PHISH & SHIPS

Kindly sponsored by:

TDG Cyber Marine
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 21 is once again 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 assess the effects of another major shipping company having fallen foul of a ransomware attack. This time it is the Chinese container giant COSCO which has been left struggling to deal with the aftermath of an attack which began on offices ashore.

We also hear from experts on their views of some of the biggest cyber security issues today. Thank you to Gideon Lenky of EPSCO-Ra for once more sharing his expertise. Phish and Ships would be nothing without the support of industry, and experts who are willing to explain complex cyber matters in a way which we all can understand. Over the past issues, we have heard from an incredible array of experts, including Sharif Gardiner, Mark Sutcliffe, James Creasy, Edwin Lampert, Tim Parker, Stuart Quick, Akash Bharadia, Ian Millen, Siraj Ahmed Shaikh, Jaqueline Spencer-Sim, Lawrie Abercromby, Chris Lowe, Michael Shen, and even the “people hacker” Jenny Radcliffe. Thank you to all of them for taking the time, and also to you for reading.

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. We even have a new addition to our stable, with our boxing match poster, with seafarers pitted against cyber security. More details inside.

COSCO SHIPPING

COSCO HIT BY CYBER ATTACK

COSCO Shipping Lines’ operations in the US were hit by a cyber-attack last month. As a result its daily operations in the US were affected, and the attack made headlines around the world.

Upon the discovery, COSCO informed its customers that its network had broken down and that some electronic communications were not available as a result.

The company then embarked on a thorough assessment of the situation, in order to mitigate all possible problems and limit the impact of the attack on operations.

Despite the high-profile nature of the incident, and the fact that it naturally caught the attention of the industry and wider public, it is not thought that the attack was on the same scale as the cyber-attack against Maersk last year.

While it was thought that only operations in the Americas were hit, COSCO nevertheless had to check its worldwide operations in its wake and released this statement:

"After the network security problem in the Americas has been detected, to protect the interests of our customers, we have taken proactive measures to isolate internal networks to carry out technical inspections on global scale. With the reliable confirmation from the technical experts that the networks in all other regions are secure, the network applications were recovered at 16:00 (Beijing Time) on 25th July in all the regions except the Americas. As of now, all the business operations have been back to normal in the regions with network recovered.

Meanwhile, we are trying best to investigate and fix the network problem in the Americas, and it is expected that the network applications will be gradually back to normal soon. We have started contingency plans, such as transfer of operations and conducting operation via remote access, to ensure continuous service in the Americas. During the network failure period, there could be delays in service response in the Americas, and we are expecting your kind understanding.

It is our core value to protect customers’ interests and guarantee network security. Therefore, all the service and communication channels we are now providing are safe and secure. Please rest assured it is safe to keep contact with us via our website, emails, EDI or CargoSmart.”

According to reports, it all began when an employee in Ukraine responded to an email which contained the NotPetya Malware. It seems the same old mistakes keep getting made. COSCO issued a FAQ sheet on the incident http://elines.coscoshipping.com/notice/FAQ.pdf
IMO Secretary-General Kitack Lim took the opportunity to highlight the IMO’s response to the changing maritime security landscape while speaking at the ‘Maritime security in the 21st century’ symposium at the Brazilian Naval War College in Rio de Janeiro. Mr Lim stated that “threats to the port and shipping sectors are constantly evolving and so is IMO’s response” and he emphasised that “IMO is addressing the digital revolution in all aspects of its work”.

The Secretary-General underlined the IMO’s deep concerns regarding cyber security, including the potential vulnerabilities presented by ships’ onboard information technology and operational technology systems.

Mr Lim stated that as the maritime industry can drive and support a growing economy to create a better world for the future, the importance of ensuring safe, secure shipping will have wider benefits reaching far beyond the industry.

According to ‘Material Handling and Logistics’, over the next five years, maritime suppliers across the value chain will increasingly adopt solutions to address security, overcapacity and accurate cost models.

