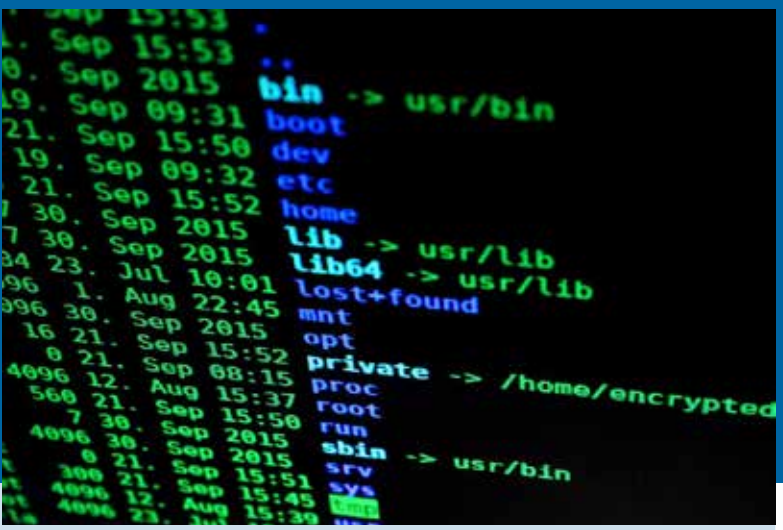
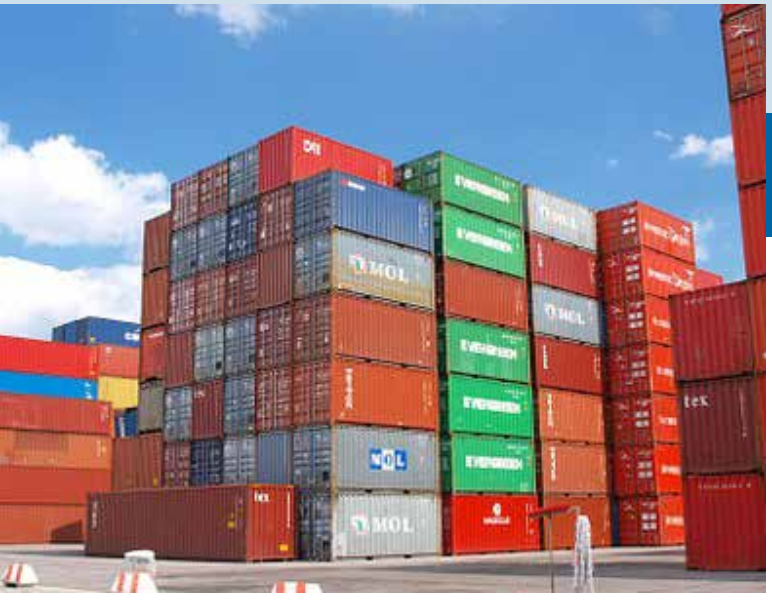


#19

JUNE: 2018

PHISH & SHIPS

BE CYBER AWARE AT SEA



Kindly sponsored by

TDG Cyber Marine

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".

Issue 19 is generously sponsored by Turrem Data Group Limited (TDG), an emerging 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. TDG works to cut through the Cyber Solutions noise to provide simple, effective and fully managed services backed up by highly experienced personnel trained in the latest cyberthreat landscape. See https://www.turremgroup.com/ for more details.

This time around we bring the latest news about maritime cyber security, and the implications of new guidelines, and we assess some of the latest cyber weaknesses which have been identified.

