Cyber Managed & Cyber Secure

A new approach to a new maritime risk

A technology report from Bureau Veritas Marine & Offshore

BUREAU VERITAS

Technology Report #07 - Summer 2020

TECHNOLOGY REPORT

CONTENTS

Editorial Team
BUREAU VERITAS

Nick BROWN
Communications Director

Alix VALENTI
Strategic Communications Manager

Jean-Baptiste Gillet
Advanced Services Director, Marine & Offshore, Bureau Veritas

Vincent Lagny
Head of Cyber Security and Safety, Chairman of IACS Cyber Security Panel

Philippe Vaquer
Advanced Services - Cyber Security Operations Manager

Jim Clark,
Associate Director/Marine Manager, MatthewsDaniel

•

Artistic Direction
KAZOAR AGENCY

•

Cover photo credits
Dimitris Vlaikos/Bureau Veritas

CONNECTIVITY & CYBER THREATS

A connected shipping industry

Every day, at any given time, there are over 54,000 IACS-class merchant ships trading internationally. Transporting every kind of cargo across the world's oceans, these merchant ships – and the estimated million seafarers manning them – ensure 90% of world trade. If these numbers are staggering, so is the notion that these ships are now all digitalized to varying degrees and virtually connected to ports and other related infrastructure around the world through the Internet of Things (IoT).

'Things' refers to any object with embedded electronics capable of transferring data over a network. In the shipping industry, the level of connectivity differs greatly among ship owners. For large shipping companies, whose fleets handle a significant share of world trade, data is key to ensuring high levels of efficiency - it can provide valuable insights into fuel consumption, cargo handling at ports, and maintenance needs, *etc.* Highly connected ships are known as smartships.

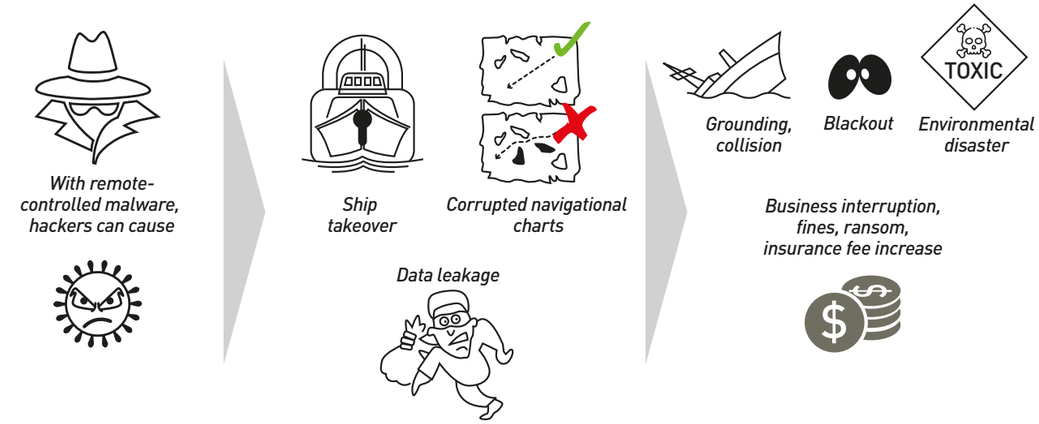
For smaller companies and ship owners, data transfer can still provide crucial information in terms of maintenance, but perhaps more importantly, for situational awareness at sea. It allows connected ships to have a full picture of the environment they are navigating and helps keep seafarers safe, preventing accidents.

A new risk threatening safety

While IoT brings substantial advantages to the shipping industry, the large volumes of data in constant flux on and among ships as well as between ships and shore also represent a significant vulnerability for ship owners and their business: connected and interconnected assets are by definition prime targets for cyber-attacks.

Critical navigation and maintenance systems, such as GPS, AIS, ECDIS, DP and PMS, can be corrupted or hijacked, disrupting vessel activity and damaging assets. Hackers can also access and expose sensitive data, and exploit system and software flaws. These attacks can have serious consequences for the safety of personnel onboard, first and foremost, but also for the safety of all other surrounding vessels and infrastructure in the event of a cyber-related shipping accident. This could even potentially have disastrous consequences for the environment as well – becoming the victim of a cyber attack and colliding with another vessel or infrastructure, leading to an oil spill.

According to the Allianz risk barometer, cyber security is the number one business risk today. In addition, a 2018 study by McCafee and Centre for Strategic and International Studies (CSIS), estimated the annual cost of such risk to the global economy to be at $600 billion in 2018. Similarly, beyond operational disruptions, recovery from cyber attacks can cost ship owners and operators dearly, both financially and in terms of lost trust from charterers and clients. As the maritime industry has seen on several occasions, the need to protect onboard and onshore systems for all types of assets is increasingly non-negotiable.



© Bureau Veritas

With an increasing number of threats to ship's connected systems, cyber protection onboard is no longer an option.

