#16

MAR:2018

PHISH & SHIPS

BE CYBER AWARE AT SEA

Kindly sponsored by

Gallagher

Insurance | Risk Management | Consulting

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 16, we welcome this month's headline sponsor Arthur J. Gallagher & Co - and thank them for their support. The fact that such a company backs our vision for sharing awareness and engaging with the challenges of maritime cyber security is testament to their commitment. It also shows that we are making great strides in supporting the shipping industry.

Also inside this issue, cyber security experts share their views on the steps to developing an effective incident response plan, and the technological advances which are shaping the future of shipping.

Remember, simply hoping for the best will never be enough! This time round we feature a host of articles on some of the key issues surrounding maritime cyber security. From the costs of attacks, through to the development of new Classification Society developments, and the latest guidance to emerge from the National Cyber Security Centre.

We bring you the latest insight - but also the tools to make a difference. It is vital that employees both afloat and ashore are cyber aware. So visit our website, see the resources we have, and make every use of them. Thank you for reading, and don't forget to make sure you are cyber aware at sea.

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

VERY SPECIAL WELCOME...

Gallagher
Insurance | Risk Management | Consulting

As we have said above, in this issue of Phish and Ships, we are extremely proud to welcome Arthur J. Gallagher & Co as our latest industry sponsor. One only has to read the storied history of the company to understand why they are supporting our initiative. The "Gallagher Way" is more than just placing coverage and selecting a plan. It is the code by which we live. Providing insurance, risk management and consulting to go beyond just business goals.

Every day, the company's clients face massive challenges across a range of issues. It is Gallagher's advisors who understand their business and how hard their clients work to deliver on promises. So they do all possible to support, acting as a global partner in achieving goals. This is an approach which only begins to describe the shared values, corporate culture and passion for excellence of the Gallagher way of doing business. Indeed, Arthur J. Gallagher & Co. - the only insurance broker on the Ethisphere Institute's list of the World's Most Ethical Companies.

The story of Arthur J. Gallagher & Co. is more than 90 years in the making, comparable to few and as unique in strengths as it is rich in history. Founded on the cornerstones of integrity, innovation, teamwork and empathy, Gallagher has built its legacy one success at a time. Today, their employees adhere to these same values, weaving them into their daily work.

In the company's own words: As the maritime sector moves towards increasing automation and a convergence of operations and communication technologies with internet-based services and technologies, the sector is experiencing a rapidly increasing, potentially largely uninsured threat as cyber exclusions are placed on most marine policies at renewal in 2018. After serious losses were experienced in 2017 by the property/ marine insurance markets for having provided cover for cyber on a silent basis, the insurance market is starting to specifically exclude these risks to ensure coverage is provided on a specifically named basis. If we look at the financial impact of A. P Moller Maersk having wiped £300M off their profits last year this is a very real threat facing our clients.

We have therefore developed a holistic cyber product which focuses on both risk mitigation, immediate 24/7 real time response and insurance transfer to support and protect our mariners every step of the way. This product has been developed specifically for the Marine industry working with a breadth of marine specialists from cyber security, education and insurance fields.

To find out more see https://www.ajg.com/

COUNTING THE TRUE COST OF HACK ATTACK

NotPetya ransomware victim Maersk has revealed it was forced to replace tens of thousands of servers and computers in the aftermath of the 17 June ransomware attack.

The company's chairman Jim Hagemann Snabe said his company replaced 45,000 PCs, 4,000 servers and installed 2,500 applications.

The massive IT undertaking along with business lost due to the almost total shutdown of the company's computer network has cost Maersk between US$ 250 million (£201 million) and US$ 300 million (£241 million).

The lessons Maersk learned from the event.

- They were "only average" when it comes to cyber-security.
- Cyber security is a competitive advantage
- Being open about the problem helped alleviate some of the issues

MASSIVE SAVINGS AND HUGE BOOST FOR MAJOR PORT

The Port of Rotterdam Authority and IBM have announced a new collaboration on a multi-year digitisation initiative to transform the port's operational environment using Internet of Things (IoT) technologies in the cloud to benefit the port and those who use it.