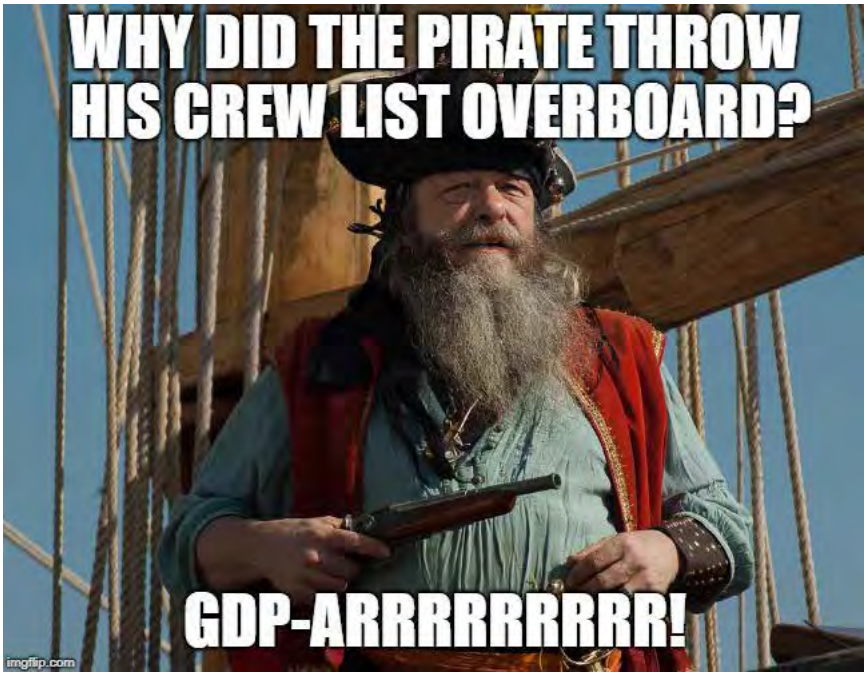
Also in this latest issue, we look at the thoughts of some key industry leaders, and gain an insight into their view of the passage ahead for shipping, as it wrestles to deal with cyber security.

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.

TURREM DATA Group

GDPR IS NO LAUGHING MATTER

Humour (or attempted humour), is often a crutch to support us in difficult times. So, as the new General Data Protection Regulations (GDPR) have arrived they have done so with a flurry of jokes and a million memes.



Our own personal favourite? Well, anything that combines pirate jokes and data protection is always going to attract the Be Cyber Aware at Sea campaign. So, yes GDP Arrrrrr...does raise a smile in the office.

Another favourite - Q: Do you know a good GDPR Consultant? A: Yes Q: Can you give me their email address? A: No!

GDPR is of course no laughing matter. The premise behind it is to protect the data of European citizens, and to close the net on those who run fast and loose with increasingly valuable pieces of information.

Companies have been left to try and find their path through - you will no doubt have been inundated with the last minute rush of emails. "Please don't leave us", and the like. Alas, the irony is that most of the companies that care enough to want you to stick around were probably not the problem in the first place. Indeed the scammers and spammers have been having a field day thanks to all this. People have been opting in to be scammed out of money!

Now though, we are in the new GDPR age - the calendar has been reset, and we are supposedly at the Year Zero for data. Will you be better protected? Possibly. Will you still receive annoying emails from who knows what, from who knows where? Undoubtedly. So, it seems that time will tell as to how effective the regulations can and will be. We are just glad you wanted to stick around.

CYBER STAKES ARE BEING RAISED

According to new research and news emerging from Nigeria, local cybercrooks in the country last year attempted to steal $3.9 million in the maritime sector.

The President of the Cyber Security Experts Association of Nigeria (CSEAN), Remi Afon, lamented that about 85 per cent of corporate organisations in the country lack cybersecurity plans and strategy, thus vulnerable to cyber attacks.

Afon stated, “Global cybercrime damages, which were about $3 trillion in 2015, will reach about $6 trillion by the end of 2021, a 100 per cent increase in just five years according to Cybersecurity Ventures. Unfortunately, over 85 per cent of organisations and government agencies in Nigeria lack cybersecurity plan and strategy while majority are unsure whether or not they’ve been a victim of cybercrime.”

However, he stated that some of the cyber threats were being evaded through increased cybersecurity campaigns while others were under-reported. He disclosed plans to further sensitise the public in its fourth cyber security conference, tagged ‘‘Mitigating Cyber Threats in the Digital Age’’ scheduled to be held in Lagos.

NO OPT OUT OF SECURITY WOES

Edwin Lampert of Riviera Maritime is a man who has his finger on the pulse of shipping, He is often ahead of the curve when it comes to the problems facing the industry - and of course about the solutions needed too. In a recent article he has been reminding us just how far shipping has come, and indeed how far it still has to go when it comes to cyber security.