They see that new digitisation solutions such as big data, blockchain, automation, drones, and robotics, are enabling the maritime freight industry to introduce game-changing approaches that will significantly reduce or eliminate non-value-added activities.

Recent examples include Wärtsilä’s acquisition of Transas to support an intelligent maritime ecosystem and Artificial Intelligence (AI), as well as Orange Business Service’s deal with Cargotec for smart cargo handling.

Global maritime freight transportation revenue is expected to grow from $166 billion last year to over $205 billion in 2023.

Beneficial Cargo Owners are gaining greater supply chain visibility and automation from start-ups providing predictive logistics data, as well as crowdsourced, on-demand, real-time benchmark and market intelligence. New service offerings into the industry include real-time geolocation tracking for containers, while smart connected ports are on the rise.

Technologies such as big data, automated operations and Augmented and Virtual Reality will drive enhanced revenues and profits but alongside their development and usage should be full and comprehensive cybersecurity. Maritime cybersecurity will be necessary to address both current and emerging threats and, duly, global spend is predicted to rise to US$1.7 billion by 2023.

There are so many fascinating changes and advances coming to shipping, but the industry needs to make sure that it is able to harness them and use the intelligence to best effect.
It is evident that marine cybersecurity has not been a crucial topic in recent years, writes Graham Thompson of TDG Cyber Marine. This observation can be attributed to the fact that the field has not been a likely target or that information on successful attacks was not well known unlike the modern malware attacks on other inshore-based industries. Nevertheless, there have been reports of marine cyber-attacks before. For instance, hackers collaborated with drug traffickers and illegally accessed a digital tracking system at the Port of Antwerp. One recent case involves the NotPetya ransomware attack on Maersk Company’s global network, causing a loss of $300 million. In addition, some of the offshore and maritime organisations that have fallen victim to cybercrime in the past may have failed to report or detect such incidents.

Today, players in the global shipping industry are increasingly adopting the latest technologies and automation that have made incredible advances. In effect, it is thoughtless to rule out the possibility of hackers to launch data breach incidents that can cause disastrous chaos at sea. For example, they can use advanced tools and skills to access and manipulate a vessel’s AIS system to start sending wrong movement information. Moreover, they can use cutting-edge hacking techniques to illegally access an entire database containing cargo information. Other vulnerable marine systems, as listed by International Maritime Organization, include the bridge systems, access control systems, cargo management systems, communications systems, passenger facing public networks, crew welfare systems, and power control systems.

For that reason, it is crucial to raise awareness of marine cybersecurity issues. In addition, some of the offshore and maritime organisations in this sector should adopt reliable and effective cybersecurity profiles that deter any common and new threats that may compromise the marine cybersecurity.

The development of effective cybersecurity policies in the sector is quite similar to that in other industries. Primarily, the process requires a top-down approach in the organisation, where the issue is addressed at the executive level. As cyber threats grow in complexity and impact, cybersecurity should become a crucial concern that should be integrated to the overall safety management in marine operations. Moreover, all stakeholders in marine companies (board, shareholders, partners, employees) will be required to follow the following basic cybersecurity procedures:

- Use effective access control and other reactive and defensive measures
- Secure the network from malware and other attacks
- Develop and implement a secure backup plan
- Update operating systems and other software regularly
- Educate employees and stakeholders to raise awareness
- Review continuously the cybersecurity policies to ensure improvement

In addition to the rudimentary measures, marine cybersecurity requires tailored solutions addressing the industry-specific software, systems, procedures, human resource, and other marine needs. An essential approach to marine cybersecurity involves distinguishing operational technology systems and information technology solutions. The industry has systems that focus on the use of data as information and to monitor and control physical processes. In effect, the protection measures adopted should consider this distinction, as well as information exchange between these two main systems.