CYBER RISK MANAGEMENT

IMO 2021 Requirements

To support key maritime and shipping industry stakeholders in their fight against cyber attacks, in 2017 IMO issued two documents:

- Resolution MSC.428(98) – Maritime Cyber Risk Management in Safety Management Systems;
- The Guidelines on Maritime Cyber Risk Management (MSC-FAL.1/Circ.3).

The Resolution states that "Safety Management Systems (SMS) must include cyber risk management in accordance with the ISM Code". Consequently, Ship owners have until January 1, 2021 to integrate cyber risk into their SMS, developing key onboard procedures and providing relevant crew training.

To achieve compliance, owners need to identify at-risk cyber systems, implement comprehensive and asset-specific security procedures, detect and respond to non-compliance, and recover from irregularities. However, while the Guidelines on Maritime Cyber Risk Management issued by IMO offer high-level recommendations for maritime cyber risk management, these fall short of providing a detailed methodology or practical template for owners to follow.

As a result, with the deadline now fast approaching, it can be quite daunting for ship owners to navigate yet another regulatory requirement, especially when there is little understanding of the real vulnerabilities and risks within the maritime industry.

A brief survey of maritime industry stakeholders reveals that the language used when discussing cyber security – generally referred to as 'cyber attacks' – may lead some people to believe they may not be vulnerable to such risks. 'Attacks' could be misconstrued as a threat targeting a specific business, rather than an industry-wide threat, which could lead some owners to mistakenly believe there are no reasons why their firm should ever be exposed to such risks.

Similarly, because these recommendations and guidelines attempt to cover all types of ships, the reference points used make it difficult to identify what should actually be protected on a ship. IMO Guidelines note that vulnerable systems could include, but are not limited to "a number of vulnerable systems", and then moves on to mention in broad terms the possible "inadequacies in design, integration and/or maintenance of systems that could lead to such vulnerabilities".

IMO definitions

IMO defines *cyber risk* as "a measure of the extent to which a technology asset could be threatened by a potential circumstance or event, which may result in shipping-related operational, safety or security failures as a consequence of information or systems being corrupted, lost or compromised."

Cyber risk management, according to the IMO, "means the process of identifying, analyzing, assessing and communicating a cyber-related risk and accepting, avoiding, transferring or mitigating it to an acceptable level, considering costs and benefits of actions taken to stakeholders."


© Bureau Veritas

A BV surveyor checking hardware equipment onboard a ship

Classification and Cyber Risk Management

A classification society's guiding mission is to keep clients' crews and assets safe, every day and under any circumstances. As cyber threats present an increasing risk to safety, classification societies need to step up to provide their clients with all the support they need to ensure adequate cyber risk management for all their assets. There are three main points on areas for which such support can be provided.

Identifying the right level of protection

While IMO regulations do apply to all connected assets, there is no one-size-fits-all approach to cyber protection. Determining an asset-specific cyber management strategy is key to limiting costs and defining the right safety measures for each vessel or offshore unit.

With the help of a classification society's cyber experts, owners can define the high-level structure of their cyber security policy and develop a complete inventory of at-risk systems before assessing criticality. Experts can then determine relevant risk mitigation measures on a per-vessel basis, developing comprehensive, asset-specific procedures for Operation Technology (OT) and Information Technology (IT) systems, operational concerns and personnel training.

Achieving compliance without specific cyber or IT teams

As cyber safety and security are still new subjects for many owners, who may not have dedicated in-house cyber or IT resources, the task of choosing who should be trained, retrained or hired, as well as the organization of the training itself, can feel daunting.

By working with classification societies to define a cyber management strategy, owners can develop a comprehensive risk overview and guidelines for achieving cyber protection. In-house personnel can then undergo training to learn the risks to connected systems, and understand the mitigation measures and onboard procedures based on IMO guidlelines.

Ensuring cyber security for new stakeholders

Cyber security introduces a new set of stakeholders into the asset management ecosystem. Cyber solutions providers, IT consultants, equipment providers and others may have access to connected systems and data, which must be secured in accordance with IMO regulations.

As part of their cyber management strategy, owners should carefully define the responsibilities of all actors, ensuring that individual stakeholders understand their role. Third party verification can then be used to keep stakeholders accountable, improving the safety of data, connected equipment and systems.

In order to provide support to shipping industry stakeholders, Bureau Veritas has developed a new rule note on 'Cyber Security for the Classification of Marine Units' (NR 659). In this document, two additional class notations have been developed:

- CYBER MANAGED for cyber security risk management;
- CYBER SECURE for cyber security by design;
- Both notations also have a version applicable to yards (CYBER MANAGED PREPARED & CYBER SECURE PREPARED).

"The rise of smart shipping and increased connectivity present asset owners with both distinct advantages and challenges. Combating cyber risk will involve the entire industry, from regulatory bodies and classification societies, to asset owners and operators, to equipment manufacturers and cyber-solution providers."

