#17
APR: 2018

PHISH & SHIPS

BE CYBER AWARE AT SEA

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".

Inside issue 17, sponsored by Arthur J. Gallagher & Co - we bring you more news about maritime cyber security, or the implications of the shipping industry's vulnerability. These problems are not going to simply go away, there is much work to be done.

So, this time round we bring you news of yet another cyber headache for Maersk, but we bring solutions too. Our good friends from Epsco-Ra share their thoughts on heading off problems, and Coventry University is now also in the maritime cyber mix.

Primarily though, we need to remind you about the human side of cyber security and the fact that executives and managers ashore need to ensure that seafarers have the tools, training and resources to act against cyber threats. A new study on maritime connectivity has highlighted the concerns of crew when it comes to cyber security, and the fact that they feel underprepared, and unsupported when facing these problems. We, the shipping industry, have to do more - so we urge you to make sure that everyone in your company is aware of Be Cyber Aware at Sea.

See https://www.becyberawareatsea.com/ for more details and please support our campaign and don't forget to download our free resources, including our poster campaign.

WATCH WHERE YOU SURF!
LOOSE CLICKS SINK SHIPS!
DO NOT FEED THE PHISH!
BE WISE TO WHAT LIES INSIDE
BE DISCREET WHEN YOU TWEET
DON'T FALL FOR THE HONEYTRAP

YET MORE CYBER WOES

In June 2017 the world's largest container shipping line, Maersk, was hit by a massive cyber attack. In the wake of that, the last thing the company needs is another cyber hit. Unfortunately, Maersk group subsidiary, Svitzer, recently revealed that it has suffered a significant data breach. A problem which has seen upwards of 50,000 emails containing private personnel information, auto-forwarded to accounts outside the company.

Localised to the company's Australian operations, Svitzer has confirmed that the hack, which began on May 27 last year, affected more than 400 employees before being discovered at the beginning of this month.

The problem seemingly went unnoticed, as for almost 10 months, between 50,000 and 60,000 emails from three Australian employees of the salvage and towing group working in finance, payroll, and operations, were automatically forwarded to two accounts outside of Svitzer, containing staff personal information including tax file and superannuation numbers and the names of next of kin.

The breach was resolved within five hours of being discovered, after the mailboxes of the external inboxes became full and the auto-forwarded emails began bouncing back to the company. Quite whether they would ever have noticed otherwise is a subject of debate.

After an investigation, Svitzer found that a rule had been set up on the three email accounts to forward the emails to the external accounts and another rule to delete the forwarded emails so the account holders couldn't see the emails were being forwarded.

Obviously the Svitzer issue was on a much smaller and less damaging scale than the attack on Maersk last year, however it does highlight that even the mundane, shorebased, workaday aspects of shipping companies are under threat.

Vigilance is necessary within all parts of the business - and while our campaign is about cyber awareness at sea, it counts for little if this is not matched ashore.

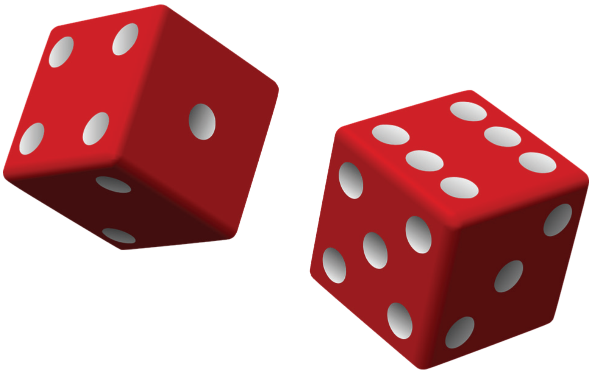
IMO STRESSES CYBER ROLE

In the face of criticism, the International Maritime Organization (IMO) has stressed the fact that it has been taking a strong lead on cyber security issues.

The IMO has discussed cyber security in both the Facilitation and Maritime Safety Committees and issued guidance. It has also adopted Resolution MSC.428(98) – Maritime Cyber Risk Management in Safety Management Systems. The resolution encourages administrations to ensure that cyber risks are appropriately addressed in existing safety management systems – as defined in the ISM Code – no later than the first annual verification of the company's Document of Compliance after January 1 2021.

