HOPE

One mitigation strategy is for each link of the supply chain to develop its own holistic, risk-based cyber strategy. The alternative is for regulators to impose cybersecurity preparedness regulations; these would need to cross national boundaries or at least comply with corresponding bodies in other linked nations.

For example, even US organisations, as direct or third party/supply chain organisations, will need to comply with the incoming European General Data Protection Regulations when it enters into effect in May 2018. Finally, industry can impose its own industry standards with the threat of loss of business for organisations that do not comply as the Oil Companies International Marine Forum has just done with its updated Tanker Management and Self Assessment guide, that now includes cyber security.

Shipping is the largest set of dominos operating today in the commercial market, it could be your domino that succumbs to an attack, or the domino of a colleague or even a third party you don't work with directly, but when one falls, the rest – including you – could follow. Conversely, strengthen your position and you strengthen the entire body.

BE CYBER AWARE AT SEA

Sponsored by:

CSO ALLIANCE MARITIME

www.becyberawareatsea.com

think@becyberawareatsea.com

With thanks to our many industry supporters....

ROYAL NAVY
navarino
NORTH
Standard Club
STEAMSHIP MUTUAL
SHIPOWNERS

P&O FERRIES
inmarsat
JWC
CSO ALLIANCE MARITIME
NORWEGIAN HULL CLUB

CITADEL MARITIME
holman fenwick willan hfw
Maritime Security Review
V.Group
fidra films

ASKET Ltd
APMG International
INCE & CO
ZEUS

integro
GOLDPHISH
ARX
wididi

Gnostech Inc.
Novae
SHIPPINGCLUSTER
SECURE A SHIP
OSP SECURITY
OSP SAFETY

Digital Ship
ENDEAVOUR MARITIME
Blaythorne
Sovereign Global UK
SAFETY4SEA
UpGuard

ARB INTERNATIONAL
NSSLGlobal
GTMARITIME
Outstanding Security Performance Awards
seafarers
The Nautical Institute

eeSea
THAMES ESTUARY PARTNERSHIP
MARITIME TRUST
FRONTIER RISKS
Maritime Cyprus
SaveOurSeafarers

Sailors' Society
WATERWAY IT SOLUTIONS
FRONTIER HORIZONS
RIGEL
MARITIME UK
Liverpool & Manchester PSA PORT SECURITY AUTHORITY

Junge
Arcanum
POLYVERSE
TURREM DATA Group
Zephyr RCCU South West Regional Cyber Crime Unit

SOFT IMPACT
IMS
SOVREN
GLOBAL NAVIGATION SOLUTIONS
ELEKTRONIK LAB INDIA (PVT) LTD.

cyberprism
abto
PORT SECURITY CENTER
ICHCA INTERNATIONAL

GASLOG
Intership
smartmaritime
ICSPA
AST
BIBBY OFFSHORE