Guide to cyber security

Incorporating the GNS
3i Cyber Security Framework

www.gnsworldwide.com

Guide to cyber security

In our modern, connected and digitised world, cyber threats have become a fact of life, capable of doing harm to people, vessels and business.

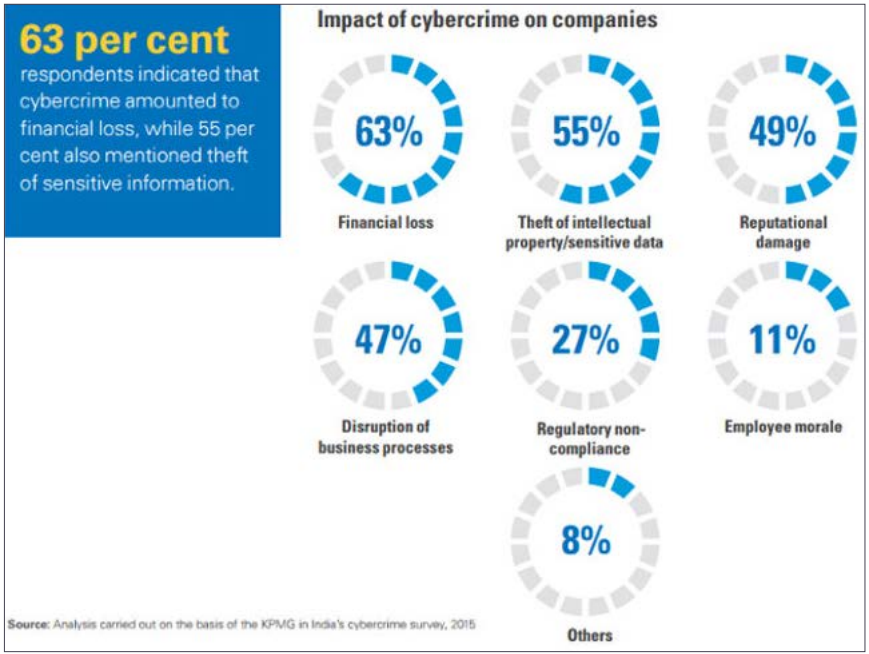
The IMO has given ship owners and managers until January 2021 to incorporate cyber risk management into ship safety. Non-compliant vessels will be at risk of detention after this deadline.

With this in mind, GNS has produced the simple, memorable **3i Cyber Security Framework** to help the industry both improve understanding of cyber security and develop best practice.

Clear and present danger

There is little doubt that cyber threats present a clear and present danger to the wellbeing of individuals, society and business in our increasingly digitised and connected world.

Whilst some of the more extreme examples of cyber risk, even if theoretically possible, are at the outer reaches of probability and imagination, and can probably be considered to be scaremongering, there are plenty of less extreme scenarios that can negatively impact upon ships, ports, people and profit margins. For example, a simple denial of service attack on a cruise ship terminal



attempting to board 3,000 hungry passengers and 6,000 pieces of luggage will still cause mayhem, reputational damage and cost lots of money.

To protect themselves, organisations need to reduce the probability of high impact events. **GNS's 3i Cyber Security Framework** provides a simple and easy to remember way for any maritime and marine organisation to achieve this by proactively harnessing the mutually supportive power of people, process and technology to address all risks, including the more scary ones, using a holistic risk-based approach.

Cyber security is a subject that needs to be understood and implemented 'From the Boardroom to the Bridge' and taken seriously if owners are to avoid problems ranging from disruption of operations to reputational damage, pollution, financial liability and, in extremis, loss of life.

If senior management are in any doubt about this, they just need to look at the cost of the cyber-attack on Maersk or, outside of shipping, the way that 'Equifax' shares plummeted after a cyber-attack that they suffered.