Additionally, the sector should adopt security standards, such as ISO/IEC 27001, ISO 22301, the IMO Guidelines on Maritime Cyber Risk Management, and NIST CSF 2014/2018 preparedness while developing their policies. As technologies and threats evolve, it is necessary for the sector to deploy a risk management strategy with resilient and evolving technical, operational, procedural, and management standards.

Combining legacy security practices and an understanding of marine-specific operations and needs will help create a safe environment for the industry in the wake of far-reaching threats from skilled cybercriminals. Besides, it is imperative to follow the guidelines provided on major cybersecurity standards.

TDG Cyber Marine is part of the Turrem Data Group of Companies that combines traditional IT best practices with a deep understanding of the maritime industry and the employed operational technologies. Our team of experts draw on extensive knowledge and experience in many relevant areas, including risk management, maritime operations and human intelligence. This helps ensure all testing and the suggested mitigation measures are tailored to the specific needs of clients.

With multifaceted vulnerabilities and cyber-attack scenarios, the answer lies in a holistic approach to reducing the risks of cyber-attacks and in a response mechanism for mitigating consequences if defences are successfully breached. TDG Cyber Marine uses a systematic and holistic approach to assess the cyber security of vessels and their interaction with land-based management. Best practices from risk management in maritime, oil & gas and energy applications come together to identify threats and build counter-strategies, looking at both technical and behavioural aspects.

Find out more at https://www.turremgroup.com/maritime-services/
UNDERSTANDING CYBER RISKS
INSURANCE POLICIES REQUIRE CALCULATED RISKS AND COSTS

According to insurance industry expert Nick Sanna, CEO of RiskLens: "As a rule of thumb, most companies buy cyber insurance for low likelihood but high impact events and spend on controls for higher likelihood events with a manageable cost."

The point is that cyber insurance should not be seen as a replacement for risk management, and certainly not used as an excuse to avoid research in risk quantification or for maintaining tighter security.

It is not a quick fix or a way of abrogating responsibilities, but insurance is a really important part of the armoury for any company.

Nick Sanna outlines the other issue concerning cyber insurance - its limitations. "Most policies are geared to mitigation for data breaches, a type of cyber event with well documented direct costs. However, it would likely be inadequate to cover reputational losses from a data breach that seriously impacted on market share or stock value."

As yet, there's no standard cybersecurity insurance policy and every insurance company handles cyber issues differently. Consequently, this means that it is up to the buyer to understand the threats that will affect them and estimate the potential losses for their specific organisation. In short, they need to start having those conversations about cyber risk quantification.

What is clear is that insurance should never be seen as a sole protection from cyber threats. In fact, insurance companies usually require as a condition of coverage that companies maintain at least the same level of security as existed at the time the policy was issued.

With the IMO requirements for maritime cyber security management to be enacted by 2021, then it is clear that actions need to be taken now.

DIGITAL SHIP SETS SAIL AGAIN

Digital Ship is excited to return to Hamburg, with the next in their series of Cyber Resilience Forums, taking place during SMM on 5 September 2018. The event provides an up-to-date insight into the cyber-threat landscape and how it is imperative to protect our business processes and data from attacks, damage or security breaches.

Ship operators need to analyse potential risks, explore legal aspects, and incorporate cyber resilience into their daily operations in order to organise business operations to reduce vulnerability. In this era of the connected ship we rely increasingly on technology, which makes cyber resilience business critical. So, how do we embed this into the maritime organisation, and into all our systems and operations? If incidents occur, how do we respond and make the necessary contingency or recovery plans? We will also investigate regulations and guidelines to develop a safe, compliant, cyber capability in shipping.