According to Lampert, “Just three short years ago the cyber security threat in the maritime industry was largely dismissed.” He adds, “We have since seen a seismic shift in attitudes which has been precipitated by a mix of high profile incidents and regulation. IMO requires that shipowners and managers incorporate cyber risks into their shipmanagement systems by 2021, and since the beginning of this year OCIMF’s SIRE programme has required tanker owners to address cyber security risks in their policies and procedures. Class societies have not been slow on the uptake either and are now issuing cyber safety notations.”

The threat is incredibly serious. Even radar is vulnerable, and no bridge system is safe from hackers! This has seen Lampert stress the need for industry education and knowledge sharing.

Shipping can no longer delude itself that the cyber threat is something it can opt out of. You can learn more at this line of thinking at https://bit.ly/2LFBD7M

IMO WILL STILL RULE WAVES

NEW LEGISLATION WILL NOT BE A SHOREBASED POWER GRAB

According to Norton Rose Fulbright partner Philip Roche, the EU's new NIS Cyber Security Directive should not directly affect shipowners.

Roche believes that cyber security rules for shipping will continue to be the domain of IMO policy and flag State regulations, he said.

However, the EU's NIS Directive, which came into effect this month, will seemingly tighten cyber security at ports including interactions between freight handling companies and ports.

This in turn will likely see an increase in the use of blockchain-type technologies as companies look to secure their interactions.

Looking ahead to the high profile European Maritime Cyber Risk Management Summit in London on June 18th 2018, Roche stated that the shipping industry's growing reliance on technology brings an amplified potential for cyber attack.

"That increasing reliance on IT is going to mean an increasingly big risk," said Roche. "So the appropriate and proportionate (security) measures ... it is hard to imagine (security measures) being out of proportion. You almost cannot take enough precautions," he added.

According to Roche, faced with these threats ports will in turn be required to tighten cyber security protocols with the freight handling companies who operate there.

"Where there is going to be a lot closer interface is with the ... trucking companies, with freight forwarders and with logistics companies who basically do their business out of the port," Mr Roche said.

Roche said ports that do not handle the inevitable technological changes well may face a loss of customers.

"In most places, people have an option as to which port to go to. And, so if you have ports which are ... constantly going down because of cyber issues and are not taking the necessary precautions of keeping the port efficient and running, then people are going to go elsewhere".

Apart from any inconveniences with ports who handle the change badly, the impacts of the NIS Directive are currently minimal for shipowners.

"I think shipowners will remain an island unto themselves. So long as they have taken the necessary precautions as set down by the IMO and flag states, they will come and go reasonably as they [have in the past]".

However, Roche could foresee a time when a leaner and more competitive industry would push cyber requirements onto shipping. If not now, the seamless logistics supply chain will eventually materialise, he said. Adding, "Eventually, I think they will all be connected together".

While the entry of a major player from the tech industry is one force that could, eventually, propel the industry towards this more seamless, integrated model.

"In a way, what is going to change the shipping industry is not the shipping industry. It is going to be the disruptive technologies coming in, the Amazons and Googles wanting to have these basically seamless transport networks with smaller ships," explained Roche.

However, Mr Roche said he was less than certain that a market entry from those tech sector giants would have as much of an impact as shipowners and operators may fear.

"It seems to me you still need to have big, heavy, metal ships on the water," he said. "And, of course, tech (the industry) does not seem to like heavy industry (as an investment). You have seen tech struggle to replace cars (with driverless automobiles), let alone running (autonomous) ships."

To find out more about the conference see http://www.shipcybersecurity.com/programme.htm

SEVEN

STEPS OF A CYBER ATTACK...

Craig Reeds, CISSP, Cyber Security Senior Consultant at DNV GL - Digital Solutions, has spotted a change in the way that hacks are being performed. Recent attacks reveal new motives and methods. The attackers were not out to steal data but were looking to disrupt services. Here are the new Seven Steps of a Cyber Attack:

STEP ONE - RECONNAISSANCE: Before launching an attack, hackers first identify a vulnerable target and explore the best ways to exploit it. The initial target can be anyone in an organization. The attackers simply need a single point of entrance to get started. Targeted phishing emails are common in this step, as an effective method of distributing malware.

