#20
JULY: 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 20 is once again generously sponsored by Turrem Data Group Limited (TDG), an expert player in the cybersecurity industry. The company offers leading edge and patented technologies to provide a more robust defence against the escalating threat from cybercriminal activity. See https://www.turremgroup.com/ for more details.

This time around we bring you more news as Classification Societies begin to align themselves on the cyber security issue. We also look at the impact on port state control inspections, and examine the real vulnerabilities in onboard systems. We also follow up on the words of security experts when it comes to seafarers and the need for them to be better trained, while looking at the steps that satellite communications providers are taking to ensure their users are kept secure.

Recent years have shown rapid growth in the reach and complexity of cyber-attacks in the maritime industry. Cyber security has become a concern. It should be considered as an integral part of overall safety management in shipping and offshore operations. We are pleased to announce that Jordan Wylie from Be Cyber Aware at Sea will be bringing his thoughts about the sector and the campaign to an event hosted by TDG Cyber Marine. This will also see CTO Mark Mottershead demonstrate some of the solutions available for the maritime industry, which will be followed by an interactive Q&A Session. To reserve your place and for more details see: https://bit.ly/2MIE89c

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

CYBER CLASSIFICATION RACE

DNV GL has released its new Class notations to help shipowners and operators protect their assets from cyber security incidents. The new class notations – "Cyber secure" – help owners and operators protect vital systems from cyber security threats and were formally published on the DNV GL rules page on July 1, 2018.

The Cyber secure class notations have three different qualifiers:

- **Basic**
- **Advanced**
- **Plus (+)**

Basic is primarily intended for ships in operation, while Advanced has been designed to be applied throughout the newbuilding process, with requirements for asset owners and operators, system integrators such as shipyards for example, and equipment manufacturers.

The Basic and Advanced qualifiers cover a number of essential systems, including propulsion, steering, navigation, and power generation. The third qualifier, Plus (+), is intended for systems that are not part of the default scope of Basic/ Advanced. This gives owners and operators the flexibility to identify the threats, assess, and secure extra systems which are of particular importance to their operations.

The Cyber secure class notations mean the security of shipboard systems can be assessed through an independent verification process. See full details at https://bit.ly/2KqndL1

Elsewhere, the American Bureau of Shipping (ABS) has announced the successful development of a ground-breaking new methodology to measure cyber-security risk associated with operational technology.

The methodology will provide a calculated risk index for vessels, fleets, and facilities — quantifying cyber-security risk and delivering actionable strategy to owners and operators.

ABS Chairman, President, and CEO, Christopher J. Wiernicki, said: "The ABS FCI Cyber Risk™ model gives owners and operators a straightforward approach to understanding their existing cyber risk and a concrete approach to reducing that risk."

The Functions, Connections, and Identities (FCI) model can calculate a cyber risk index for individual assets or entire fleets, allowing owners and operators to target cyber-security investments to focus on.

The quantifiable and calculable method evaluates not only the operational systems and connections of a vessel, but also the human and machine identities, clearly enumerating the level of cyber risk exposure. See https://bit.ly/2KnYsiF

SHIPS IN DIRE CYBER STRAITS

"Security on board ships is often dire" – that is the view of ethical hackers who have once again demonstrated how attacks on vessel systems can cause all kinds of chaos and problems for safe navigation.

Ken Munro of Pen Test Partners, chose the recent Infosecurity Europe exhibition in London as the place to highlight results of tests they have conducted, and hacks which have occurred, to show where the weaknesses and problems lie. Munro showed that it is possible to take advantage of weaknesses in cyber security to reconfigure a ship's ECDIS software in order to mis-identify the location of its GPS receiver.

The receiver's location can be moved by only about 300m (984ft), but that is enough to force an accident. In poor visibility Munro states that can be the difference between crashing and not crashing. He added that it is also possible to make the software identify the vessel as being much bigger than its true size - up to 1km sq.

