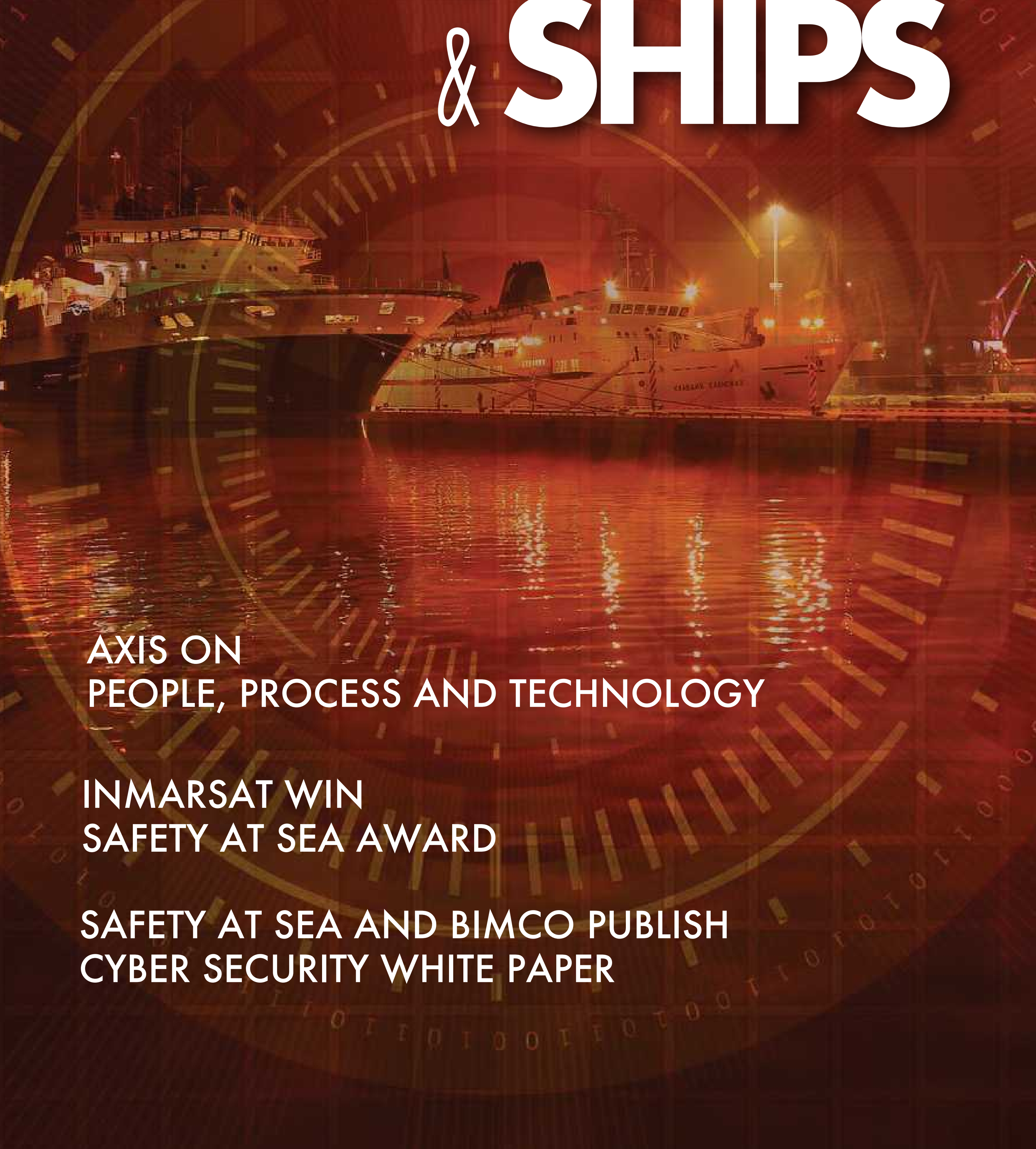
BE CYBER AWARE AT SEA

Kindly sponsored by

AXIS

#35 / OCTOBER 2019

PHISH & SHIPS



AXIS ON
PEOPLE, PROCESS AND TECHNOLOGY

INMARSAT WIN
SAFETY AT SEA AWARD

SAFETY AT SEA AND BIMCO PUBLISH
CYBER SECURITY WHITE PAPER

FROM THE EDITOR

OUR AWARDS

WINNER 2018
SMART4SEA TRAINING AWARD

HIGHLY COMMENDED 2017
SAFETY AT SEA AWARDS

WINNER 2017
BEST CYBER AWARENESS CAMPAIGN
INTERNATIONAL CYBERSECURITY AWARD

PHISH & SHIPS

Welcome to this month's edition of Phish & Ships, brought to you by The Be Cyber Aware at Sea campaign.