Further, IMO Member States have adopted the strategic plan for IMO at the last assembly, which recognises the need to integrate new and advancing technologies in the regulatory framework – balancing the benefits derived from new and advancing technologies against safety and security concerns, the impact on the environment and on international trade facilitation, the potential costs to the industry, and their impact on personnel, both on board and ashore.

MODELLING THE LEVELS OF CYBER RISK FOR BUSINESS



Guessing whether you are at risk of cyber attack is easy - the answer is yes. However, it can be useful to actually understand and model the full scale of the threat and of the vulnerabilities within your company.

Risk modelling firm, Risk Management Solutions (RMS), has developed its first probabilistic risk model for cyber attacks, with contagious malware such as NotPetya as wildcards for future cyber catastrophes.

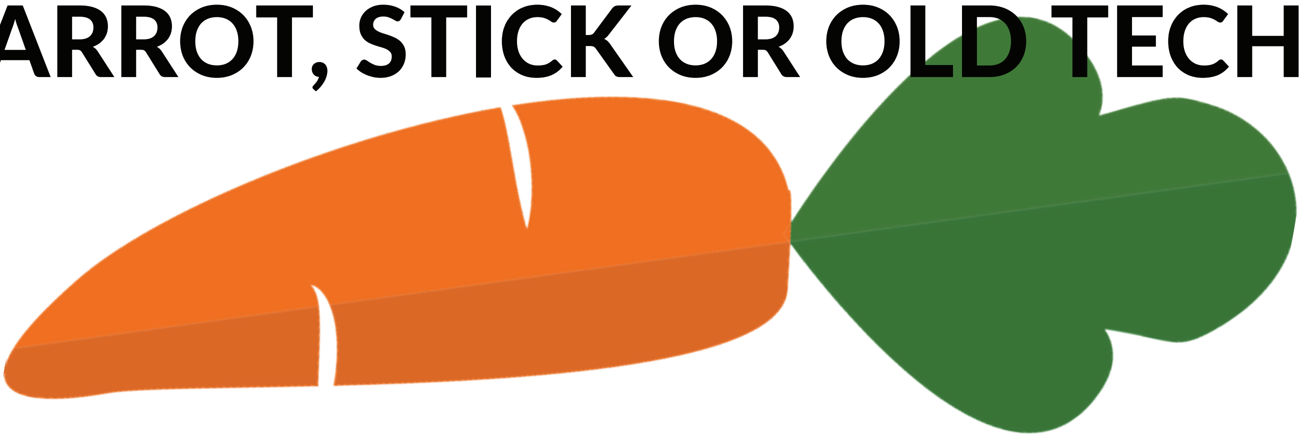
The probabilistic risk model splits cyber into five basic types of attack:

- data exfiltration;
- contagious malware;
- financial theft;
- cloud outage; and
- distributed denial of service (DDoS) attacks

Data exfiltration has accounted for just over half of an estimated $2.3bn in cyber insurance claims over the past six years in the US market alone, according to the company who has established the new system, RMS.

The risk modelling enables insurers to allocate risk capital and to design products and risk solutions that reflect the full nature of cyber risk. It also adds additional functionality to apply to reinsurance of cyber losses, providing financial perspectives to all reinsurance stakeholders. In addition, it provides tools to allow model users to incorporate their own loss experience into the model and develop their own view of risk.

CARROT, STICK OR OLD TECH



HOW SHOULD THE MARITIME INDUSTRY TACKLE ITS CYBER SECURITY?

Given the vulnerability of the maritime industry to cyber attack, a researcher at the US-based Center for International Maritime Security has suggested two ways in which the industry can fight back. One is funded, one is to use better training, and use of existing facilities:

COURSE OF ACTION A: Government Subsidies for Mandated Cybersecurity Awareness and Training

A Government-enabled focus on prevention and response would proliferate horizontally and vertically across the maritime shipping community.

Such an approach would subsidise the buy-in for industry to approach cyber security as a cost-effective asset. Simultaneously, educating the lower echelons of the workforce on digital hygiene to understand the transmission of ransomware and other forms of cybercrime.

Complacency and overhead costs are often cited, and so this funded model could assist companies to get past such barriers. Though the researcher himself questions whether it is the role of government to provide funding to make cyber security more attainable when good governance and management shows just how vital this is. However, it would be interesting to see how a carrot approach could sit alongside that of the usual stick.