The whole point of this phase is getting to know the target. The questions that the attackers are seeking answers to are:

- **Who are the important people in the company?** This can be answered by looking at the company web site or LinkedIn.
- **Who do they do business with?** For this they may be able to use social engineering, by make a few "sales calls" to the company. The other way is good old-fashioned dumpster diving.
- **What public data is available about the company?** Hackers collect IP address information and run scans to determine what hardware and software they are using. They check the ICAAN web registry database.

The more time hackers spend gaining information about the people and systems at the company, the more successful the hacking attempt will be.

STEP TWO - WEAPONISATION: In this phase, the hacker uses the information that they gathered in the previous phase to create the things they will need to get into the network. This could be creating believable Spear Phishing e-mails. These would look like e-mails that they could potentially receive from a known vendor or other business contact.

The next is creating Watering Holes, or fake web pages. These web pages will look identical to a vendor's web page or even a bank's web page. But the sole purpose is to capture your user name and password, or to offer you a free download of a document or something else of interest.

The final thing the attacker will do in this stage is to collect the tools that they plan to use once they gain access to the network so that they can successfully exploit any vulnerabilities that they find.

STEP THREE - DELIVERY: Now the attack starts. Phishing e-mails are sent, Watering Hole web pages are posted to the Internet and the attacker waits for all the data they need to start rolling in. If the Phishing e-mail contains a weaponized attachment, then the attacker waits for someone to open the attachment and for the malware to call home.

STEP FOUR - EXPLOITATION: Now the "fun" begins for the hacker. As user names and passwords arrive, the hacker tries them against web-based e-mail systems or VPN connections to the company network. If malware-laced attachments were sent, then the attacker remotely accesses the infected computers. The attacker explores the network and gains a better idea of the traffic flow on the network, what systems are connected to the network and how they can be exploited.

STEP FIVE - INSTALLATION: In this phase the attacker makes sure that they continue to have access to the network. They will install a persistent backdoor, create Admin accounts on the network, disable firewall rules and perhaps even activate remote desktop access on servers and other systems on the network. The intent at this point is to make sure that the attacker can stay in the system as long as they need to.

STEP SIX – COMMAND AND CONTROL: Now they have access to the network, administrator accounts, all the needed tools are in place. They now have unfettered access to the entire network. They can look at anything, impersonate any user on the network, and even send e-mails from the CEO to all employees. At this point they are in control. They can lock you out of your entire network if they want to.

STEP SEVEN – ACTION ON OBJECTIVE: Now that they have total control, they can achieve their objectives. This could be stealing information on employees, customers, product designs, etc. or they can start messing with the operations of the company. Remember, not all hackers are after monetizable data, some are out to just mess things up. If you take online orders, they could shut down your order-taking system or delete orders from the system. They could even create orders and have them shipped to your customers.

If you have an Industrial Control System and they gain access to it, they could shut down equipment, enter new set points, and disable alarms. Not all hackers want to steal your money, sell your information or post your incriminating e-mails on WikiLeaks, some hackers just want to cause you pain.

So, what now? Prepare for the attack: What can you do to protect your network, your company, even your reputation? You need to prepare for the attack. Let's face it, sooner or later the hackers WILL come for you. Don't let yourself think that you don't have anything that they want. You do!

See www.dnvgl.com for more details.

A-Z OF CYBER SECURITY

K L M N O

K is for keystroke. This is the act of tapping a key when typing. Some malicious programs or devices log keystrokes to obtain passwords or other confidential info.

L is for least privilege. The principle of least privilege is an important part of maintaining cyber security by granting access to information and functions on a strictly 'need to know' basis within a particular network.

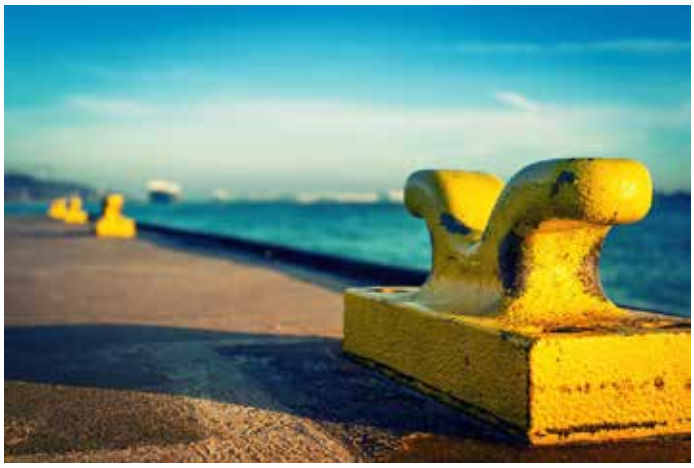
M is for malicious software, commonly known as malware, which is a type of program designed to infect and damage computers.