In recognising that there are real problems, experts commenting in the press said they felt rather than pursuing expensive technical solutions, that the focus should be on addressing seafarer training. Ship officers must be instructed to lock down their equipment with strong passwords and ensure the latest software patches are installed.

VULNERABILITIES CLEAR TO SEE

There were numerous demonstrations of the problems surrounding maritime cyber security at the recent Infosecurity Europe exhibition held in London.

Weak default passwords, failure to apply software updates, and a lack of encryption – all suggest "crappy IoT kit" to the security experts. These enable a variety of attacks against vessels and related operations. Network segregation on ships is also rare, which means anyone able to hack the satcom terminal gains access to the vessel network.

The issue of crew training was discussed at the event, and also the culture of some less experienced officers at sea. Cyber experts warned that, "younger crews get 'screen fixated' all too often, believing the electronic screens instead of looking out of the window."

This is a major concern, and it needs good training and crew resource management to ensure watchkeepers are acting as the guardian of navigation, rather than being passive observers to what may well be erroneous data.

They also highlighted a different technique which can exploit Operation Technology (OT) systems on ships, which control the steering gear, engines, ballast pumps and more.

These systems communicate using the NMEA 0183 specification, and the messages are in plain text – no authentication, encryption or validation. "All we need to do is "man in the middle" and modify the data," one expert warned.

"This isn't GPS spoofing, which is well known and easy to detect, this is injecting small errors to slowly and insidiously force a ship off course." PTP's demo showed that an attacker could change the rudder command by modifying a GPS autopilot command. Truly terrifying stuff.

Vessel owners and operators need to address these issues quickly, or more shipping security incidents will occur, the researchers concluded.

INDUSTRY WORKING GROUPS

CLASS SOCIETIES WORKING ON SOLUTIONS WITH SHIPPING

The Posidonia exhibition in Athens is one of the most important in the shipping calendar. Often this is the bellwether of change, and it was interesting to note that maritime cyber security was very much to the fore at the event held in June.

One of the most important and significant discussions was that of the International Association of Classification Societies (IACS). In an industry undergoing rapid change, the outgoing IACS Chairman Knut Ørbeck-Nilssen identified the need for classification societies and IACS itself to be adaptable and prepared for change, while staying true to the core purpose of classification.

Mr Ørbeck-Nilssen said that over the past year great progress had been made in modernising classification to deal with the digital transformation of shipping: "I'm pleased to see the progress that was made in modernising the concept of class, to adapt to the digital transformation we see in shipping today. I say transformation because the progress has truly been astonishing. IACS has embraced the challenges and changes ahead, to support the industry – contributing to the development of a safer and more secure maritime world. Looking ahead, the organisation needs to continue to focus on being agile in addressing relevant industry topics, to strengthen the role of class and to ensure that IACS keeps its position as the leading technical association in these times of rapid change," he added.

Robert Ashdown, IASC Secretary General, also commented: "On behalf of the IACS organisation I would like to thank Knut and the DNV GL IACS team for the great collaboration throughout this chairmanship. The Chairman's drive and ambition to modernise classification have prompted valuable discussions with the industry and the development of a robust long-term strategy that ensures the IACS organisation is fit for the future." IACS' achievements during this chairmanship cover key areas such as autonomous shipping, cyber security, modern survey techniques, and internal benchmarking.

In autonomy, an IACS working group has examined all the relevant resolutions, to identify which standards present potential regulatory barriers to autonomous ship operations. The findings included barriers relating to machinery and electrical systems, safety systems, hull structures and survey procedures. As a next step, a pilot project looked at how to overcome these barriers.

To help the maritime community ensure the cyber-resilience of their assets, IACS established a joint industry working group focused on cyber safety. In its own panel, IACS is developing a number of recommendations for the newbuilding stage to assist shipbuilders in delivering cyber-resilient vessels.