The initiative will also prepare the Port of Rotterdam's entire 42-kilometre site to host connected ships in the future. It begins with the development of a centralised dashboard application that will collect and process real-time water (hydro), weather (meteo) sensor data and communications data, analysed through the IBM IoT platform. This will enable a new wave of safer and more efficient traffic management at the port.

As the largest port in Europe, the Port of Rotterdam handles over 461 million tonnes of cargo and more than 140,000 vessels annually. Previously the port relied on traditional radio and radar communication between captains, pilots, terminal operators, tugboats and more to make key decisions on port operations.

Now, as the Port of Rotterdam begins its digital transformation, sensors are being installed – spanning from the City of Rotterdam into the North Sea – along the Port's quay walls, mooring posts and roads.

The sensor data will be analysed by IBM's cloud-based technologies and turned into information that the Port of Rotterdam can use to make decisions that reduce wait times, determine optimal times for ships to dock, load and unload, and enable more ships into the available space.

Rotterdam will now be able to predict the best time based on water level, to have a ship arrive and depart Rotterdam, ensuring that the maximum amount of cargo is loaded on board. Meanwhile operators will also be able to view the operations of all the different parties at the same time, making that process more efficient.

It is estimated shipping companies and the Port stand to save up to one hour in berthing time which can amount to about $80,000 US dollars in savings.

SEAWORTHINESS & CYBER SECURITY

Cyber attacks and everyday malware infections are increasingly common, and shipping is being targetted. The Port of Los Angeles recently stated that its Cybersecurity Operations Center has handled an unprecedented 20 million-plus cyber intrusion attempts in 3 years.

Despite such incredible levels of activity, most shipping companies and ports are tight-lipped about data breaches. Attacks have been occurring, but nobody wants to talk, so a lot of people don't believe they are happening.

Ken Munro, an expert on cyber security, claims the maritime domain is lagging behind the likes of the aviation sector. He says the aviation industry has deployed anonymous reporting systems for all kinds of situations, and there is a culture of an incident being viewed as something you can learn from, not something you should hide.

Although many worst-case scenarios at sea – ranging from a hacker taking control of a vessel's navigation systems or causing a ship to spill its oil, explode or sink – have been shown to be theoretically possible, the list of major publicly known cybersecurity incidents is relatively short and not as dramatic.

Over the last few years, cybersecurity specialists have uncovered or demonstrated software vulnerabilities and, just as worrying, human oversights that could allow a cyber intruder to gain access to or control of a variety of ship systems. USB sticks that seafarers still carry and can connect to ship systems are one way malware can make its way to ships and cause trouble, according to Andy Davis, transport assurance practice director at the cybersecurity consulting firm NCC Group .

It is also still uncommon for ship technology manufacturers to offer a straightforward way for outside researchers to flag software vulnerabilities or bugs they find. "The manufacturers – they really haven't woken up to security yet," said Munro.

"It's going to take them several years to get onboard vessel control systems to a point of security where everyone else is already at."

For now, major publicly known targeted attacks have largely involved stealing critical information, not compromising a ship's physical systems. But it can also be hard to tell whether a cyber incident has even occurred.

As a legal matter, it's now even possible that ship owners could potentially be held accountable if a real disaster strikes because of a cyberattack they could have easily prevented. Seaworthiness has long been an issue for shipping, and now cyber weaknesses can undermine not just a ship but the entire shipping business.

RANSOMWARE: THE BIG HITS

Ransomware is difficult to stop even for Windows computers running antivirus, although that situation is improving. The only reliable defence is a backup, but even that can come under attack if it can be reached from the infected PC. These are some of the most influential and destructive examples yet to emerge.

GandCrab: A new strain of ransomware discovered early in January 2018. The malware demands a cryptocurrency fee for the return of any files. More worrying, GandCrab is being marketed as a ransomware-as-a-service package to budding cyber criminals, who could split the profits with the developers 60:40.

GoldenEye: The ransomware attacks reported in Ukraine, which hit the national bank, state power company and Kiev's largest airport on June 27, 2017, was, caused by GoldenEye ransomware, which is thought to be a mixture of Petya and another ransomware, called Mischa. GoldenEye will prevent computer systems from being booted up and from victims retrieving any stored data. When the user reboots, instead of Windows they could see a skull and crossbones splash screen with a ransom demand.