Why is it that before we accept an issue or threat is real, we have to withstand the phase of denial? Given the last few years, the number and severity of incidents in our industry and elsewhere, it seems odd to hear that there are still so many deniers of cyber threats, yet that is sadly the case.

Nevertheless back when this initiative was founded, the threats discussed in our pages were still relatively unappreciated and look where we are now, only a few years down the road. Today we can report about the strides made by technology to combat cyber-crime, like the award-winners at Inmarsat, and share the work done by industry leaders such as BIMCO and Safety at Sea to guide us all to stronger cyber security. Barring the few deniers, there is plenty of reason to remain optimistic.

Please continue to follow us at:
Website: www.becyberawareatsea.com
Twitter: @CyberAwareAtSea
Facebook: Be Cyber Aware At Sea
Linkedin: Be Cyber Aware At Sea

Your Editor-in-chief,
Jordan Wylie MA, BA (Hons) Founder,
Be Cyber Aware At Sea

BE CYBER AWARE AT SEA

Kindly sponsored by

AXIS

ONBOARD: UNDERSTANDING PEOPLE, PROCESS AND TECHNOLOGY

Cybercrime is estimated to cost the global economy around $600bn1. With a B. The maritime sector is such a large part of the global economy and given the growing dependence on technology, good cyber habits onboard a vessel are essential.

There is a tremendous amount of content online (including a lot of posters!) on how to practice good cybersecurity at sea. This suggests that a lack of awareness isn't the reason the maritime trade is still feeling so much heat from cybercrooks.

The issue might actually be information overload, so below is a summary of key steps to secure a ship, aligned to three areas – People, Process andTechnology. Hopefully these tips are a bit easier to absorb for non-technical staff.

PEOPLE

Cybersecurity is everyone's responsibility.

A Cyber-Aware staff culture leads to a reduced attack surface, which makes the criminal's job a lot harder. You wouldn't leave your house front door open if you were heading away for a week as you'd probably get burgled. Similarly, each one of us can ensure we keep 'doors' locked on the network in a few different ways – for example, setting **strong, complex passwords** and only **using personal devices for personal browsing**.

Go to cyber school – **educate yourself**. There is a wealth of free information on the internet but to graduate with a First Class Honours, a strong resource is the Be Cyber Aware At Sea MCSA course. It focuses on the people rather than the technology, helping build up a "human firewall" whilst still letting crew stay in touch with friends and family at home.

PROCESS

A ship probably has several processes and technologies that aren't made by the shipping company. While these enable access to systems and capabilities beyond a ship's suite, they also create entry points for malicious software to access the network. Suppliers have easy access – **validate suppliers to ensure they are 'Cyber Secure'** (compliant with Information Security Management standards like ISO27001 or NIST).

TECHNOLOGY

Technology makes the world turn – it's critical to each person or business who uses it. There is a lot of technology onboard a vessel, each piece usually requiring its own security control. Much of this technology releases with a default set of credentials that can be looked up online within a matter of seconds. **Change the password from the default one**, and use a password manager like 1Password to help create, manage and remember different, complex logins.

Unsecured USB ports are the equivalent of an open cat-flap in a locked front door. Best practice is to **secure any USB ports on the vessel,** either through hardware controls or software limitations. If the port needs to be accessed for system patching, use a dedicated USB for this specific activity and keep it secured when not in use. Some manufacturers produce an encrypted USB drive that requires a PIN typed into the drive itself before a computer will recognise it.

Artcile By Akash Bharadia, Technology Specialist – Cyber Unit , AXIS

[1] McAfee & CSIS Report - Economic Impact of Cybercrime— No Slowing Down (https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/rp-economic-impact-cybercrime.pdf)

WHEN YOUR VESSELS ARE VULNERABLE TO ATTACK,

THIS IS THE RIGHT COVERAGE TO BRING ON BOARD.

With cyber security becoming a fast-growing concern at sea, AXIS Marine Cyber is here to bridge the protection gap. See the chart below to understand the difference this innovative coverage makes.