N is for network. This is a group of linked computers and/or other IT systems and devices that are able to communicate with each other and share resources. Once one of these systems is successfully hacked the rest of the network can be compromised.

O is for outsourcing. This is the process of using an outside third-party to provide certain services for your company, which can increase the level of risk for your business. Cyber security solutions are also often outsourced to specialist contractors.

source: medium.com

PORTS AND CLIENTS FACING NEW CYBER SEASCAPE



HFW's Matthew Gore recently wrote on the implications of the Directive on Security of Network and Information Systems (EU 2016/1148) (the Cyber Directive), which was transposed into UK law on May 9, 2018.

This brings cyber security onto a legislative footing. It applies to organisations termed as 'Operators of Essential Services' (OES) and requires such organisations to demonstrate that they have implemented 'appropriate and proportionate' cyber security measures to prevent, or at least alleviate, the potential harm of cyber security incidents.

According to the UK Government, OES status within the maritime transport sector will apply to harbour authorities, ports or port operators that either have annual passenger numbers greater than 10m or that account for more than 15% of the UK's ro-ro traffic, 15% of the UK's lo-lo traffic, 10% of UK total liquid bulk; or 20% of UK total bio-mass fuel.

The Cyber Directive will also impact sea freight carriers that handle more than 30% of freight at any UK port that falls within the parameters above, and 5m tonnes of total annual freight in UK ports as a whole.

OES within the maritime transport sector will be required to comply with a set of fourteen security requirements based on the following four objectives as defined by the National Cyber Security Centre:

- Managing security risk
- Protecting against cyber attack
- Detecting cyber security events
- Minimising the impact of cyber security incidents

Once the Cyber Directive is effective, the Secretary of State for Transport, and by extension the Department for Transport will have the responsibilities of the Competent Authority in this domain, and their duties will include the designation of OES; monitoring the application of the Cyber Directive; the publication of guidance (including incident reporting thresholds); and enforcement and the imposition of penalties. The Competent Authority will have the right to impose financial penalties (up to a maximum of £17m) on OES which contravene the Cyber Directive.

CRUISE PASSENGER DATA AT RISK

Rising passenger numbers on cruise ships have resulted in the introduction of new technologies and the internet of things (IOT) in order to make the journey more engaging and personalised.

What is great for passengers is the fact that new technology means that every facet of the ship is digital, from the dinner reservations to locating people on the ship. However, there is a flip side, and with thousands of people's information available cruise line digitisation makes them a target for hackers.

As we have stressed since the very first issue, and lest we forget the name of this magazine, email phishing can be used to implant a virus on to a ship just as easily as one of the thousands of passengers on board opening an email or uploading a USB drive that is infected to provide an attacker access to the internal systems.

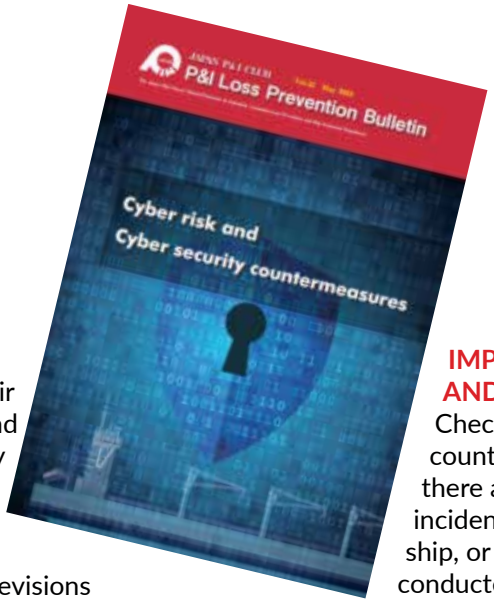
Cruise liners are reliant on the interconnectivity of IT systems and operational technology to create a digital environment to manage the successful delivery of a holiday to every passenger. Which means the cruise industry is far more likely to have the data of its passengers taken advantage of.