COURSE OF ACTION B: Leverage Manual Operations and Dated Communications Technologies

A no-and-low-tech approach encourages the use of manual navigations operations and older long-range navigation (LORAN) systems to circumvent disruptions to navigational and operational systems.

A positive consequence of this approach is the standardisation of backup operations for seamless continuity of operations on land, while also mitigating the overreliance on technology at sea.

This is a probable course of action given the existing LORAN infrastructure and the crippling effect of cyber attacks on shipping company capabilities.

However, a negative consequence is a proliferation in ransomware attacks deliberately targeting this industry since the approach would be passive in nature. However, others may argue that manual training and a functional secondary means of communication mitigates adverse costs from future ransomware attacks.

CONCLUSION

Course of Action A provides the highest return on investment to address the ransomware threat to the American maritime shipping industry. This prevention-focused and proactive approach will induce a top-down, lateral, and public-private approach to address maritime cyber security.

While Course of Action B identifies the existence and use of alternative approaches to circumvent – or, at worst, mitigate the consequences of – a ransomware attack, it fails to place a premium on industry-wide digital hygiene which is arguably the most cost-effective, scalable, and fastest approach to ransomware prevention.

What do you think? We'd love to hear your thoughts - should governments be funding cyber resilience in shipping? Or does the international nature of the industry nullify that approach?

Should we be looking to older, more robust ways of operating? Drop us a line and let us know:

think@becyberawareatsea.com

- -

CLASS SPLASHES OUT BUYING CYBER OUTFIT

Lloyd's Register (LR) has acquired cyber security services provider Nettitude, which it describes as a research-led organisation with 'some of the most sophisticated technical capabilities in the industry'. "This is an important acquisition for Lloyd's Register to enhance our capability in assuring the increasingly complex supply chains in which we operate," said LR CEO Alastair Marsh.

"As the worlds of Information Technology and Operating Technology collide, the need to build integrated cyber security solutions will become essential," commented Nettitude founder and ceo Rowland Johnson, pointing up LR's geographic reach, and "vision for how technology and data will influence industry." LR already provides a range of cyber security services to its clients, including certification, compliance, training, audit and security consulting.

MARITIME CYBER INTRUSIONS SPIKE

Covert attacks against the U.S. tied to a suspected Chinese cyberespionage group known as "Leviathan" have spiked since early 2018, new research reveals.

FireEye, a California-based security firm which investigates major hacking groups known as advanced persistent threats (APTs), claims the group—which it codenames "TEMP.Periscope"—is ramping up attacks on American entities working on issues associated to the disputed South China Sea territory.

The espionage unit, which is well-resourced and known to focus on high-level targets including government agencies, shipping and engineering firms, research institutes and defence contractors, shares malware code with "other suspected Chinese groups" and infiltrates victims using email spearphishing tactics.

Since early 2018, FireEye has been tracking this ongoing wave of intrusions and the current campaign is a sharp escalation of detected activity since summer 2017.

TEMP.Periscope BACKGROUND

Like multiple other Chinese cyber espionage actors, TEMP.Periscope has recently re-emerged and has been observed conducting operations with a revised toolkit.

Active since at least 2013, TEMP.Periscope has primarily focused on maritime-related targets across multiple verticals, including engineering firms, shipping and transportation, manufacturing, defence, government offices, and research universities.

However, the group has also targeted professional/ consulting services, high-tech industry, healthcare, and media/publishing. Identified victims were mostly found in the United States, although organisations in Europe and at least one in Hong Kong have also been affected.

IMPLICATIONS

The current wave of identified intrusions is consistent with TEMP.Periscope and likely reflects a concerted effort to target sectors that may yield information that could provide an economic advantage, research and development data, intellectual property, or an edge in commercial negotiations.

MALWARE ARSENAL

In their recent spike in activity, TEMP.Periscope has leveraged a relatively large library of malware shared with multiple other suspected Chinese groups. These tools include:

AIRBREAK: a JavaScript-based backdoor also reported as "Orz" that retrieves commands from hidden strings in compromised webpages and actor controlled profiles on legitimate services.

BADFLICK: a backdoor that is capable of modifying the file system, generating a reverse shell, and modifying its command and control (C2) configuration.