LAUNCHING THE MARITIME CYBER EMERGENCY RESPONSE TEAM (MCERT)

According to Mark Sutcliffe of CSO Alliance, it has become increasingly clear, it has become increasingly clear that maritime cyber criminals are effective at sharing and selling ideas and information. If we are serious about protecting our maritime supply chain we need to learn to work as one and so a dedicated maritime industry response capability has been launched by CSO Alliance – the Maritime Cyber EmergencyResponse Team (MCERT).

The partners bring a range of experience: Templar Executive, Wartsila and the Maritime Port Authority of Singapore are supported by the Maritime Cyber Alliance (https://www.maritimecyberalliance.com). This new 24/7 operation allows for the assembling of criminal cyber tactics, techniques and procedures to be rapidly understood and shared. This knowledge then drives effective incident management and advice to better support corporate and crisis management and through this learning office staff, Captains and crews.

Run by Chris Gibson, who set up and ran the UK CERT for the last three years, it will be based in Singapore and co-located with the new Maritime Cyber Centre of Excellence.

Free to attend workshops to introduce the MCERT are being run in London (10 July), Rotterdam (12 July) and Antwerp (13 July). For more information visit maritimecert.org.

FIVE

MYTHS ABOUT GDPR DEBUNKED...

The European Union's GDPR (General Data Protection Regulation) went into effect on May 25th. So, ok, you have missed the deadline - but you still have to act. Is your business ready?

Let's look at the myths and start to see how they stack up:

MYTH 1: GDPR doesn't affect US businesses...

FACT: GDPR applies to any company that does business with any EU citizen. That includes American companies.

MYTH 2: GDPR only applies to big companies

FACT: If your business, big or small, processes or stores EU customer data, you are required to comply.

MYTH 3: You need an IT guy to implement GDPR compliance

FACT: Everyone in your business is responsible for data security and should know GDPR compliance rules. Even sole proprietors can manage and secure company data. Having an IT guy is not required.

MYTH 4: Your current privacy policy is good enough

FACT: Businesses have had to update their privacy policies and gain explicit consent from the consumer about processing, using, and storing data. Just having users agree to your current privacy policy is not good enough.

MYTH 5: GDPR puts undue stress on businesses

FACT: GDPR is meant to help businesses develop better and stronger cybersecurity plans to protect their customers' data.

So how can your data protection practices better protect your customers and your business?

Audit existing data

To comply with the GDPR, you'll need to start by running an audit on your business's data. This means you'll need to examine what type of personal data you're storing, how you're storing it, why you're storing it, and who's in charge of keeping it secure.

Update privacy policies

Has your inbox been inundated with privacy policy updates recently? The GDPR requires businesses to notify their customers about how they secure and use customer data. For more information, please visit GDPR article 28.

Control employee data access

Control who in your business has access to your data. Implement data security procedures across teams and make sure each employee understands that the business's data is only as safe as the weakest password.

Ensure total transparency

As you're storing your customers' data, it's their right to know how you're using it. Your website needs to state explicitly the how, where, when, what and why of your data practices.

Implement a data breach plan

The GDPR states that all cyberattacks must be reported within 72 hours. To comply with this new law, draft and implement a data breach plan. This should include data lockdown procedures, password changes, customer notification, and insurance agent notification.

Acquire cyber insurance

Given the hefty non-compliance fines, cyber insurance is an important, final step in preparing for the GDPR. Cyber insurance offers crisis management services, lost income reimbursement, legal support, and more.

GDPR is an opportunity to more productively leverage customer data and nurture stronger customer experiences. In doing so, your business will generate longer-term loyalty and higher bottom lines, all while maintaining compliance.

For more information on GDPR, and how to do the right thing - even if you may have missed the May 2018 deadline, see the guidance from the UK government, and start doing the right things today.

https://www.gov.uk/government/publications/guide-to-the-general-data-protection-regulation

A-Z OF CYBER SECURITY

P

Q

R

S

T

P is for point of sale malware. When you buy something on a card, the terminal can scrape the card details and send them to criminals.