According to a new report by Ian Richardson CEO and Co-Founder of TheICEway and Patrick Carolan Technical Director for CRIBB Cyber Security, if a passenger's data such as a bank card or personal information has been uploaded onto the online shipboard systems, (which would be used to make their stay more personalised and automated) then their details can be infiltrated and they could become the victim of fraud.

Cruises are increasingly popular, but this will quickly diminish if passengers feel unsafe. It is apparent that the time to define a clear and secure strategy relating to cyber security is paramount to maintaining confidence in the cruise industry from its customers.

With the developments of cruise ships as "floating digital worlds" of their own, it is crucial for the safety and integrity of the industry and it passengers that cruise lines start recognising and understanding the increasing threats and what the outcomes could be.

JAPAN CLUB ISSUES CYBER GUIDANCE



The Japan P&I Club has released new guidance to its members on ship communications devices, their connected onboard PCs, navigation electronics and propulsion equipment are crucial to cyber security countermeasures.

The guidance concerns with setting out a specific approach to the examination of risk assessment, revisions to the SMS or SSP. Actions such as the use of illegally copied software and illegally downloaded sites are some of the factors which may make a system easy to infect.

To prevent cyber security problems, the Japan Club describes a set of actions that can provide a solution:

IDENTIFY IT SYSTEMS: In order to list them up.

IMPLEMENT RISK ASSESSMENT: Risk assessment is to be implemented by examining the possible outcomes of a cyber attack, frequency and current management method.

ESTABLISH NECESSARY COUNTERMEASURES: As a result of risk assessment, countermeasures are to be planned, implemented and operated.

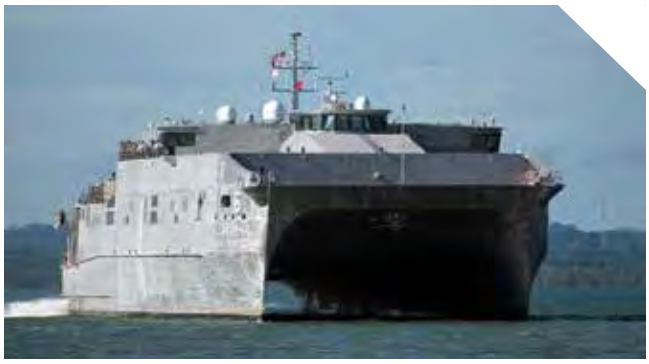
IMPLEMENT, OPERATE AND MANAGE INCIDENTS: Check the status of additional countermeasures and verify that there are no flaws using reports of incidents and near misses from the ship, or an ISM/ISPS internal audit conducted by a superintendent.

INCIDENT STATISTICAL ANALYSIS: Companies have to conduct statistical analysis based on the reports of incidents and near misses from the ship, and the results reported from the ISM/ISPS internal audit.

REVIEW AND IMPROVE: After a statistical analysis, a review is needed as to whether the additional countermeasures are working, and if the countermeasures are not enough or if a new risk was reported, the risk assessment has to be implemented again.

Access the Japan Club guidance: https://bit.ly/2LJ1MT7

US NAVAL VESSELS CYBER PROBLEMS



An entire class of US Navy ships designed to quickly move troops and equipment around the world has major problems that could prevent them from accomplishing that mission. That's the conclusion of a new report from the US Defense Department Inspector General.

The report finds that the class of aluminium catamaran-style ships 'lacks capability', of which one of the key ones is securing control systems aboard the vessels.

"Cybersecurity vulnerabilities could potentially lead to hackers disabling or taking control of systems, preventing the EFP vessel from accomplishing its missions," the report stated.

According to the Inspector General, information assurance control deficiencies have been corrected by the MSC (Military Sealift Command) which is responsible for the operation and sustainment of the EPF vessels.

Across the Navy, network and information security continues to emerge in importance, with top officials emphasizing the need to secure onboard systems in particular. This was underscored in the Navy's investigations into the 2017 collisions of the USS John McCain and the USS Fitzgerald in which teams from Space and Naval Warfare Systems Command and Fleet Cyber Command/Tenth Fleet were brought in. Rear Admiral Christian Becker, SPAWAR commander, commented that the fact they were brought in was "an indicator of the new reality of today, where our systems across the board are reliant on the network".