CryptoLocker: Long gone but it deserves infamy because its heyday of 2013 proved to cybercriminals how successful ransomware could be.

Locky: Locky is as bad as ransomware can get. Locky's creators seem to have thought of everything, not only encrypting a wide range of data files but even Bitcoin wallets and Windows Volume Snapshot Service (VSS) files in case users try and restore files using that. Reaches out to attached shares and even other PCs and servers. Uses strong encryption and has found several high-profile victims.

WannaCry: EuroPol has described the WannaCry ransomware, which shut down hospital infrastructure all over the UK and uses a leaked exploit first developed by the National Security Agency, as unprecedented in scale.

zCrypt: zCrypt tries the unusual technique of spreading as a virus. This means that it doesn't rely on malicious emails to find victims and can spread on USB sticks.

Cyber security experts warn that more hits are on their way, and that even more clever and dangerous strains will emerge.

YEARNING FOR PIRATES NOT HACKERS

Writing in the maritime media, Aybars Oruc a shipping executive in the tanker industry has been discussing how shipping must get to grips with cyber attacks.

This is a threat which he believes is so serious, we may even be better off facing Somali pirates with AK47s, rather than hackers with access to shipboard systems.

Despite warnings of major maritime authorities and class institutions such as IMO, BIMCO, ICS, INTERTANKO, most in shipping have been ill prepared for any attack. Oruc, urges us to close our eyes and imagine your ECDIS, GPS, and even AIS devices are hacked. Imagine that your main engine stopped running during navigation in narrow waters.

Oruc says we must open our eyes, because this is all happening in the maritime industry. Main systems that could be affected from a cyber attack:

- Bridge Navigation Systems (GPS, ECDIS, AIS etc.)
- Communication Systems (V-SAT, FBB etc.)
- Mechanical Systems (Main Engine, Auxiliary Engine, Steering Gear etc.)
- Ship Monitoring and Security Systems (CCTV, SSAS, Access Control Systems etc.)
- Cargo Handling Systems (V/V Remote Control Systems, Level/Pressure Monitoring Systems etc.

Although it is impossible to escape the attack, risks can be mitigated. Risks can be minimised by keeping the software updated, using antivirus software, developing redundancy methods, changing default passwords after installing the devices, restricting file sharing, constantly monitoring network configurations (see also Penetration Test), eliminating all problematic areas, and increasing awareness and knowledge level of office staff and ship crew.

To read more of Oruc's thoughts see: https://goo.gl/SJv44X

NO PAINTING OVER CYBER CRACKS

The US Coast Guard is busy updating the service's old IT systems to stay one-step ahead of the latest online threats. Head of the branch's Cyber Command, Rear Adm. Kevin Lunday is tasked with defending the IT networks, telecommunications, and command and control systems for the service's global fleet.

He recently outlined plans for keeping the service safe and stressed the need for agencies to change the way they view security in the years ahead. "If we think about cyberspace as an operational domain ... it means investing in [technology] as a strategic asset," he said. "You can't paint a racing stripe on it ... like we do with our cutters and our aircraft, but it's just as important to getting the mission done as the traditional assets that are very visible."

Since taking the helm of CGCYBER in 2015, Lunday has overseen the service's efforts to build agile IT systems that can be constantly updated against the latest threats.

The Coast Guard is on track to complete the first phase of its IT modernisation plan, which entails updating the hodgepodge of outdated operating systems in the branch's IT infrastructure to Windows 10, by the end of March, he said.

The initiative would not only equip officers with a more secure operating system but has also required upgrading most of the branch's computer hardware and network infrastructure, he said. It also marks a big step toward the Pentagon's proposed Joint Information Environment.

CGCYBER is also responsible for supporting the Coast Guard's recent investments in the biometric and unmanned aircraft technologies that help intercept international traffickers and criminals before they enter the country, he said. But while the agency needs the right tools to accomplish its mission, the "people, not technology, are most important," Lunday said.

DID YOU KNOW?

The "AIDS Trojan", also known as the PC Cyborg virus, was the first ransomware virus documented. It was released via floppy disk in 1989!

Created by biologist Joseph Popp. He handed out 20,000 infected disks to attendees of the World Health Organisation's AIDS conference. The disks were labeled "AIDS Information - Introductory Diskettes".