Want to learn more? Contact Georgie Furness-Smith at georgie.furness-smith@axiscapital.com or Sharif Gardner at Sharif.Gardner@axiscapital.com

AXIS Marine Cyber covers:	**AXIS Marine Cyber**	**Standard Hull Insurance**	**Standard Cyber Insurance**
Breach Response Costs and System Restoration	✓	X	✓
Physical Damage to the Vessel	✓	**Infrequently**	X
Income Loss & Expenses from a Breach	✓	X	✓
Third Party Costs and Regulatory Fines	✓	X	✓
Access to Pre-Breach Education	✓	X	**Occasionally**
Access to Specialists During a Breach	✓	X	✓

Coverage is provided by an insurance company subsidiary of AXIS Capital Holdings Limited or by AXIS Syndicate 1686. AXIS Specialty Europe SE is regulated by the Central Bank of Ireland. AXIS Insurance Company, an Illinois property and casualty insurer, is licensed in all 50 states of the United States and the District of Columbia. AXIS Syndicate 1686 is managed at Lloyd's by AXIS Managing Agency Ltd. AXIS Managing Agency Ltd is authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority (Firm Reference Number 754962). AXIS Managing Agency Ltd is registered at Willkie Farr & Gallagher (UK) LLP, 'Citypoint', 1 Ropemaker Street, London EC2Y 9AW (company number 08702952). Coverage may not be available in all jurisdictions and may be available only through licensed producers.

The product information is for descriptive purposes only and does not provide a complete summary of coverage. Consult the applicable policy for specific terms, conditions, limits, limitations and exclusions to coverage.

www.axiscapital.com

AXIS

‘CYBER DENIERS’ - A THREAT TO SUPPLY CHAIN SECURITY

Many shipping executives refuse to acknowledge they are at risk from the growing tide of cyberattacks on the maritime sector by hostile actors, according to one leading lawyer.

As reported in FreightWaves, digitalization is now making it possible to operate entire fleets as a single business. This hugely increases the number of potential security weak links in supply chains as nation states and criminal gangs look for easy targets.

“The shipping industry is being increasingly targeted by a wide range of cyber criminals and terrorist groups as well as international governments, hacktivists and cyber have-a-goes,” said Julian Clark, global head of shipping at London-based law firm Hill Dickinson.

Yet, while some shipowners and managers are proactive on cyber defense and management of risk, “there are still far too many ‘cyber deniers’ in fairly senior positions within shipping organizations.” Clark said these “cyber deniers” see issues such as the NotPetya attack on Maersk in 2017 “as a misplaced bullet or simply collateral damage.”

He added, “All my research, including that carried out with senior figures in both British and U.S. intelligence services, makes it quite clear that this is not the case.” According to Clark, shipping will continue to digitize and boost connectivity to increase business efficiency and to help comply with environmental protection regulations and the demands of crew to have full internet access for family interaction and recreational use.

However, this is “multiplying the doorways through which a cyberattack can be launched,” he said. “Further, as we move toward automation of vessels — and this does not have to be full automation with no crew members at all on board — there will be increased cyber risk and exposure for the maritime community.”

Speaking to FreightWaves on the sidelines of a seminar hosted by Hill Dickinson at London International Shipping week Sept. 10, he said ship operators had no excuse not to act.“Three years ago, I described the situation as technology moving at the speed of a bullet with the regulatory and legal protection regimes riding a bicycle,” he said. “Thankfully through the efforts of the maritime community, growing awareness and guidance provided by institutions such as the IMO, BIMCO, Intertanko and the International Group of P&I Clubs, we do at least now have a clear road map detailing how to arrive at a cyber-safe destination.”

This is already paying dividends with legal firms and security companies reporting an uptake in requests to review the Safety Management Systems of international operators to ensure their cyber policies are up to date. Just as critical as preventing an attack, added Clark, is ensuring recovery after an infection.

“As equally important as having a cyber-prevention regime in place is that a company faced by an almost inevitable cyberattack has the procedures in place in order to recover as quickly and efficiently as possible,” he said.“As with all things, often less is more, and an excellent guide is that provided by the U.S. National Security agency in their ‘Top 10 Cyber Security Mitigation Strategies’ document, which simply lists the 10 top strategies which must be adopted all operating under an overall guidance mantra of Identify, Protect, Detect, Respond, Recover.”

https://www.freightwaves.com/news/cyber-deniers-are-a-threat-to-supply-chain-security

INMARSAT WINS SAFETY AT SEA'S BEST SECURITY PRODUCT OF THE YEAR AWARD

Inmarsat, the world leader in global, mobile satellite communications has won the Safety at Sea Award 2019 for Best Security Product of the Year, after recognition by a panel of judges from ship owner, marine insurance, maritime education, classification, crewing and training organisations.