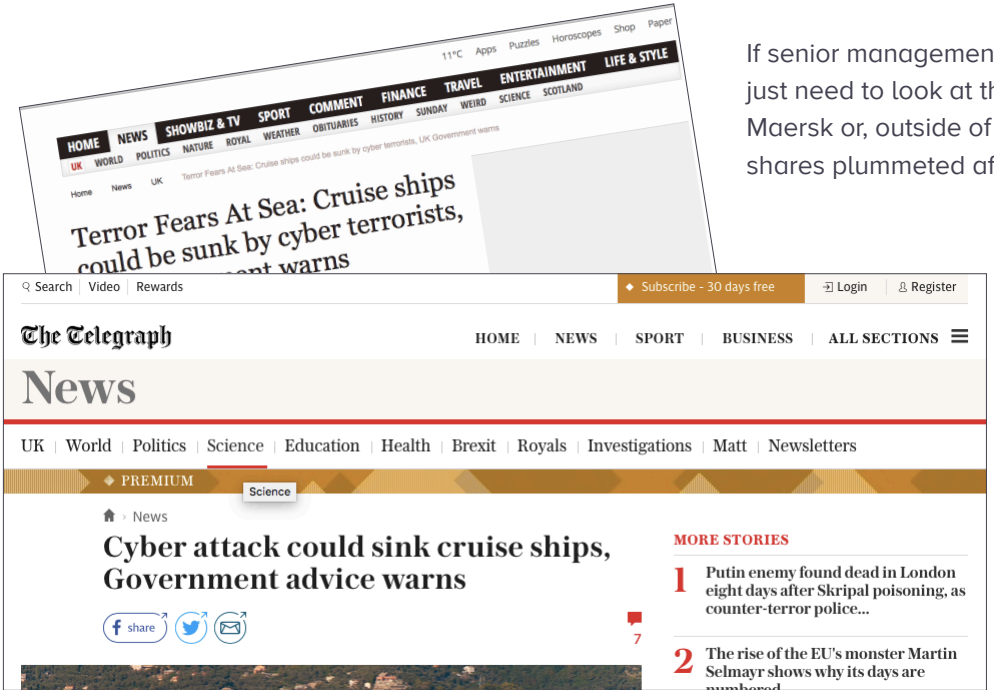


Image left: When the UK Government launched the IET Standards 'Code of Practice – Cyber Security for Ships, a UK newspaper ran sensationalist headlines. The reality is that this is at the outer reaches of probability and imagination.

Beware of information overload

At the time of publishing this white paper there were no fewer than 37 cyber security documents listed on the Be Cyber Aware at Sea website.

These range from the short and strategic IMO guidelines on Maritime Cyber Risk Management to the detailed and dense guides that classification societies, shipping associations, the IET and others have published.

The message is clear, that cyber security is now being taken seriously and that measures to deal with cyber threats need to be incorporated into existing risk management processes and tackled in the same way as we deal with other safety and security threats.

“There is danger of information overload.”

Jordan Wylie, Founder, Be Cyber Aware at Sea

Leading industry authority on cyber security and founder of the ‘Be Cyber Aware At Sea’ campaign, Jordan Wylie, has said ‘there is a danger of information overload’ for anyone trying to make sense of the large amount of information available today.

To write this paper, GNS’s resident marine security expert, Ian Millen, undertook a comprehensive review of all the available guidance from government, shipping industry entities and technology suppliers and distilled it down to create this very simple, practical **3i Framework** for managing cyber security risks.