Q is for Quantum Cryptography. As computing power continually increases, the strength of encryption needs to increase in parallel. So we may soon be looking at quantum computers generating encryptions.

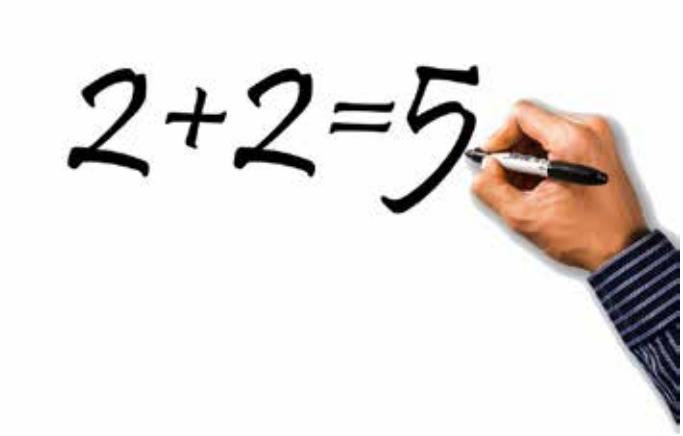
R is for ransomware. This is the most prevalent form of cyber crime. Criminals infect a computer or system and charge a ransom to allow the owner back in.

S is for spear phishing. Phishing emails are generic in nature and usually provide a link to a bogus website designed to harvest credentials. Spear phishing emails are more targeted, seeking to trick the recipient into disclosing credentials.

T is for targeted attack. Most malware is indiscriminate. Cyber criminals usually don't really care who their victim is as long there is a possibility of profiting from them. Targeted attacks are very different. They're usually the work of organized, state sponsored groups and their main motivation is espionage.

source: medium.com

HUMAN ERROR CAN EASILY BE AVOIDED



Most ship cyber security breaches are consequent of human error but can easily be avoided by implementing cutting edge technology and policies to prevent crews from inadvertently infecting shipboard systems.

That was one of the key take-aways from a major maritime cyber conference held in London recently at which delegates were informed of the potentially catastrophic consequences when Operational Technologies are hacked.

“The problem is that when crew or operators use USB sticks to upload system files or log on using their own mobile phones, laptops and tablets or open an infected email, they can potentially upload a malware virus or worse,” Naval Dome CEO Itai Sela told delegates attending the European Maritime Cyber Risk Management summit.

“The biggest maritime cyber issue is the internal attack and the human element,” said Sela.

As 150 million emails are sent globally every minute by more than 4 billion Internet users, it is safe to assume that some of these will be infected and opened by unsuspecting crew members.

“The biggest issue is the internal attack and the human element is definitely part of the problem. Crew training alone is not a solution,” said Sela. “Also, when a technician boards a vessel and connects a laptop or equipment directly to the ECDIS or RADAR to fix or service these systems, can they verify their own systems are secure and have not been infected?”

But there is also an external threat, warned Sela. “Since headquarter and vessel operations go hand-in-hand, it is important to know that when a shipping company’s offices have been hacked it means the company’s vessels are also compromised.”

It emerged at the summit that many systems onboard are still based on old operating systems, such as Windows XP, Windows 7, or Linux – systems designed and manufactured without consideration of the cyber threat. That many of these systems remain unprotected with critical PC-based IT and OT systems frequently using the same Internet connection was a significant concern raised by Lloyd’s Register’s Elisa Cassi, Product Manager, Cyber Security.

CANADIAN NAVY CLEAR ON CYBER

Representatives from the cyber security industry have been invited to work with the Canadian Maritime Forces Pacific (MARPAC), in order to understand how robust the systems are that the Canadian Navy has in place...and of course to suggest improvements which can be made.