The prestigious award was collected by Inmarsat Senior Vice President, Safety and Security, Peter Broadhurst, at a ceremony at the Marriott hotel in Grosvenor Square staged during London International Shipping Week 2019. It recognises the contribution to maritime security made by Fleet Secure Endpoint, a key element in Inmarsat's Fleet Secure portfolio of solutions to guard against ever increasing Cyber threats.

"The Safety at Sea Awards consistently recognise improvements in maritime safety, security, training and seafarer well-being, celebrating the organisations and individuals who make positive contributions to protecting lives and working conditions at sea," Broadhurst said. "We are delighted that Fleet Secure Endpoint working on the Fleet Xpress platform has been recognised as 2019's product or service best demonstrating innovation, originality and the potential to improve security on board ship, online and on shore."

The transformation triggered by digitalisation brought with it the need to protect ships and shipping against cyberattacks that could compromise reputations, profits and safety, said Broadhurst.

"The Fleet Secure Portfolio encompasses security measures to protect the user and systems on shore and onboard by inspecting, detecting and responding to any malicious activity so that the seafarer can focus their attention on their day job."

Addressing a key vulnerability of ships at sea, Fleet Secure Endpoint had been developed with ESET (Essential Security against Evolving Threats) to detect and isolate threats introduced by unauthorised or infected devices.

Peter Broadhurst, Senior VP Safety and Security, receiving the award from broadcaster Colin Murray (left) and Guy Platten, Secretary General, International Chamber of Shipping

"Fleet Secure Endpoint provides the local protection on board, taking action when the portal reports a 'rogue node'," said Broadhurst. "This could be a potential attacker or even a new crew device which has no security installed."

In addition, Fleet Secure Cyber Awareness delivers seafarers with effective cyber security training aimed at preventing threats from escalating into full-blown cyber-attack.

Fleet Secure Endpoint will also support ship owners in their efforts to comply with International Safety Management (ISM) code revisions due in force from 1 January 2021.

"In practice, ISM code revisions will mean that, to comply, ships must be able to demonstrate what assets, personnel and procedures are in place onboard and ashore to deal with cyber risks issue, what happens if systems are compromised and who has control," said Broadhurst. "Compliance depends on having the right risk management, infrastructure and procedures in place. Fleet Secure Endpoint offers a scanning and record-keeping tool to document the efforts made to follow guidelines developed by industry organisations such as BIMCO, the International Chamber of Shipping and Intermanager."

https://maritime-executive.com/corporate/inmarsat-wins-safety-at-sea-s-best-security-product-of-the-year-award

SAFETY AT SEA AND BIMCO PUBLISH CYBER SECURITY WHITE PAPER

Safety at Sea, its parent company IHS Markit and its partner BIMCO, have been conducting surveys for years and the white paper, supported by ABS Advanced Solutions, combines an analysis of four years (2016-2019) of survey findings and feedback from experts and matches them to cyber behaviour and investment trends observable in the wider maritime industry.

Gathering knowledge of cyber security is an important tool and will benefit the entire industry.

“BIMCO takes cyber security very seriously and we are continually working on raising awareness among shipowners about cyber risks and how to prepare for cyber incidents.” says Aron Sørensen, head of Maritime Technology & Regulation at BIMCO.

A SHIFT IN INDUSTRY ATTITUDE

In the four years that Safety at Sea has partnered with BIMCO to run the Maritime Cyber Security Survey, a notable shift in industry attitudes to a greater understanding of the threats it faces has been detected, largely boosted by the 2017 Maersk cyber incident.

Conversations have evolved from “awareness” to “preparedness” and this year’s survey showed that companies are working to protect their IT systems, operational technology systems and against vulnerabilities introduced by third parties.