GNS 3i Cyber Security Framework

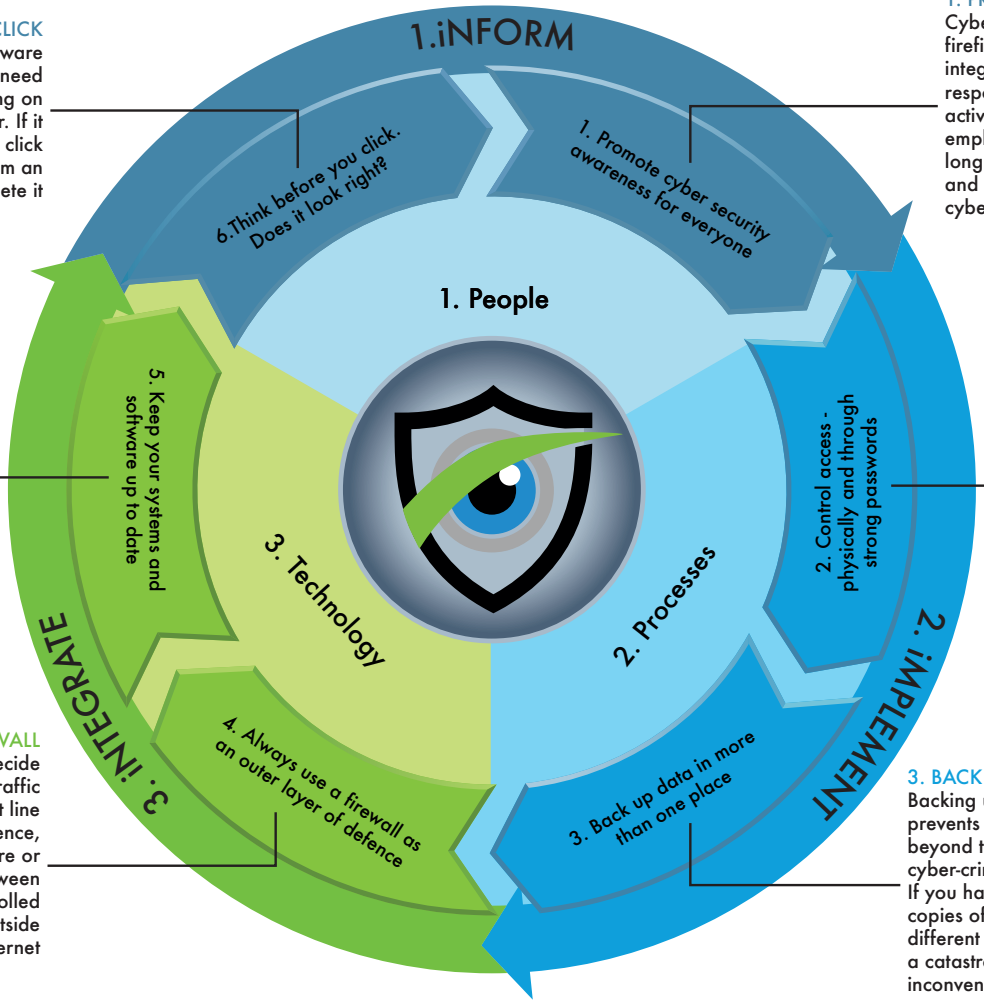
The shipping industry is used to managing and protecting assets in a business and operating environment fraught with risk, through education, training and a highly developed risk-based culture. It makes sense to extend this methodology to cyber security.

The **GNS 3i Cyber Security Framework** is a simple and memorable way to help both improve understanding of cyber security and develop best practice.

In defending against any threat, it is good practice to have more than a single measure. Cyber security is no exception. For this reason the **GNS 3i Framework** is based upon a layered approach with each of the elements and measures working in combination to form a robust, yet easily understandable, strategy to achieve effective cyber security protection.

The Framework comprises three main elements of people, process and technology, supported by the measures of inform, implement and integrate.

The Framework also provides six simple steps that everyone can take to significantly reduce the risk posed by cyber security threats long before the need to invest in professional support or high-technology. It also helps make individuals, organisations and systems more resilient.



6. THINK BEFORE YOU CLICK

The 'WannaCry' ransomware attack demonstrates the need to think twice before clicking on anything that is not familiar. If it doesn't look right, don't click on it and seek advice from an IT professional or delete it

1. PROMOTE AWARENESS

Cyber security, like first aid, firefighting or watertight integrity is everyone's responsibility - a whole ship activity. Simple measures employed by all can go a long way to preventing costly and sometimes dangerous cyber security problems

5. KEEP UP TO DATE

Modern business software and anti-virus programs feature regular updates which should always be downloaded and run - they are useless if not implemented - and can be set to 'auto-update' on trusted systems

2. CONTROL ACCESS

Physically and through strong passwords. Controlled access to IT sytems, supported by policies and processes, ensures that they are only used by those authorised to use them, for the purposes they are intended, in a way that they should be used

4. USE A FIREWALL

Firewalls can be used to decide whether to allow or block traffic and often represent the first line of technological defence, providing a hardware or software barrier between secured and controlled networks and untrusted outside networks such as the internet

3. BACK UP DATA

Backing up critical data prevents loss and puts it beyond the reach of cyber-criminal ransomware. If you have accessible copies of your data in different locations, you turn a catastrophe into an inconvenience.