According to Becker, cyber resilience in the fleet "starts with designing in that resiliency from the beginning, implementing IT standards, and making sure that when we deliver the capability for which we're responsible, those capabilities are up-to-date, integrated properly, secure and ready for sailors to operate and maintain."

DON'T LET MARITIME BECOME ANOTHER EXAMPLE OF GDPR AND HOW NOT TO DO BUSINESS

By Steve Tytler, Founder and Business Development Director

Turrem Data Group have 30 years of combined expertise and skill sets within the cyber security area. They provide leading patented technology to ensure more robust defence against cybercriminal activity.

Back in January 2016 I watched a talk by General Zukunft of the USCG discussing cyber security in the ports of the USA. In this speech he explained how cyber hygienic the oldest armed force of the USA was but asked the question: 'How clean are the vessels coming into our waters?'

The USA, as any good maritime company knows, has over 360 ports putting trillions of dollars' worth of trade through them. This prompts the question – what would happen if a vessel were to be taken over remotely and steered into one of these ports? It would lead to what we know as 'supply chain disruption' and the consequent massive butterfly effect rippling through the system would stop your company ever being used again…

Fast forward to today and the maritime market is getting better with its security and education through excellent schemes such as 'Be Cyber Aware at Sea'. However, last year's Maersk attack did not have the desired outcome that should have seen all shipping companies upping their game. The message is sound but uptake is slow.

GDPR AND LESSONS TO BE LEARNT

Years ago, when Turrem Group was founded, we knew of the long overdue tabled draft law called GDPR. We educated the best we could with the limited and somewhat confusing information we had but the uptake by enterprise was slow and the SMB market was non-existent. Then, last week as the deadline of the 25th of May hit, all of us received emails to ask for consent to stay in contact. So, why is this relevant to a maritime company you may ask?

In June 2017 the IMO took a much-needed stance and put a date of 2021 for maritime organisations to put in place a cyber risk management strategy that could be inspected. These baby steps are essential but like GDPR, the essential tasks to meet the deadline may be left till the last minute. Again, remember all those consent emails in May?

What the maritime sector and the IMO must learn is that while new regulations are essential in a connected world, they are a business hindrance as we are all so busy. This is especially the case in the maritime sector that has several factors to consider – OT, IT, human systems, networks, software, ongoing operations.

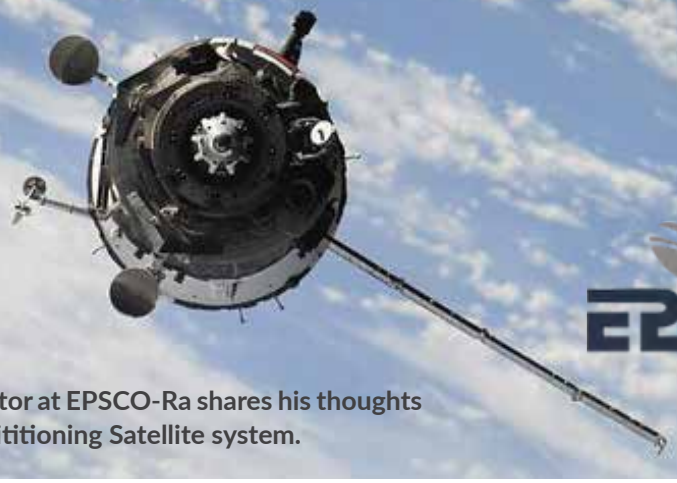
GDPR for land-based organisations has been badly handled by the ICO and after the 25th May deadline many 'experts' have now left, just like the short-term expertise generated by the millennium bug. A structured approach is now needed for cyber security for both landlocked and at sea systems with several steps to compliancy, and there is a reason behind this.

GDPR will force both supply chains of enterprise and the 'down-the-line' business food chain to make themselves more cyber hygienic, and to prove it standards such as the UK's Cyber Essentials and ISO 27001 will need to be in place. This of course will include maritime shipping as it delivers 90% of global trade. These landlocked clients are, put simply, your customers.