The human factor is often claimed to be the weakest link. Ship operators need to increase cyber awareness both in the office and on-board. In this Forum, we will discuss ways to mobilise internal commitment, set up training and incorporate cyber awareness into daily procedures. See online for details and to book your place: https://www.smm.thedigitalship.com

PHISH & SHIPS
The Allianz’s annual Safety and Shipping Review 2018 has recently been released. Each year this review focuses on key developments in maritime safety and analyses shipping losses (of over 100 gross tons from the preceding 12 months, to 31 December 2017 for this report). It also identifies some of the key risk management challenges the industry faces moving forward.

The report confirms that shipping is the lifeblood of the global economy, transporting approximately 90% of global trade. There are over 50,000 merchant ships trading internationally, carrying every kind of cargo, so the safety of vessels is critical. Losses at sea remained stable, even declining slightly to 94 – the second lowest total over the past decade – while over a 10-year period, ship total losses have declined by more than a third, driven by multiple factors including advances in risk management and safety.

Allianz’s report cites technological breakthroughs in playing a significant part in ship safety at sea and it highlights the value in protecting these technologies from cyber threats. As might be expected, the report found that shippers were getting ‘serious on cyber’, starting with its inclusion, for the first time, in the top 5 risks to marine and shipping according to survey respondents. It also outlined more fully the extent of major attacks, such as NotPetya, which caused around $3bn of economic losses, affecting some 2,000 organisations across 65 countries with one logistics company, FedEx, picking up $300 million in lost business and clean-up costs. The high-profile nature of these attacks have however, created a renewed urgency in tackling the threats posed to vessels and the supply chain, as well as increasing interest in cyber business interruption insurance.

However, Allianz still expressed concerns about the current lack of incident reporting, which they fear masks the true picture in shipping when it comes to cyber risk. New regulations such as the European Union’s Network and Information Security Directive are predicted to change that, with the UK announcing that it could impose sanctions of up to $22.6 million in fines if companies do not report series breaches.

Allianz state that shipping companies need to focus on a positive inclusive approach to cybersecurity, including robust training and auditing as well as vessel safety management systems. They find that many in shipping are actively looking to improve cybersecurity on board, for example by separating IT systems for different functions, such as navigation, propulsion and loading.

You can access the full report at https://bit.ly/2msclig
This might seem like an odd topic for maritime; however, over the past year mobile device malware has accounted for the majority of security incidents my company handles aboard vessels. Typically, the incident pattern unfolds as follows, someone brings an infected mobile device aboard and then connects it to a WiFi network onboard. The infected mobile device is remotely under the control of an unknown third party via the Internet connection and thus the vessel network the device is connected to is now visible to the attacker from across the public Internet. From the attacker’s perspective it’s game on. Luckily we catch these things fairly quickly and shut them down, though I doubt the intended target in these cases was a vessel in the first place.

It’s a casual topic and it comes up outside of my professional conversations more than any other specific security topic. It usually starts out “Is iPhone or Android more secure?” My answer is determined by whom I’m talking to because the answer isn’t the same for everyone. In general for most people the answer is the iPhone is more ‘secure’, meaning less likely to be exploited by malware. That is, the most security enabled phone on the market, the Silent Circle Blackphone, is based on Android. A heavily modified Android that is expensive, inconvenient and for the most part, only for the Secret Squirrel types who are willing to compromise features and a bit of performance in favour of privacy and security.

So for most people the Apple mobile devices are simply a better choice for security. This is because the Apple model uses an application “Whitelist”, meaning only applications on the list can run on the device. Since there’s only one place to get the applications, the Apple App Store, it’s hard for attackers to get their code onto the device.

Mobile application developers will attest to the lengthy wait between submitting their code and it being available in the App Store. This is due to a process designed to scrutinize the application and identify potential malicious code or application behaviour that violates Apple policy. The only way to load an application that is not from the Apple store is to “jailbreak” the phone. This will allow you to run software that is not approved by Apple from third party repositories. This gives more access to free third party apps but defeats the safety controls built into IOS. It’s not a perfect system, nothing is, but it is fairly effective compared to what Google Play does with Android.