The 3i focus areas

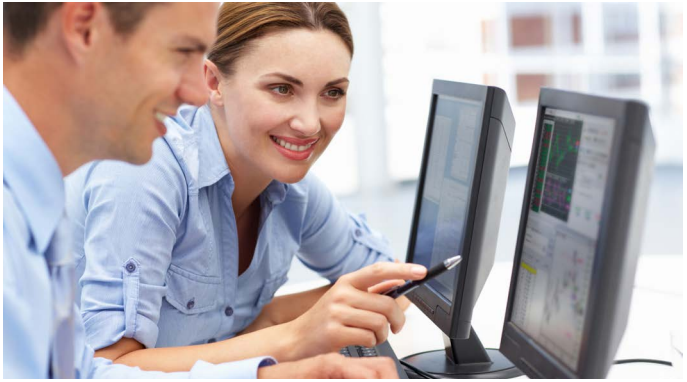
The **3i Cyber Security Framework** has 3 key areas of focus. These areas will be unsurprising to anyone already well versed and/or involved in risk management.

1 PEOPLE

Primarily concerned, although not limited to, the education training and awareness of staff ashore and afloat.

As with most things, the best place to start with cyber security is with people. Without doubt, people are the greatest asset when it comes to mitigating risk, but can equally become the greatest weakness, especially when process is ignored or technology is used incorrectly.

When vigilant, well-educated and well-trained they are the greatest single asset in protecting against Cyber threats. Unaware and untrained, they become the greatest liability and can themselves create vulnerabilities in otherwise secure systems.



When unaware of cyber threats and untrained in the ways of reducing cyber risks, an individual is more likely to inadvertently open a digital door for someone with malicious intent or, perhaps, infect a critical system through misuse of technology or failure to follow simple rules. The unauthorised USB or mobile phone charger in ECDIS terminal is often used as an illustrative example. However, if we make that same individual aware of the

threats and familiar with safe practice, we have a very different situation.

Unsurprisingly, developing the required risk-based culture starts with education and training to address awareness of the problem. Leadership, of course, sets the tone for the development of this culture, so it's important to educate those in shipping's boardrooms and operational headquarters to the fact that cyber security is not the latest fad or a problem for the IT department alone, but as necessary a part of everyday business as good financial and operational management.

2 PROCESS

Process provides the organisational foundation for other 3i elements, illuminating the path that people should follow.

Policies, procedures, protocols and guidance that set standards and articulate agreed ways of working (including access controls, workflows, information and operational technology regulations) provide the guidance for the safe use of information and operational technology (IT/OT) systems.

3 TECHNOLOGY

Primarily IT-related protective programmes and systems, including supporting specialist individuals and, where available, security operations centres (SOC).

Technology, from virus checkers to 24/7 endpoint monitoring, patch management and other IT/OT related computing and engineering capabilities.

The 3i measures

Importantly, the **3i Cyber Security Framework** also includes 3 key measures as follows:

1 iNFORM

People should be **iNFORMED** through regular education and awareness training, creating a healthy culture of cyber hygiene through free to use awareness initiatives, such as 'Be Cyber Aware At Sea' and its supporting communications (e.g. poster campaign and Phish & Ships monthly newsletter).

iNFORM also includes the need to share knowledge of threats and incidents across the industry and beyond, to make others aware of the risks and mitigation measures to protect people, organisations and systems against cyber-criminals. Solutions such as the Maritime Cyber Alliance, which provides access to information about latest cyber and other maritime crime, so that shipping companies and crew can guard against similar attacks, can help with this.

Appropriate, accredited training should also be provided to all those who operate IT/OT at sea with regular reviews of competency. An example of such training is the Be Cyber Aware at Sea Training solution - just one of the applications in GNS's **Voyager HUB** back of bridge software solution.

Such training and assessments should be addressed with the same focus as those that address quality, health, safety and environment (QHSE) issues, as cyber threats have the potential to adversely affect all of these areas.

2 iMPLEMENT

Policies, procedures, protocols and guidance should be developed and **iMPLEMENTED** to create the foundations for sound cyber security processes, as well as plans for disaster recovery and business continuity in the event of a successful cyber-attack.

Process documents and workflows should set policies on all elements of layered defence, including the roles and responsibilities of individuals. Such documents should also be based upon comprehensive cyber security assessments and gap analyses.