Cyber security therefore will become part of the norm for any company in the future to prove this point. The deadline of 2021 may be a target, but Turrem Data Group have a feeling the maritime supply chain will have to move quicker to satisfy land-based customers.

So, like any good Sea Scout – Be Prepared – as you may be asked to work harder for the business a lot sooner than you think, making the 2021 deadline an irrelevance.

HOW VULNERABLE IS GPS NAVIGATION?



Gideon Lenkey, Technology Director at EPSCO-Ra shares his thoughts on the security of the Global Posititioning Satellite system.

Far from its roots in military applications, GPS has become something most people use in one way or another almost every day. Your smartphone has a receiver built in and if you have a late model car it will come equipped with a GPS navigation system. In addition to a personal convenience however, GPS is also a critical navigation aid to the entire transportation industry.

GPS is so important that it could be argued it is an essential 'utility' that is part of a global critical infrastructure. So just how vulnerable is the maritime industry to attacks on GPS?

GPS works on a relatively weak signal across very great distances, about 20 watts at a distance of 22,000 miles. This means it doesn't take much to overpower it. Theoretically, a slightly elevated 1 watt terrestrial transmitter could easily overpower the satellite signal for miles. An attacker wouldn't even have to be very knowledgeable to do this either.

For about $600 USD a would-be attacker can purchase a portable jamming device about the size of a hand-held radio that will jam multiple satellite navigation frequencies in a 100 meter radius. That means if a crewman brought one on board it could potentially disable GPS navigation and it would be very difficult to detect the source.

Now a GPS attack might seem unlikely or far fetched but it actually happens quite frequently and sometimes for questionable yet understandable reasons. According to Spirent, a company that specializes in GPS related attack countermeasures, there are over 150,000 reported incidents of GPS attacks. Typically, attacks fall into two categories, jamming and spoofing. Jamming is fairly easy to detect (signal lost) and is really just overpowering the satellite signal with noise on the same frequencies so that the GPS receiver doesn't function.

GPS is sometimes jammed by privacy seeking individuals to avoid being tracked, criminals to avoid warrantless tracking devices or even by car thieves to defeat GPS equipped anti-theft devices.

Spoofing on the other hand is a far more serious concern. When GPS signals are spoofed the receiver doesn't indicate an alarm but reports a false position. A GPS spoofing attack involves manipulating the signal in such a way so that the receiver indicates the position the attacker wishes it to. This is obviously much more sophisticated than a jamming attack and is likely out of reach for your average car thief or criminal, at least for now. Confirmed spoofing attacks to date have largely indicated nation state actors and the spoofed positions hint at the reasons behind them.

In the vast majority of reported cases in Maritime, the spoofed position has been an airport. This is significant as it makes the spoofing attack immediately obvious. It also makes perfect sense as it could interfere with both military equipment and commercial autonomous vehicles that honour geofencing protocols.

Geofencing is the practice of delineating areas where autonomous or semi-autonomous vehicles like drones aren't supposed to go. In fact some commercial drones won't even take off if they sense they're within a no-fly area like an airport. This speaks to the defense aspect of GPS jamming and adds weight to the nation state actor suspicions, as these attacks affect very large areas in some cases.

Military forces around the globe are well aware of the battlefield implications of their reliance on satellite positioning systems. As nations continue to develop both offensive jamming and spoofing weapons, as well as defensive countermeasures, the commercial sector simply becomes increasingly vulnerable.

As with all technology, spoofing – like jamming – will move downsteam and become more available to non-military users over time. In the wrong hands this technology could allow an attacker to manipulate a vessel's position for a variety of reasons potentially putting lives at risk. It's a frightening thought.

Until more resilient satellite navigation receivers are more widely available, Maritime operators are well advised to develop procedures to crosscheck GPS navigation in areas where GPS interference has been reported and to practice navigation methods without GPS during periods of outage.

TDG
Cyber Marine

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 accesible team acting as a virtual extension of your in-house resources.
- Improving the effectivenes 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 there 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.

A member of Turrem Data Group Limited.
a : Watchoak Business Centre, 5 Chain Lane, Battle, East Sussex TN33 0GB.
t : 0330 043 1723 e : contact@turremgroup.com w : www.turremgroup.com