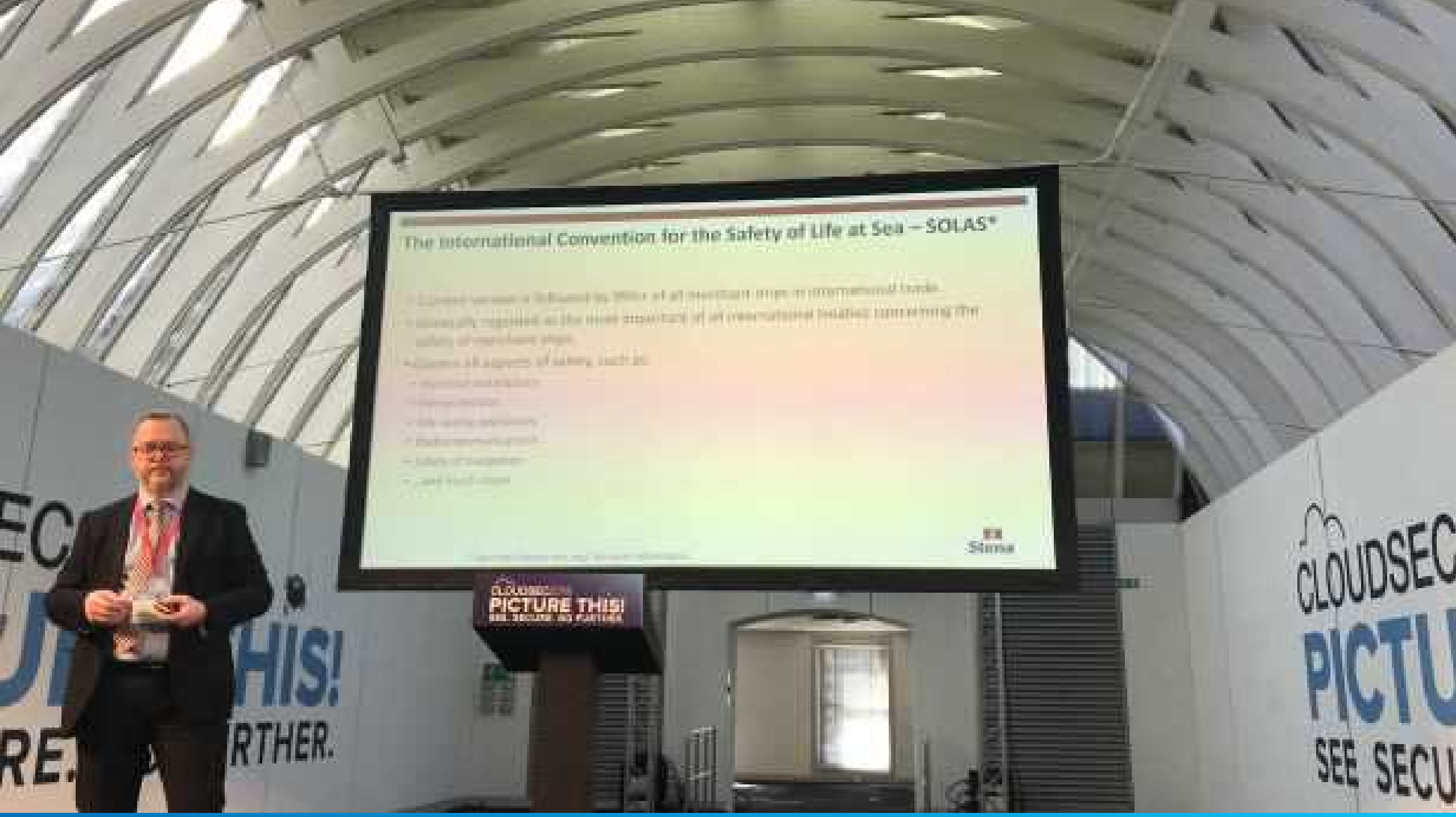
However, the size and scope of the cyber security threat within the maritime sector are still largely unknown, due in part to shipowners’ reluctance to share their experiences for fear of reputational damage.

From the white paper, readers will gain a comprehensive overview of the key cyber security issues facing maritime, touching upon past major incidents and industry-best practice, as well as practical advice on prevention and recovery. The paper also focuses on risk assessment, training and cultural change, insurance and operational technology.

This year, BIMCO, CLIA, ICS, INTERCARGO, InterManager, INTERTANKO, IUMI, OCIMF and WSC published version 3.0 of The Guidelines on Cyber Security onboard Ships, which offers guidance to shipowners and operators on how to assess their operations and develop the necessary procedures and actions to improve resilience and maintain integrity of systems onboard their ships.