Where guidance is clear and easily understandable, risk can be significantly reduced through the proper adherence by people to safe and secure ways of working with available technologies.

3 iNTEGRATE

Protective technologies that monitor threats, prevent unauthorised actions and threat penetrations should be integrated into the overall protective systems. These are not a panacea but, when used effectively, can be an extremely effective element of the overall cyber security layered defence system.

Such technologies should b e**iNTEGRATED** into the overall system and should be operated (sometimes by people), reviewed, maintained and replaced in accordance with company cyber strategies and plans provided by the Process element.

The 3i practical steps

There are number of quite simple things you can do to significantly reduce the risk of falling prey to a cyber-attack or, in the worst case, ensure a quicker recovery afterwards.

The following six practical steps are not the whole story, but are a very good place to start for ship owners, managers and operators to improve cyber security.

1 Promote cyber security awareness for everyone

Cyber security, like first aid, firefighting or watertight integrity is everyone's responsibility – a whole ship activity. Simple measures, employed by all can go a long way to preventing costly, and sometimes dangerous, cyber security problems.

2 Control access

Physically and through strong passwords, controlled access to IT systems, supported by policies and processes, ensures that they are only used by those authorised to use them, for the purposes they are intended, in a way that they should be used.

3 Back up data in more than one place

Backing up critical data prevents its loss and puts it beyond the reach of cyber-criminal ransomware. If you have accessible copies of your data in different locations, you turn a catastrophe into an inconvenience.

4 Always use a firewall as an outer layer of defence

Firewalls can be used to decide whether to allow or block traffic and often represent the first line of technological defence, providing a hardware or software barrier between secured and controlled networks and untrusted outside networks such as the internet.

5 Keep your systems and software up to date

Modern business software and anti-virus programs feature regular updates which should always be downloaded and run – they are useless if not implemented – and can be set to 'auto-update' on trusted systems.

6 Think before you click. Does it look right?

The 'WannaCry' ransomware attack demonstrates the need to think twice before clicking on anything that is not familiar. If it doesn't look right, don't click on it and seek advice from an IT professional or delete it.

In light of the IMO's recent decision to give ship owners until 2021 to incorporate cyber risk management into ship safety, the clock is ticking.

Some will argue that there is no such thing as 100% cyber security, as criminals will continue to develop new threats. Others will try to stay one step ahead with technology and processes to prevent and defeat their malicious activities.

Forward thinkers will not be waiting for the deadline, but will be making cyber security as instinctive a part of ship management as watertight integrity. They will also be training their crews in the basics to make sure they have an understanding and awareness of cyber threats and simple steps to minimise the risk.

Those that wait for the 2021 alarm call, continue to believe that cyber security is a IT department issue or see it as just another way for opportunistic suppliers to make money from fear, will risk the negative impacts of non-compliance and also lay themselves open to greater risks in the meantime.

A few relatively simple measures, such as those documented in the **GNS 3i Cyber Security Framework**, can and will greatly reduce the risk of attack or, at the very least, minimise the impact should the unthinkable happen.

It should, of course, be recognised that shipping companies, managers and vessels will be subject to whatever the pre-eminent regulation is for their particular flag, classification society or other requirements with which they need to comply.

Specific plans and actions will naturally and necessarily need to take specific requirements into account. However, having a highly memorable framework, like the **GNS 3i Cyber Security Framework**, will assist all by providing a common language and a practical starting point.

Mike Hawthorne, CEO of Cobweb Cyber Ltd and former Commander of the UK Ministry of Defence Joint Forces' Cyber Group sees the problem through the stereoscopic vision of a cyber expert and former vessel captain.

He likens the cyber issue to the instinctive understanding of keeping a ship afloat, saying that 'Watertight integrity can be breached

Mike Hawthorne
CEO, Cobweb Cyber

through any untoward activity or event that allows the ingress of water into unwanted areas or compartments of a vessel.

It is the individual responsibility of all employees, visitors, contractors and clients to be aware of how watertight integrity might be breached, often communicated in a ship safety brief. In the same way, the maritime sector should demand an instinctive understanding of maritime cyber security.'

Maritime cyber security guidelines

The latest guidance pages on the Be Cyber Aware At Sea website, details some 37 documents, with the number increasing at a steady rate as more guides join the ranks. With so much guidance available, how to make sense of it and put it to practical use?