DO NOT FEED THE PHISH

In new industry guidance, “Phishing Attacks: Defending Your Organisation”, the UK National Cyber Security Centre (NCSC) aims to provide companies with the knowledge and skills to protect themselves, their assets and systems.

Phishing represents a huge threat to everyone’s online security, and the NCSC spends a lot of time combating it in different ways. This guidance is an important addition to a growing portfolio of anti-phishing measures.

This guidance is aimed at organisations of all sizes, in all sectors, it describes how to protect against email phishing threats, drawing on knowledge and research across real working environments.

Phishing Attacks: Defending Your Organisation is not a set of hard rules. It is the starting point to help decide on the right approach. Anti-phishing capabilities depend on many things, and the advice is that even if you can’t implement all of the recommendations, then at least address some of the mitigations from within each of the layers of defence.

The NCSC believes that user training can’t ever entirely solve the phishing problem. In fact, there’s a growing body of evidence to suggest that focusing excessively on users’ role in foiling phishing attacks can cause a great deal of organisational harm.

It opens the door to a ‘blame culture’, and the establishment of punishments and sanctions for users who ‘fail’ at spotting phishes. The truth is that no matter how hard they may try, no users can spot all phishes all of the time. Punishing them doesn’t make them magically able to do so, and it can often cause wider problems.

You can access the NCSC guidance here: https://www.ncsc.gov.uk/phishing

Digital Ship

MARITIME CYBER RESILIENCE FORUM

@APM, 15 MARCH 2018

Digital Ship is excited to return to Singapore, with the next in our series of Cyber Resilience Forums, taking place during APM on 15 March 2018.

Cyber security is high on our agenda with ever-increasing threats being proven to disrupt business continuity. Real life examples in the maritime industry, and related sectors; including ports, terminals and the supply chain, clearly demonstrate the impact of cyber-attacks.

An up-to-date insight into the cyber-threat landscape 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, with developments such as the cloud, IoT, electronic data exchange in the logistic chain, electronic navigation systems, we rely increasingly on technology, which makes cyber resilience business critical. So, how do we embed this into the maritime organisation, and how do we incorporate cyber security 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.

With an amazing line up of speakers, there will be 4 sessions covering key topics:

Session 1: Facing the Cyber Threat: An Overview of Maritime Cyber Challenges and Focus on Building Resilience

Session 2: Business Planning and Cyber Preparedness

Session 3: New Developments in Maritime Cyber Regulations and Guidelines

Session 4: Training, Awareness & Human Factor

For more information on speakers and agenda please see https://www.singapore.thedigitalship.com/ or contact
cathy@thedigitalship.com

DEALING WITH THE CLEAR AND PRESENT CYBER DANGER

"There can be little doubt that cyber threats represent a clear and present danger to the wellbeing of individuals, society and business in our increasingly digitised and connected world", so begins the White Paper on Cyber Security in the Maritime Domain soon to be released by GNS. The subject couldn't be more important for a company whose core business is to help its shipping clients make practical use of the increasing volumes of data and streamline operational processes.

In addition to its origins in navigation products, and with a strong collaborative ethos, GNS works with some of the world's leading marine solutions companies, to deliver a range of services, from voyage optimisation and compliance, such as weather routing and EU MRV reporting, to maritime and cyber security products and services, as well as other critical functions such as cash to Master services.

"With such levels of aggregation and exchange of data, cyber security risk management could not be more important", says Paul Stanley – GNS CEO, "in our latest release of our Voyager HUB, we bring together vast amounts of data to help our client vessels get from berth to berth more efficiently and safely, so it makes absolute sense to support important campaigns such as 'Be Cyber Aware At Sea' as vehicles for educating those who use our systems and data to deliver their cargoes on time and keep their crews safe."

As a responsible supplier in a high technology sector, GNS is committed to playing its part in the fight against cyber-crime, through its contributions to industry forums and stakeholder groups, such as the CIRM Cyber Risk Working Group (CRWG) and takes an active role in thought leadership on the subject.

As the company engages in ever-closer data integration with trusted partners and observes the closing contact of IMO Maritime Cyber Risk Management regulation in January 2021, it believes it has a role to play in helping its clients to understand the threats, manage the risks and avoid the pitfalls of getting cyber security wrong.