Android apps are downloaded from Google Play. You can also load apps from other locations and even files as well, a practice called sideloading. While Android is configured by default not to do this, enabling sideloading is simply an option in Android settings. It is a fairly common practice to load non-Google Play apps in this way. And therein lies the problem. It is very easy for an attacker to download a legitimate application, modify it with malicious code and then put in either back onto Google Play with a slightly different name or simply provide it from another location so it can be sideloaded “for free”. Both the Google Play security process and sideloading are problematic. For example, earlier this year Google Play removed 22 flashlight applications which were identified by security firewall vendor, Check Point, as containing a malicious adware called LightsOut. In this case, it was only annoying adware; however, it demonstrates the problem.

Had Check Point not identified the apps, they would probably still be there. Ask an app developer about uploading the Google Play and they’ll tell you it’s very fast. Very different from the Apple App Store process.

So back to our mobile device incidents aboard vessels at sea. Do you care to take a guess which kind of devices are involved? If you guessed Android, you would be correct. Android users must be especially careful which applications they load and where they load them from.

And therein lies the problem. It is very easy for an attacker to download a legitimate application, modify it with malicious code and then put in either back onto Google Play with a slightly different name or simply provide it from another location so it can be sideloaded “for free”. Both the Google Play security process and sideloading are problematic. For example, earlier this year Google Play removed 22 flashlight applications which were identified by security firewall vendor, Check Point, as containing a malicious adware called LightsOut. In this case, it was only annoying adware; however, it demonstrates the problem.

Had Check Point not identified the apps, they would probably still be there. Ask an app developer about uploading the Google Play and they’ll tell you it’s very fast. Very different from the Apple App Store process.

So back to our mobile device incidents aboard vessels at sea. Do you care to take a guess which kind of devices are involved? If you guessed Android, you would be correct. Android users must be especially careful which applications they load and where they load them from.

Even then, there are no guarantees since a legitimate looking app from Google Play can contain malware. Load only what you need and stay away from sideloading ‘free’ apps that normally cost something in Google Play.

To learn more about EPSCO-Ra see https://www.epsco-ra.com
**A-Z OF CYBER SECURITY**

**U** is for update. You may get tired of being asked to update software, but they protect against cyber attacks. Software updates are vital, so don’t delay.

**V** is for vulnerability. No piece of software is perfect and, even after years of testing, new bugs are often found. Vulnerabilities are bugs that permit someone to use the software in a bad way.

**W** is for WannaCry. This was a major cyber security news story last year. These days it’s quite rare for a single piece of malware to cause overnight panic. WannaCry was similar to most families of ransomware, and these are still a problem.

**X** is for XSS. Cross Site Scripting (XSS) is one of the most commonly used methods to attack visitors to a website. XSS works by exploiting vulnerabilities in web applications that permit attackers to insert their own code to steal credentials or cookies, allowing them to access their accounts and/or impersonate them.

**Y** is for YARA. As the number of new malware threats multiplies every year, protecting against them presents a constant challenge, requiring innovative new tools and techniques. One tool that is growing in popularity is YARA. An open source initiative, YARA is a tool firms can use to identify and flag malware.

**Z** is for Zero Days. Vulnerability exploits are a key tool for attackers attempting to compromise a computer or web server. Zero-day vulnerabilities are the holy grail for attackers; they are previously unknown vulnerabilities that have yet to be patched by the software vendor.

source: medium.com
A NEW CYBER SECURITY FRAMEWORK

In our modern, connected and digitised world, cyber threats have become a fact of life, capable of doing harm to people, vessels and business. The IMO has given ship owners and managers until January 2021 to incorporate cyber risk management into ship safety. Non-compliant vessels will be at risk of detention after this deadline.

With this in mind, GNS has produced a new guide to cyber security, and the simple, memorable “3i Cyber Security Framework” to help the industry both improve understanding of cyber security and develop best practice.