Much of the advice and guidance is unsurprisingly similar in content, reflecting the input of cyber security experts and the gradual emergence of best practice across the many volumes of guidance.

Such a broad and growing body of work is a testament to the growing appetite to understand and tackle cyber security threats for operational, reputational and business critical reasons. This appetite for guidance is encouraging, in spite of the fact that no current international regulation exists, as it does for other aspects of maritime quality, health, safety and environment (QHSE). Such regulation is, however, on the horizon as the IMO's January 2021 deadline for the incorporation of cyber risk management into ship safety systems draws near.

The challenge with the volumes of comprehensive, informative and detailed guidance so far published is that they can't possibly be all things to all people. Board members and senior executives are unlikely to wade through many tens of pages of advice, just as ships' crew members will not get the straight forward guidance they need from some of the dense documents, mainly written in English. There is absolutely a place for these

documents, but there is also a need to distil their content into manageable chunks that are easy to consume and digest.

That's where Be Cyber Aware At Sea has succeeded with its posters and videos aimed at transforming vulnerable, unaware and untrained crew members into vigilant anti-cyber warriors, alongside executives and managers ashore who can understand the scale of the problem, learn from the experience of others and guide efforts to protect their people and their business from cyber criminals.

Its also where tools like the **GNS 3i Cyber Security Framework** come in - doing the work of reading and digesting all the information available and turning it into practical advice and guidance that can be applied across the whole organisation.

If you are interested in reading some of the reference material that we have drawn on to produce this white paper, we would recommend these three primary documents:

- The IMO Guidelines on Maritime Cyber Risk Management (MSC-FAL.1/Circ.3) .
- The BIMCO (et al) Guidelines on Cyber Security Onboard Ships (ver 2.0).
- The IET Code of Practice Cyber Security for Ships (2017)

These documents range from the IMO's high-level, international policy-related guidance to detailed advice that describes the threats, vulnerabilities, protections and responses in far greater detail. These documents, taken together, provide a comprehensive picture which will assist organisations in educating staff, developing processes and procuring appropriate technologies to support their businesses.

The IMO Guidelines on Maritime Cyber Risk Management

The IMO Guidelines on Maritime Cyber Risk Management, published on 5 July 2017 as MSC-FAL.1/Circ3, provide high-level recommendations, advising stakeholders to take the necessary steps to safeguard shipping from current and emerging threats and vulnerabilities in the age of digitisation, especially in view of the increasing

integration and automation that characterise the modern shipping industry.

These guidelines, necessarily brief and expressed in broad terms, sit at the strategic level of advice, recognising the existing volumes of industry guidance and best practice.

Recognising the authority and requirements of other bodies and administrations, and noting the need for users to comply with relevant industry standards and best practice, the IMO Guidelines highlight the parallels between the practice of risk management in the physical domain with the approach and measures needed to replicate this same approach to address cyber security threats and risk in the digital domain. The guidelines recognise the critical role that numerous systems play in 'safety, security and the protection of the marine environment', detailing vulnerable systems that 'could include, but are not limited to:

- Bridge systems
- Cargo handling and management systems
- Propulsion and machinery management and power control systems
- Access control systems
- Passenger servicing and management systems
- Passenger facing public networks
- Administrative and crew welfare systems
- Communication systems

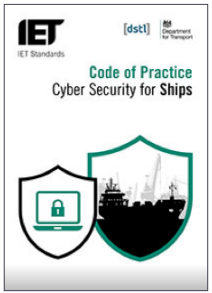
Furthermore, and in recognition of not re-inventing practices that are fit for purpose in other areas of risk management the guidelines 'recommend a risk management approach to cyber risks that is resilient and evolves as a natural extension of existing safety and security management practices.' Critical to the success of effective cyber risk management, the guidelines encourage a holistic and flexible approach across all levels of an organisation, with senior management embedding a strong culture of cyber risk awareness, with a risk-based approach that results in the most effective use of resources.

With five functional elements, the IMO Guidelines, detail the non-sequential steps of Identify, Protect, Detect,

Respond and Recover, as encompassing the ‘activities and desired outcomes of effective cyber risk management across critical systems affecting maritime operations and information exchange, and constitute an ongoing process with effective feedback mechanisms.’