In its, soon to be released, White Paper, GNS examines the context of current cyber threats, welcomes the voluminous guidance on cyber security and introduces a simple, memorable framework (The GNS 3i Framework), to put this complex subject into terms all can understand. Identifying human factors (People) as both the greatest asset and greatest liability, the GNS paper stresses the need for awareness, education and training from the Boardroom to the Bridge (and beyond), strongly supporting the Be Cyber Aware at Sea campaign as a critical education tool, as well as the nascent Maritime Cyber Alliance, that focuses on the collective benefits of information sharing to combat current and emerging threats through industry-wide cooperation and collaboration.

To assist its own clients, ashore and afloat, in developing good cyber hygiene, GNS will also soon be offering access to the full range of BCAAS materials as well as the UK MCA-accredited, and GCHQ-assured Maritime Cyber Security Awareness (MCSA) course, directly from the Voyager HUB onboard, making critical education and training more widely available through a partnership with JWC International and Be Cyber Aware at Sea.

Summing up the company's latest contribution to cyber security, Paul Stanley says, "Our paper isn't about adding to the existing body of work in a technical way, there's plenty of that out there already, written by some very smart experts. Instead, like our navigational roots, we hope to help our clients to understand their current position and provide them with a head mark toward their destination."

GNS's Voyager HUB is available as a free download from the GNS web site at www.gnsworldwide.com/Voyager-Hub with applications like the Be Cyber Aware at Sea training and awareness tools available for a small annual subscription.

IMPORTANCE OF AN INCIDENT RESPONSE PLAN

If it hasn't happened to you already... it probably will . One of your computers will be exploited and you now have to try and figure out what systems are involved, how it impacts you, how to recover and if possible how it happened. If the incident involves computers that handle data covered under regulations like the GDPR you may even have to notify people potentially affected by the breach.

When I hear someone exclaim, often proudly, "We've never had a breach!" I have to hold back the big sarcastic grin. What they're really saying is they've never detected a breach, which of course is nothing to brag about given how common it is to have malware on a computer. Malware that is usually under the control of an unknown third party and whose purpose is unknown and certainly malicious. I suppose what they're really saying is they've never had serious consequences from a breach but that's just dumb luck. Not knowing you've been breached is fairly common, in fact most serious breaches still go undetected for months and often aren't noticed until a law enforcement agency determines that a group of victims has one thing in common... your company.

Incidents come in all shapes and sizes. Sometimes you get lucky and things are really easy. For example a user complains their machine is really slow and an investigation reveals the presence of a new service installed that is communicating with a crypto currency mining pool. While your AVS didn't detect it and your firewall didn't block it, the malware is easily removed using a scanning tool you downloaded and the mining pool can be blocked at the Internet border using your firewall. An incident like this is easy because helpdesk and IT can take care of it on their own and the malware's purpose is fairly obvious, steal processing power and mine crypto currency.

Then there is the other end of the spectrum, the malware that's impacting operations but no AVS detects and no scanner removes. The ransomware that comes back as soon as you restore from backup. The malware that reinstalls itself after you completely wipe the system... The stuff of nightmares. This will likely happen to you at some point and you'd be well advised to have a good plan. IT and/or helpdesk probably aren't going to be able to handle this one on their own and unless you're a big enough company to have a dedicated incident response team you're going to need outside help. Depending on the incident you'll likely need access to subject matter experts in network forensics, malware binary analysis, data forensics and cyber crime. All highly specialized skills that most companies don't have on staff. Knowing what needs to happen and who will do what will save precious hours and quicken the remediation process.

By forming relationships in advance with the partners and vendors who will assist you with a serious incident and creating a comprehensive incident response plan you can significantly reduce both operational impact and costs. Having the plans and relationships already in place allows you the opportunity to conduct exercises and simulations to practice your incident response plan. This way you're not learning or suffering setbacks from unanticipated circumstances during an actual incident response.

If you wait until the incident occurs you may find yourself calling around trying to find someone to help you. When you do find someone who can help you may find yourself rushing through paperwork like non-disclosure agreements, statements of work and purchase orders. Also you may be in a position of desperation and perhaps pay more than you would if you had time to properly negotiate a contract.