PHOTO: a DLL backdoor also reported publicly as "Derusbi", capable of obtaining directory, file, and drive listing; creating a reverse shell; performing screen captures; recording video and audio; listing, terminating, and creating processes; enumerating, starting, and deleting registry keys and values; logging keystrokes, returning usernames and passwords from protected storage; and renaming, deleting, copying, moving, reading, and writing to files.

HOMEFRY: a 64-bit Windows password dumper/cracker that has previously been used in conjunction with AIRBREAK and BADFLICK backdoors. Some strings are obfuscated with XOR x56. The malware accepts up to two arguments at the command line: one to display cleartext credentials for each login session, and a second to display cleartext credentials, NTLM hashes, and malware version for each login session.

LUNCHMONEY: an uploader that can exfiltrate files to Dropbox.

MURKYTOP: a command-line reconnaissance tool. It can be used to execute files as a different user, move, and delete files locally, schedule remote AT jobs, perform host discovery on connected networks, scan for open ports on hosts in a connected network, and retrieve information about the OS, users, groups, and shares on remote hosts.

China Chopper: a simple code injection webshell that executes Microsoft .NET code within HTTP POST commands. This allows the shell to upload and download files, execute applications with web server account permissions, list directory contents, access Active Directory, access databases, and any other action allowed by the .NET runtime.

A-Z OF CYBER SECURITY

A

A is for Authentication, which is the backbone of data exchange. We tend to use single factor - username and password, but this poses many security problems.

B

B is for Business Email Compromise scams which are among the most lucrative for cyber criminals. Also known as “whaling” or “CEO fraud”, BEC scams don’t require too much technical sophistication.

C

C is for Cryptocurrencies such as Bitcoin. These have had a major impact on cyber security. Cryptocurrencies have quickly become the default currency on the cyber underground and made ransomware.

D

D is for Denial of Service (DoS). One of the biggest causes of online disruption is denial of service attacks, where websites or the networks of entire organizations are knocked offline, usually by flooding them with traffic.

E

E is for Exploit Kit, one of the methods cyber criminals use to infect people with malware. They allow attackers to use a website to infect unsuspecting visitors. They work by exploiting vulnerabilities in software in order to install malware.

source: medium.com

VULNERABILITY MANAGEMENT IN MARITIME

Gideon Lenkey, Director of Technology at Epsco-Ra brings us his thoughts on some of the cyber challenges facing shipping and the unique solutions which may be needed.

Vulnerability Management, at its most basic, is a process by which computer or device vulnerabilities are identified and fixed at a frequency high enough to have a positive effect on the rate of security incidence.

Let's unpack that a bit. The most common way to identify vulnerabilities is to use a vulnerability scanner, Nessus or OpenVAS, for example. This only works when the computers are network connected because that's how the scanner communicates with them. The scanner finds open ports and associated running services, identifies their version numbers and in some cases configuration settings, which are then compared to a database of known vulnerabilities. Some scanning software will also log into the machine being scanned and look for additional areas of vulnerability, such as default configurations, unidentified services and weak registry settings. This is called authenticated scanning.

Vulnerabilities detected are ranked by severity. A vulnerability that can be exploited to perform remote command execution, run an attacker's code essentially, would be considered critical because the machine is at immediate risk of being compromised by an attacker. A vulnerability that results in leaking information, the machine name or internal IP address, might be classified as serious because while it may give an attacker some information or advantage, it can't be directly exploited. Generally speaking, vulnerabilities should be remediated in order of severity. This quickly lowers risk based on the information gathered.

How often you run a vulnerability scan and the frequency depends on a number of factors such as, how critical the machine is, how often it's patched and how quickly detected vulnerabilities can be fixed. On networks of critical machines weekly is not uncommon, whereas for general user populations monthly is a popular choice of frequency. Scanning at a lower frequency, i.e. quarterly, may be appropriate for equipment that doesn't change much, i.e. VOIP appliance, but would be too low for end user computers. Scanning at too low a frequency means that a vulnerability may go undetected for an extended period of time which increases the chance it will be exploited.

Maritime has its own industry specific challenges when it comes to vulnerability management on vessels. Some vessels have very limited Internet network speeds and data plans which aren't patch friendly in the first place.

Vulnerability management as a business process on vessels such as this is almost non-existent. There might be the occasional patch delivered on removable media while in port but aside from an Anti-Virus database update, it's more likely to be focused on software versioning than software security updates. Malware introduced by a laptop, tablet or USB would be devastating in this case as remote network assistance is not very practical, if even possible. In the event that critical systems, such as the communication PC on the bridge were infected with something persistent, the crew would have to revert to secondary or emergency processes and live without until returning to port.