Source: BIMCO

> **“ BIMCO takes cyber security very seriously and we are continually working on raising awareness among shipowners about cyber risks and how to prepare for cyber incidents. ”**
>
> - Aron Sørensen, Head of Maritime Technology & Regulation at BIMCO.


The International Convention for the Safety of Life at Sea – SOLAS*
Stena
PICTURE THIS!
CLOUDSEC
PICTU
SEE SECU
HIS!
RTHER.

STENA SECURITY HEAD LIKENS THE MARITIME DISASTER TO CYBER SECURITY BLUNDERS AND GIVES HIS THOUGHTS ON HOW TO MOVE FORWARD

Speaking at Cloudsec 2019 Magnus Carling, the CISO of worldwide conglomerate Stena AB, likened modern cyber security practices to the mistakes made on board Titanic leading to disaster.

As reported by Connor Jones for IT Pro, Carling first said that Titanic's captain ignored warnings from other ships about the ice ahead. This correlates to system administrators either ignoring or misreading warning signs of an imminent attack.

Secondly, Carling stated that the captain, by speeding into an ice field at 22 knots, much higher than was considered safe, he was demonstrating unsafe work practices. Again, this equates to managers ignoring security best practices for effective cyber hygiene.

Thirdly, the crew of Titanic were not drilled in disaster training, akin to having no cyber attack strategy in place, and not drilling employees in how to react.

Finally, Carling stated that the Titanic was outfitted with too few lifeboats for the number of passengers and crew onboard, and the crew knew and ignored this fact when they departed port. Carling compared this to when employees silence "the security voice".

"I can bet my dog that someone somewhere told someone in charge [that] it's not a good idea to run in that high speed, it's not a good idea to not have lifeboats and not train the crew how to use the lifeboats - and I think we're seeing this today, in many cases," he added.

While the analogy is perhaps a little laboured, Magnus Carling makes clear points about where the industry sits, that mistakes are being made that will, in retrospect, seem all to obvious. However, just in the wake of the maritime disaster regulations were tightened to prevent similar tragedies, he also believes the future of cyber security lies in stronger regulations rather than self-policing. "…a lot of

> “The Titanic’s captain ignored warnings from other ships about the oncoming iceberg, just like how system administrators sometimes either ignore or misread warning signs that a business may be under attack.”
>
> - Magnus Carling, CISO of Stena AB

people think that regulations are like this heavy weighted blanket [and that] it's a lot of work being compliant. But they do help you because they give you arguments that you should improve your cyber security stature."

Carling heralded regulations such as the network and information systems (NIS) directive adopted by EU member states in 2016 - the first EU-wide cyber security regulation – and compared it to the safety of life at sea (SOLAS) convention adopted in the maritime industry.

The directive is aimed to unify the standards of cyber security within the EU to help protect member states from being attacked through vulnerabilities in other nations and was implemented in UK domestic law at the same time as GBPR.

He also raised the practice run at Stena of testing their defences internally in cyber attack training days. They run such exercises three times a year, pitching one team of cyber security practitioners against another, a ‘red’ attack team and a ‘blue’ defensive one.

Connor Jones reported that upon being asked about outcomes from these exercises, Carling said that they discovered that asset management was something they realised they faced issues with. "[The red team] will find devices that are not supposed to be there and utilise them, they will breach them and get in. If you have a good red team, you can't stop them, they will get in one way or another," said Carling. "The only difference is how long it takes for them to get in. The improvement that we want to see is whether the blue team is getting better at detecting them."

In addition to regular exercise, Stena also has a global SOC which gives their security experts a holistic, business-wide view of their facilities' security. "No captain would ever navigate without radar," he said, so there's no reason why security professionals should operate without an extensive view of oncoming threats.”

The latest technique used by the company is deploying cyber security ambassadors where individuals from different Stena facilities who have shown an interest in cyber security can congregate and receive extensive training and then head back to their base and spread that knowledge to their team.

https://www.itpro.co.uk/security/34443/modern-cyber-security-bears-great-resemblance-to-the-titanic-disaster-says-stena-ciso

DIGITAL SHIP ATHENS - Now in its 17th year - reviews the most important topics of maritime digitalisation, in the world's largest centre of shipping and technology. We are at early stages with the agenda but here are some of the topics we might be discussing this year:

- **Satellites**
- **Cybersecurity**
- **Onboard systems**
- **Digitalisation project management**
- **Fuel efficiency data**
- **Predictive maintenance**

Venue: Athens Marriott Hotel
Leof. Andrea Siggrou 385
Athina 175 64 Greece

No admission charge for ship owners, operators, managers and builders.
To register: https://www.athens.thedigitalship.com/register/
Enquiries: lyndell@thedigitalship.com

ClassNK BOOSTS MARINE CYBERSECURITY CAPABILITIES

Tokyo-based ocean ship classification society ClassNK is boosting its cybersecurity capabilities by setting up a cross-sectional team of marine and security experts.