A key part of the knowledge sharing exercise was the fact that Navy instructors and the cyber security specialists were able to discuss the cyber security requirements unique to naval fleet operations.

“When it comes to cyber security, it’s going to take everyone,” said Gary Perkins, the Government of British Columbia’s Chief Information Security Officer. “In order to protect our networks, we have to proactively address threats. The Government of B.C. alone sees 240 million unauthorized access attempts per day.”

After a few briefs at MARPAC, visitors boarded HMCS Calgary for a tour with the crew who highlighted the communications and monitoring equipment throughout the ship. The future of cyber security within the Canadian Armed Forces is a focus of Canada’s new defence policy – Strong, Secure, Engaged – which names cyberspace as a critical component of modern military operations.

Digital Ship

MARITIME CYBER RESILIENCE FORUM

@SMM HAMBURG, 5 SEPTEMBER

5th September 2018 sees Digital Ship building on the great success of the Maritime Cyber Resilience Fora in Rotterdam, Athens, Singapore, as they return to the Hamburg Messe und Congress GmbH. The 3 key sessions during this Digital Ship’s Maritime Cyber Resilience Forum in Hamburg will contain plenary presentations and panel discussions:

- Session One: Facing the Cyber Threat: An Overview of Maritime Cyber Challenges and Focus on Building Resilience
- Session Two: Business Planning and Cyber Preparedness
- Session Three: Training, Awareness & Human Factor

To Register: http://www.smm.thedigitalship.com/register

Enquiries, please contact: cathy@thedigitalship.com

HOW WILL PORT STATE PLAY CYBER POLICE?

Norton Rose Fulbright partner Philip Roche believes port state control will play a limited role in enforcing cyber security.

Mr Roche, the global co-head of the firm's shipping group, told attendees at the European Maritime Cyber Risk Management Summit in London that the shipping industry was likely to continue to rely on classification societies and P&I clubs to understand regulatory compliance.

"It's hard to see a port state control officer – a guy who's been at sea, who understands engines and fuels and lifeboats – suddenly becoming armed with the ability to check a ship's cyber security," Mr Roche said.

"It seems to me a lot of reliance is going to be – as it is now – put on classification societies certifying whether a ship is safe to go to sea. Under SOLAS … under Marpol, and those kind of things."

In addition to class notations Mr Roche said the industry could also see something akin to an international oil pollution prevention certificate which ships would carry around to prove they are compliant.

"What I can see is port state control doing basic checks. I cannot see them doing penetration testing, I cannot see them going into great depth, but I can see them doing a check that there is a policy in place."

However, he said there was still room for both P&I clubs and classification societies to collaborate to develop and unify compliance guidelines.

"I understand that there is a P&I working group, that the classification societies have gotten together to get a working group and to have a think about these things and deal with how compliance may well look," he said.

Mr Roche said he did not expect port state control in many countries to be quick to create an enforcement regime, but expected a quicker response from US authorities.

"US Coast Guard, of course, will apply an American approach to this and over-regulate and over-fine anybody who is found to be in breach. There is an interesting US Coast Guard letter about reporting suspicious activity and reporting breaches in relation to US ships," he said.

HYBRID WARS: SHIPS ON THE FRONTLINE

Chris Kremidas-Courtney, Multilateral Cooperative Engagement Coordinator for U.S. European Command (EUCOM) recently shared his thoughts on the maritime cyber threats facing shipping. Access the full article here: https://bit.ly/2K3dQh3

Today, state and non-state actors are challenging nations, institutions, and private companies through a wide range of overt and covert activities targeted at their vulnerabilities. Both NATO and the European Union refer to these as "hybrid threats" and the maritime domain has proven to be especially vulnerable.

Such "hybrid warfare" uses subtle, far-reaching, and opportunistic methods – and seldom with a return address. In other cases, they can be more brazen, but operate in a grey zone in which the impacted state has few good response options without escalating the situation into armed conflict.