Vessels with newer high speed Internet have more options. Vulnerability management is possible through either on-board scanning or shore based scanning through a VPN. The higher Internet speed also accommodates remote remediation of critical vulnerabilities while under way. The vulnerability management process gives the IT manager the information needed to decide what to fix/patch and when. If you're not doing this or something similar, then you really should be.

One final thought; One issue maritime must consider is that the (potentially) network attached systems onboard, such as SatCom, propulsion, cargo, sensors etc., are not subjected to the same level of scrutiny as something like a Microsoft operating system or Cisco router. This means that this equipment, the infrastructure of the vessel itself, likely has unknown and exploitable vulnerabilities which will NOT show up in a vulnerability scan.

The maritime industry as a whole should have a hard look at how other industries are addressing and even incentivizing the discovery and documentation of vulnerabilities. If maritime doesn't address this then the very infrastructure the industry is tying it's future to could be easily exploited by a long list of malicious actors.

EPSCO - RA
Maritime Cyber Security Solutions

MARITIME SYSTEMS

THE CHALLENGE OF CYBER SECURITY

The UK's reliance on a secure and stable maritime sector makes maritime cyber security a key concern. Cyber security is defined by the recently released National Cyber Security Strategy of the UK as the protection of information systems (hardware, software and associated infrastructure), the data on them, and the services they provide, from unauthorised access, harm or misuse. This includes harm caused intentionally by the operator of the system, or accidentally, as a result of failing to follow security procedures.

The strategy has also clearly identified cyber-physical systems to be potentially vulnerable to interference from cyber threats. Cyber-physical systems are engineered systems that bring together a mix of traditional electronics, advanced sensing and connectivity, and physical components (such as maritime infrastructure and vessels). This vulnerability is particularly so due to increased connectivity and reliance on digital components, increased levels of autonomous control and globally accessible navigation systems.

Cyber security measures need to protect assets against a range of low-level crime to national security concerns. Such assets could be tangible, for example ships, vessels, rigs, port equipment and navigation aids; or could be intangible, for example, data, information services and supply chain elements. At an operational level, it is a mix of both types of assets that underpin the maritime sector. Therefore cyber security measures need to protect a complex set of assets.

Over the past decade or so, a number of cyber attacks have been identified within the maritime sector, which have a range of demonstrable impacts including manipulating enterprise and information assets, jamming and subverting GPS and navigation systems, and hijacking critical control systems to cause physical damage. We briefly discuss each of these class of attacks.

Enterprise systems are designed to achieve efficient digitisation of information services. Attacks on such systems have aimed to disrupt enterprise activities but have also resulted in theft of information that is far more damaging in terms of organisational services and objectives. The risks posed by such attacks are low to medium however, as enterprise data, operations and procedural aspects may be potentially violated, with no or very little physical disruption, and no loss of life.

Certain virtual-technology-driven attacks take advantage of design issues and inherent vulnerabilities, exploited to undermine services dependent on such technologies. GPS and navigation technologies, given their acute use in the maritime sector, are a particular target that have come under close attention. The risks posed by any such attack is medium to high as, alongside data and operation protocol violation, there is potential for physical damage.

With the aim of disrupting national security, more advanced cyber attacks have targeted control systems to cause maximum damage, including actual physical disruption or damage. These originate from either state or non-state actors often driven by motivation to achieve political goals. Such intent is established through the level of preparation and resources deployed, typically including intelligence gathering using a mix of digital and other means, theft of state secrets and location of assets, industrial espionage to subvert technological safeguards, and the level of skills and know-how used to deliver the attack. The maritime infrastructure offers a number of critical assets that could be targets for such attacks. These include ports and related land-based assets, ships and smaller vessels, as well as satellite communication, positioning and navigation systems.

Across these incidents a visible rise in criticality has been observed in terms of threat motivation, technical competence of attackers and complexity of employed attacks. Besides the increasing seriousness of such threats, some technological developments for the maritime industry merit special attention: these include advances in communication, improved sensing, and intelligent and autonomous control systems. All three pose cyber security challenges as they build over existing digital technologies, allowing for broader access to ships and vessels, as well as making potential software-dependent weaknesses easier to exploit for malicious gain.