ClassNK said that it is boosting its cybersecurity capabilities to meet the expanding needs of clients. A key development was a decision of the Maritime Safety Committee, part of the UN's International Maritime Organization, to adopt "Resolution MSC.428(98) Maritime Cyber Risk Management in Safety Management Systems." Among other things, that resolution encourages the shipping industry to ensure that cyber risks are "appropriately addressed" in ship management systems no later than Jan. 1, 2021.

PRACTICAL CYBERSECURITY

ClassNK said that ship cybersecurity is "entering a practical stage."

In response to questions from FreightWaves, ClassNK said its main concept for cybersecurity is to take measures "in a holistic and comprehensive way. This is why we have gathered ship and security experts to work on cybersecurity efficiently, instead of separately, resulting in faster and more practical service."

This approach will include measures based on a combination of physical, technical and organizational approaches "such as designing ships and onboard equipment with security by design, and constructing management systems during service to mitigate cyber risks in both information technology and operation technology."

CLASSIFICATION SOCIETY SUPPORT

ClassNK told FreightWaves that it is setting up its cybersecurity team in response to the expanding needs of clients and will include cybersecurity class notation for ships and ship/company management system certification.

The classification society says that ship owners and operators will receive support from ClassNK to update their safety management systems in line with the resolution from the Maritime Safety Committee. This will include help with the development of advanced projects including support through the issue of certification, ClassNK told FreightWaves.

To date, ClassNK has set out four sets of guidelines on this topic. These include:

- The basic Cyber Security Approach (February 2019)

- Guidelines for Designing Cyber Security Onboard Ships (February 2019)

- Cyber Security Management System for Ships (March 2019)

- Guidelines for Software Security (June 2019)

CLASSIFICATION SOCIETIES

Classification societies are fundamentally important to the operation of international ocean-going ships. A classification society carries out several functions. Primarily, it creates technical standards for the safe operation of ocean-going ships. It also carries out inspections and surveys of ships to check that the vessels are seaworthy. The society will also issue classification certificates to ships if they are seaworthy and meet the applicable rules and standards.

A ship without a classification certificate cannot receive and sustain its liability insurance, equipment insurance or hull and machinery insurance. A ship that falls out of class for any reason will automatically invalidate its insurances. A ship operator that runs a ship without marine insurance runs a phenomenal financial risk in the event of any kind of accident.

In addition a ship that falls out of class will almost certainly be in breach of various contracts (whether for hire or carriage, or for any loan on the vessel) and the ship will very likely be detained by the authorities at the first port of call. An ocean-going ship that is not "in class" essentially cannot trade.