Commercial vessels and ports are vulnerable to hybrid threats in the form of sabotage, navigational spoofing, and cyber-attacks on supply chain information systems, resulting in lost or disrupted cargo, denial of access to critical port facilities, and environmental damage. At the same time, foreign ownership and control of commercial port facilities can lead to the disruption of their use when these same facilities are required in times of crisis.

Some commercial shipping companies are currently testing technologies to enable the use of cyber-controlled unmanned container ships to move commodities across the world's seaways. Obviously, the risks associated with this potential development are self-evident when looked at through the lens of maritime hybrid threats, with a potential scenario of a cyber-hacked unmanned vessel being turned into a weapon.

WHAT YOU NEED TO KNOW ABOUT I.T. AND O.T. NETWORKS

Gideon Lenkey, Technology Director at EPSCO-Ra shares his thoughts on maritime cyber security systems and weaknesses.

The maritime cyber security landscape changes rapidly with terms, issues and focus areas bubbling up seemly out of nowhere (even if they've been around for quite some time). At the moment, Operational Technology is all the rage. Let's have a look at OT and compare it to the more common IT.

First off let's define IT and OT. The IMO provides a succinct definition in their publication MSC-FAL.1/Circ.3, section 2.1.2:

Information technology systems may be thought of as focusing on the use of data as information. Operational technology systems may be thought of as focusing on the use of data to control or monitor physical processes.

So, a PC on the bridge used to send and receive email is an IT system. A group of such systems would make an IT network. The IT network is usually connected to the outside world through a satellite data connection. An engine control system used to monitor and manage the main engine is an OT system. It may or may not be connected to other controllers or sensors on a network, and if it is, that network may or may not be connected to the outside world.

OT encompasses and includes Industrial Control Systems (ICS) which are typically made up of Programmable Logic Controllers (PLCs), Discrete Process Control systems (DPCs) or Supervisory Control and Data Acquisition or SCADA systems. So in the OT environment you can have everything from a single controller board using a custom firmware to do a very specific task, control a solenoid for instance, to a PC based system that is monitoring and controlling a network of discrete devices, sometimes from across the public Internet.

When OT systems are stand alone and not connected to a network or the outside world, the threat to their continued operation is quite limited. Threats might include a data update using a USB or other removable media that happens to be infected with malware on a controller that uses an embedded windows or linux operating system. Threats don't always have to be malicious either. For example, a technician making an upgrade that unintentionally makes the controller non-functional is just as effective at rendering it inoperative as the latest and greatest malware.

When you connect multiple OT systems on a network risk increases. This is because the compromise or even malfunction of one connected device can lead to failures in other connected devices. Once again this can be intentional as in the case of a malware agent utilizing a default password or exploit against the underlying operating system or firmware application. Or this can be unintentional as in the case of a malfunctioning device flooding an OT network with chatter that prevents the other devices from communicating properly. Once again the net result is the same, the affected systems cease to function properly with consequences as severe as rendering the vessel immobile in some cases.

When you connect an OT network to the outside world, the risk increases yet again and for two reasons. Firstly, the more complex a system gets, the more unanticipated consequences are likely to emerge. You might remember the USS Yorktown, if not Google "Yorktown divide by zero" and enjoy. The fact your OT environment now has a connection to the Internet also increases your risk because it opens the possibility that the connection could be exploited by an unauthorized outsider or even malware.

As vessel OT environment increase in complexity in an effort to capitalize on the cost and efficiency benefits of digital ship technology, ship managers must keep pace with the rising risk that goes along with it. The risk management practices are probably already in place for other operational areas but do not yet include cyber security in most cases. Ship managers must develop threat scenarios, understand where they are vulnerable and create processes and controls to manage the increased risk. This is considerably more than a technology problem and it will take considerably more than technology to manage it. It's going to take an effort from the C-suite through to the crew to understand and manage the risk which comes with the digital ship revolution.

EPSCO-Ra

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