IET STANDARDS CODE OF PRACTICE ‘CYBER SECURITY FOR SHIPS’

The UK Department for Transport (DfT) sponsored and Institution of Engineering and Technology (IET) authored ‘Code of Practice’ on ‘Cyber Security for Ships’ was launched during London International Shipping Week in 2017.



The 72 page document was produced in collaboration with the UK’s Defence Science and Technology Laboratory (dstl) and follows on from the 2016 publication of ‘Cyber Security for Ports and Port Systems.’

Whilst the document is most applicable to those operating UK-flag ships in UK waters, the well-researched text and helpful checklists in the main body and appendixes are no less helpful to those who operate under different flags, outside of UK jurisdiction and with non-British crews.

The Code of Conduct provides good practical advice, especially on the elements of a Cyber Security Assessment (CSA) and Cyber Security Plan (CSP). Appendix I of the document contains helpful checklists that provide a very useful start point for both understanding and action. The document is helpful, if ambitious in the scope of its anticipated readership, which ranges from those with direct responsibility for the protection of ships, cargo, passengers and stores to those who build, maintain, manage and insure vessels amongst others.

As a code of conduct, it is not a statutory document, but of course those who it supports will be expected to have knowledge of it in the event of something going badly wrong because insurers will read every sentence to see if a claimant has been negligent in their application of the common-sense advice it contains.

THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS

This document has been produced and is supported by BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, OCIMF and IUMI and is the product of a wide range of stakeholders. As with other available guidance, the document is designed to assist companies develop resilient approaches to cyber security onboard ships.

The guidelines draw upon the National Institute of Standards and Technology, US Department of Commerce (NIST) framework, which help to understand, manage and express cyber security risks both internally and externally.

The document is also aligned with The IMO Guidelines on Maritime Cyber Risk Management (MSC-FAL.1/Circ3) and broadly follow the high-level guidance in the IMO document, with a structure based around identifying threats and vulnerabilities, assessing risk, developing protection, detection measures and contingency plans, as well as responding to and recovering from cyber security incidents.

While this document doesn't boast as many helpful diagrams and checklists as the IET Code of Conduct, its strength lies in the input from a very wide range of stakeholders from the shipping, cruise and insurance industries, as well as supporting cyber professionals.

FURTHER READING

You may also wish to explore two current initiatives aimed at increasing awareness of cyber security and combating of combating cyber criminals through information sharing and collaboration.

Be Cyber Aware At Sea is doing much to educate seafarers and the wider shipping industry through simple, easily understandable messaging and training resources such as those available in GNS's Voyager HUB. With over 33,000 subscribers to its monthly Cyber Awareness Newsletter 'Phish & Ships' and 100,000 downloads of its awareness poster series.

The Maritime Cyber Alliance is a collaborative initiative that brings together maritime practitioners and cyber expertise with the aim of improving information sharing and awareness.

About GNS

GNS, the maritime solutions company, supports more than 12,000 commercial shipping vessels and super yachts around the world.

We use data intelligence to help our customers enhance safety, improve efficiency and reduce costs. Through our comprehensive suite of products and services, we deliver a broad range of solutions for real-time navigation, navigation management, voyage optimisation, regulatory compliance, ship-to-shore communications and cyber security.

GNS is present in major shipping hubs worldwide providing 24/7/365 support to the vessels and companies we serve.

To learn more about GNS please visit

www.gnsworldwide.com

Contact us

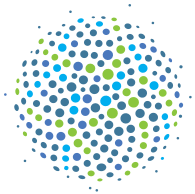
GERMANY, HAMBURG
E: DE.INFO@GNSWORLDWIDE.COM
T: +49 40 374 811 0

GREECE, ATHENS
E: GR.INFO@GNSWORLDWIDE.COM
T: +30 216 400 5000

E: SG.INFO@GNSWORLDWIDE.COM
T: +65 6270 4060

TURKEY, ISTANBUL
E: TR.INFO@GNSWORLDWIDE.COM
T: +90 216 493 74 01

UK
E: UK.INFO@GNSWORLDWIDE.COM
T: +44 191 257 2217



GNS

GNS Ltd
17 Elm Road
North Shields
NE29 8SE, UK
Email: enquiries@gnsworldwide.com

www.gnsworldwide.com