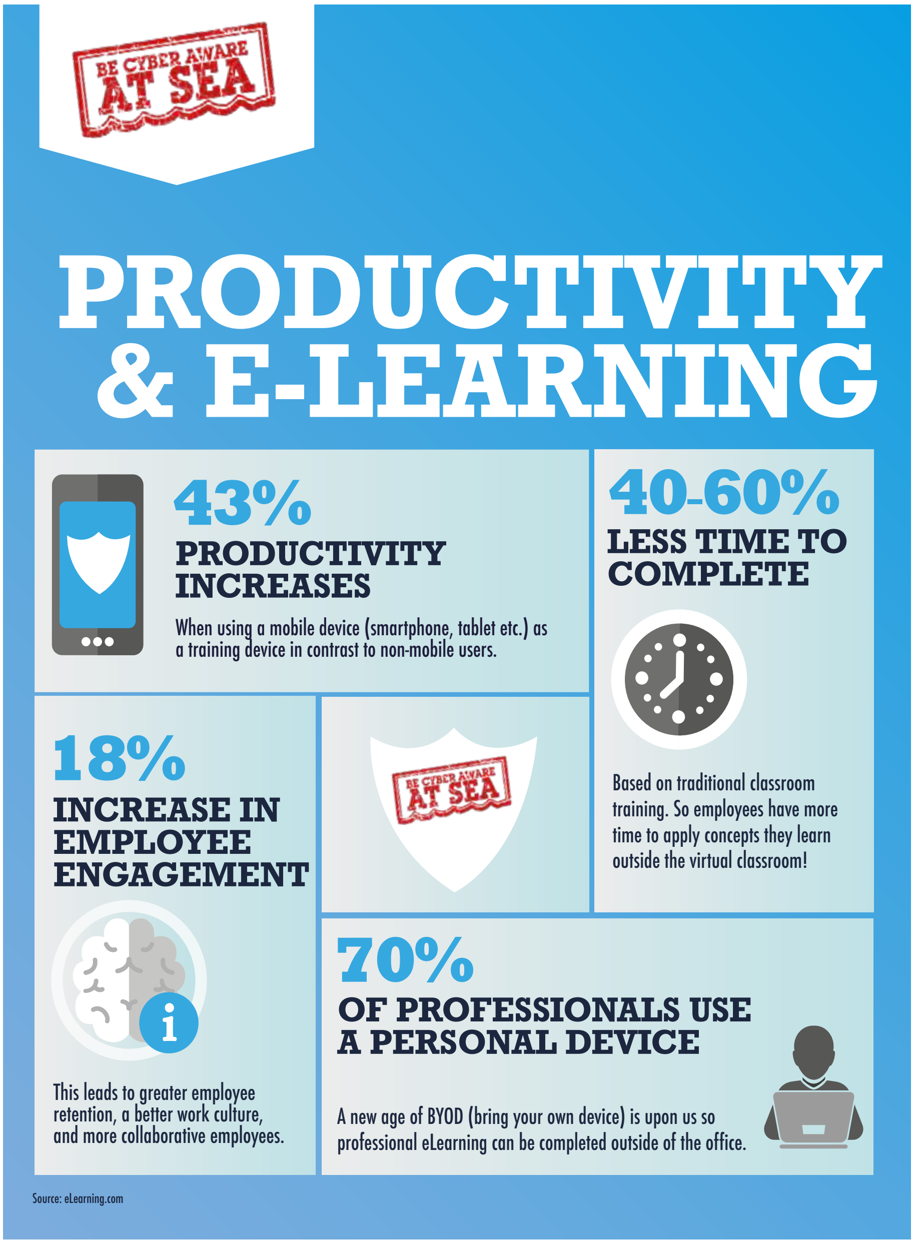
https://www.freightwaves.com/news/classnk-boosts-marine-cybersecurity-capabilities

Why Choose eLearning?

In today's 24/7 hectic world finding time to attend a week-long training course can be quite a challenge. Even getting a couple of days away from the workplace can be difficult.

eLearning enables you to learn at a time and place convenient to you. You can repeat lessons / sections of a course until you are sure you understand them and easily monitor your progress too.

Our infographic also looks at how eLearning can help with productivity.



PRODUCTIVITY & E-LEARNING

43% PRODUCTIVITY INCREASES

When using a mobile device (smartphone, tablet etc.) as a training device in contrast to non-mobile users.

40-60% LESS TIME TO COMPLETE

Based on traditional classroom training. So employees have more time to apply concepts they learn outside the virtual classroom!

18% INCREASE IN EMPLOYEE ENGAGEMENT

This leads to greater employee retention, a better work culture, and more collaborative employees.

70% OF PROFESSIONALS USE A PERSONAL DEVICE

A new age of BYOD (bring your own device) is upon us so professional eLearning can be completed outside of the office.

Source: eLearning.com

1 Hour MCA Recognised & GCHQ Approved Training

Maritime Cyber Security Awareness Course (MCSA)

The ‘human factor’ is your biggest vulnerability to cyber crime.

Educate your workforce today to protect themselves and your organisation tomorrow.

- Easy access 1-hour online course
- Designed to complement current approaches to cyber security
- Suitable for all personnel – onboard and ashore
- MCA Recognised and GCHQ Approved

JWC INTERNATIONAL

For more information or to book, please visit us: www.maritimecybertraining.online

BE CYBER AWARE
AT SEA

CLOUD SECURITY

USE IT WISELY AND PREPARE FOR ANY WEATHER!

Use secure passwords
Back up the more important files
Keep Anti-virus software up to date
Be aware of what you are storing