To protect themselves, organisations need to reduce the probability of high impact events. GNS’s 3i Cyber Security Framework provides a simple and easy to remember way for any maritime and marine organisation to achieve this by proactively harnessing the mutually supportive power of people, process and technology to address all risks, including the more scary ones, using a holistic risk-based approach.

The shipping industry is used to managing and protecting assets in a business and operating environment fraught with risk, through education, training and a highly developed risk based culture. It makes sense to extend this methodology to cyber security.

Cyber security is a subject that needs to be understood and implemented ‘From the Boardroom to the Bridge’ and taken seriously if owners are to avoid problems ranging from disruption of operations to reputational damage, pollution, financial liability and, in extremis, loss of life.

If senior management are in any doubt about this, they just need to look at the cost of the cyber-attack on Maersk or, outside of shipping, the way that ‘Equifax’ shares plummeted after a cyber-attack that they suffered.

Find out more about GNS’ innovative new approach online, by visiting: https://bit.ly/2mSbJTj
According to a recent whitepaper released by Arthur J. Gallagher & Co, the transportation industry now ranks third in security vulnerability. They state that GPS tracking, computer networks, and automation are all specific vulnerabilities within the industry.

Adam Cottini, managing director of the cyber liability practice with Gallagher says, “An overlooked component of this discussion is when you think about the premises, the grounds themselves, where you have automation put into the actual movement of goods and products on the ground into the vehicles themselves”.

The fallout from a breach for a shipping company can impact others inside and outside of the industry – consumers and resellers, for instance. A pause in operations as well as products being transported, often ensues when a transportation company is struck with a hack. With serious consequences up and down the chain.

Hacking can cause a tremendous amount of ripple effect, and at the end of the line, people hoping to buy goods might be left empty-handed if those items never make it to stores. This means that business interruption is a key component of the cyber insurance coverage for this sector.

“The biggest and most sought after component of insurance for the transportation business is the cyber extortion coverage and the business interruption coverage,” said Cottini. “That piece of the pie has contingency concerns that exist uniquely in the space of transportation that a lot of other entities may not feel as strongly about.”

While the transportation industry has implemented technology in some ways, namely to increase efficiency in operations, the adoption of technology that minimizes vulnerability to cyber threats hasn’t necessarily occurred at the same rate. Cottini cites an endpoint technology that monitors for cyber attacks through AI and machine learning, and can detect zero-day attacks, which are new and never-before-seen, and thus don’t have a known signature yet. “The transportation business as a norm is less willing or less inclined to adopt this technology than we have seen from other industries,” he said.

While the discussion around cyberattacks is growing, especially as Gallagher’s whitepaper states that 2017 was a record year for cyberattacks and the average total cost per breach for the average company has reached $3.79 million, there are certain elements missing that make the conversation relevant to the transportation industry.

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 latest in our series can be seen above, and captures the fact that seafarers are in a daily fight against not just the cyber security risks and threats which face them, but actually the tools which are meant to help them.

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.

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

Stay safe and cyber secure out there!
Marine Overwatch Services

**Dedicated**
- A strong determination to hunt and lock down cyber threats to ocean going vessels.
- A pledge to keep you constantly informed about your security posture.
- A commitment to continuously enhance our services.

**Focused**
- A friendly and accessible team acting as a virtual extension of your in-house resources.
- Improving the effectiveness and ease of our solutions through implementation of customer feedback.
- Regular reports and service reviews to keep your IT and management teams updated about your security posture.

**Experts**
- In depth analysis and advice you can trust.
- Experience in protecting global shipping and their land-based headquarters.
- A friendly and marine knowledgeable team qualified to world-class standards.

**Flexible**
- Cost effective cyber security solutions that can be tailored to meet exacting technical and commercial requirements.
- Easy to manage technology that can be deployed on vessels easily as virtual or physical appliances.
- Highly scalable solutions designed to keep pace with your growing network infrastructure.