As the availability and adoption of such technologies grow, their integration is expected to converge across the maritime platforms. This will be a step change in the nature of design and engineering involved to ensure safety and cyber security.

What does this mean for the technology integration and platform engineering needs of the future?

Traditional engineering methods have coped with safety-critical systems engineering of such ships and vessels in these examples with modelling and design techniques focused entirely on safety and with little thought to security. Not only are accidents to be avoided but systems need to be designed to defend against malice and manipulation with intent (to cause damage). Early research suggests that designing secure safety-critical systems poses a substantial challenge with a view that engineering complex embedded-and cyber-physical systems requires a holistic view on both product and process. This implies a clear need for best practices and compliance standards alongside rigorous engineering that incorporate both security and safety. The notion of risk-based systems engineering is therefore one way forward that acknowledges cyber security risks in the systems engineering lifecycle.

Siraj Ahmed Shaikh is Professor of Systems Security and leads the cyber security group at the Institute of Future Transport and Cities (FTC) at Coventry University.

CYBER NEWS IN SHORT

IRISH GOVERNMENT GUIDANCE

The Irish Department of Transport, Tourism and Sport (DTTAS) has issued an advisory to the maritime sector to make cyber security an integral part of their risk assessment exercises and continuity plans. This follows the Maritime Safety Committee (MSC) of the International Maritime Organization (IMO) in 2017, where measures were agreed in relation to the cyber risk being taken into account by shipping companies in respect of the International Safety Management Code.

Cyber risks have to be appropriately addressed in safety management systems no later than the first annual verification of the company's Document of Compliance after 1 January 2021. In relation to ports, Ireland is to incorporate a cyber security risk element in the security assessments which are carried out in accordance with Regulation (EC) No 725/2004 1 and Directive 2005/65/EC 2 in ports and port facilities.

The next five-yearly renewal of these assessments is due in all Irish ports by 30 June 2019. The Irish Government has issued new guidelines which can be accessed at https://goo.gl/Qjd7ps

NEW CYBER NOTATION

Classification Society Bureau Veritas has developed a comprehensive approach to support shipowners in addressing maritime cyber risks. A new series of classification notations, guidelines, and services enable owners to comply with regulatory requirements, safeguard their crews, and protect their assets from both malfunction and malicious attack.

Bureau Veritas now offers two cyber notations. The first, SW-Registry, focuses on software change management and requires the creation and maintenance of a certified register of software used in the ship's onboard systems. A second new notation, SYS-COM, addresses cyber security, and is directed at preventing malicious cyber attacks.

CAREFUL ON CHARTER PARTIES

BIMCO has begun the task of investigating the need for a cyber security clause and what issues it should address. The focus is on raising general awareness of cyber risk among owners and charterers – being proactive and encouraging them to establish common sense procedures and policies that will help them manage their cyber risk. But if they fall victim to a cyber attack, will the provisions of the charter party be robust enough to protect their interests - or will they be exposed to uncertainties?

Read BIMCO's Grant Hunter's thoughts: https://goo.gl/fUdtR8

Gallagher

Insurance | Risk Management | Consulting

Marine Cyber Insurance

Specifically developed to respond to cyber
risks of the Maritime sector

24/7 GLOBAL EMERGENCY RESPONSE

Crisis Response both onshore and offshore including IT forensic costs

BUSINESS INCOME LOSS

Due to network interruption or downtime

RISK MITIGATION

Maritime specific employee training

CYBER EXTORTION

Including the payment of cryptocurrencies as approved by insurers.

LIABILITIES FOR LOSS OF INFORMATION

Including corporate sensitive data such as cargo locations

To find out more get in touch:
www.ajginternational.com

Michael Ingham
·+44 20 7204 1864
Mike_Ingham@ajg.com

James Richardson
+44 20 3425 3232
James_Richardson1@ajg.com

Edward Remnant
+44 20 7204 6033
Edward_Remnant@ajg.com

Arthur J. Gallagher (UK) Limited which is authorised and regulated by the Financial Conduct Authority. Registered Office: The Walbrook Building, 25 Walbrook, London EC4N 8AW.
Registered in England and Wales. Company Number: 1193013. www.ajginternational.com. FP198-2018 exp. 21/2/19.