Incident response is a team activity and a team skill. Like any skill it benefits from practice. Forming your team and practicing for the bad day can make all the difference in how you come away from it. While an incident may be inevitable an operational nightmare, with a bit of planning, need not be.

EPSCO-Ra

NEW CYBER SHIP

COSCO Shipping Aries is the first ever container ship to receive Lloyd's Register's (LR) cyber-enabled ship descriptive note Cyber AL3 Secure Perform for its energy management system.

The 20,000 TEU ship was built by Nantong COSCO KHI Ship Engineering Co.

The ship complies with the revised version of LR's cyber-enabled ships (CES) ShipRight procedure, issued in December 2017. AL3 is defined by LR as "cyber access for autonomous/ remote monitoring and control (onboard permission is required, and onboard override is possible)".

TOP 6 MUST DO CYBER TIPS

1. Create strong passwords
2. Secure mobile devices
3. Protect your data
4. Use secure wireless networks
5. Install latest updates
6. Use security software

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.

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.

BE CYBER AWARE AT SEA

www.becyberawareatsea.com

think@becyberawareatsea.com

With thanks to our many industry supporters....

ROYAL NAVY · navarino · NORTH SERVICE. STRENGTH. QUALITY · Standard Club · STEAMSHIP MUTUAL · SHIPOWNERS

TK · P&O FERRIES · inmarsat The mobile satellite company · JWC INTERNATIONAL · CSO ALLIANCE MARITIME · NORWEGIAN HULL CLUB

ANGLE YACHTS · CITADEL MARITIME · HFW · Maritime Security Review · V.Group · fidra films

UNITY FOR SAFETY AT SEA IFSMA · ASKET Ltd The Worlds Trusted Maritime Security Broker · SISS SAFETIC INTERNATIONAL SAFETY & SECURITY · APMG International Accrediting Professionals · British Ports Association · ZEUS

HB · GCHQ Certified Training · integro · GOLDPHISH CYBER RISK MANAGEMENT · ARX MARITIME · Owidiqi

Gnostech Inc. · AXIS · SHCL SHIPPINGCLUSTER · SECURE A SHIP · OSP SECURITY PROFESSIONALS · OSP SAFETY PROFESSIONALS

Digital Ship MARITIME CYBER RESILIENCE FORUM · ENDEAVOUR MARITIME · Blaythorne Equipped for Life · SovereignGlobal UK · SAFETY4SEA · UpGuard

ARB INTERNATIONAL · NSSLGlobal ON LAND • ONBOARD • ONLINE · GTMARITIME · INCE & CO · seafarers UK 100 · The Nautical Institute

eeSea · THAMES ESTUARY PARTNERSHIP · MARITIME TRUST PLATFORM · FR FRONTIER RISKS · Maritime Cyprus International News Forum · www.SaveOurSeafarers.com

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

ALUMNI SECURITY RISK MANAGEMENT · Junge · Arcanum CYBER SECURITY · POLYVERSE · TURREM DATA Group · Zephyr RCCU South West Regional Cyber Crime Unit

IMS SECURITY AT SEA · CYBERimpact · SOVREN · SEA & SHORE SAFETY · GLOBAL NAVIGATION SOLUTIONS · ELEKTRONIK LAB INDIA (PVT) LTD. SKY IS NOT THE LIMIT

cyberprism · e-worthy · abto ASSOCIATION OF BULK TERMINAL OPERATORS · PORT SECURITY CENTER KEEPING OUR MARITIME WORLD SECURE · www.tototheo.com Communication • Navigation • Surveillance · ICHCA INTERNATIONAL

GASLOG · Intership · smartmaritime · ICSPA International Cyber Security Protection Alliance · AST · BIBBY OFFSHORE because we love this business

ESCO-RA Maritime Cyber Security Solutions · Propulsion Analytics · SENTINELMARINE · EOS RISK GROUP Advise Protect Assist · MF Shipping Group · REGIONAL MARITIME INFORMATION SHARING CENTRE

ROXANA SHIPPING S.A. · Outstanding Security Performance Awards · Fairplay Insights from IHS Markit · sirm · Safety at Sea Insights from IHS Markit · THOMAS MILLER SPECIALTY

CA.FI.MA. · KOTUG · BLUE BORDER · ISMS.online · CR nordic · VIBE Cyber

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.