Vincent Lagny
Head of Cyber Security and Safety,
Chairman of IACS Cyber Security Panel


© Bureau Veritas

© Elisa Larus, NYK Line

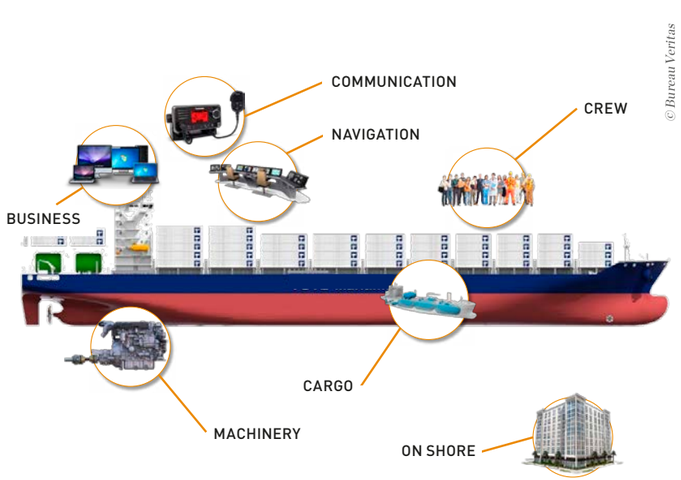
France LNG Shipping SAS (a French ship-owning company jointly owned by NYK and Geogas LNG) has taken delivery of the LNG carrier Elisa Larus from Hyundai Samho Heavy Industries in South Korea. The new vessel has been awarded a Bureau Veritas cyber security notation.

BUREAU VERITAS' CYBER MANAGED

Applied primarily to in-service vessels, this new class notation aims to support ship owners in developing an approach to cyber risk management using safety standards similar to those already used onboard. In practice, this means that CYBER MANAGED employs a risk-based methodology and standardized framework to assess and protect ships from cyber risks.

Identifying Vulnerabilities

Key to the development of an effective risk management approach is an in-depth and comprehensive understanding of all systems and their vulnerabilities. Based on this, risk mitigation measures can be determined and implemented. These are the key elements of IMO Guidelines on Maritime Cyber Risk Management.



© Bureau Veritas

CYBER MANAGED's comprehensive cyber risk management approach covers all IT & OT equipment onboard and on shore.

Cyber Repository

The first step of CYBER MANAGED focuses on providing methodological guidance and training to ship owners by developing a Cyber Repository: a comprehensive equipment and network inventory - including remote access - for each type of vessel in their fleet. While these systems are essential for the proper functioning of a ship, it is not uncommon for ship owners to lack a comprehensive picture of what these systems are, how they are interconnected and the type of onboard and onshore connections they might have.

Cyber Risk Analysis

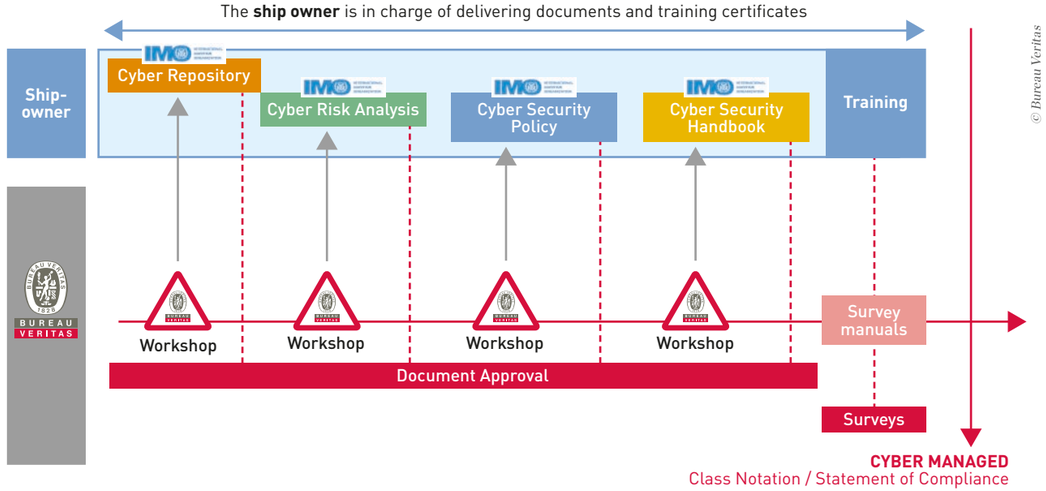
On the basis of the mapping carried out for the development of the cyber repository, ship owners are then required to undertake a thorough risk analysis of the inventoried systems. Such analysis is not limited to threats; it also assesses safety and security impacts resulting from the exposure or exploitation of vulnerabilities in IT and OT systems.

Bureau Veritas provides guidelines and tools, as well as a recognized, step-by-step methodology, to assess equipment potential vulnerabilities to cyber attacks, and consider mitigation measures that have been applied as well as those that will be applied.

© Bureau Veritas

"CYBER MANAGED is not only a tool supporting ship owners in the implementation of IMO 2021. The notation allows owners to digitalize the way onboard IT systems are managed, lowering costs and improving utilization of these systems. CYBER MANAGED encourages the development of higher standards of operations for onboard IT and OT systems."

Jean-Baptiste Gillet
Advanced Services Director,
Marine & Offshore, Bureau Veritas



© Bureau Veritas

CYBER MANAGED approach

Developing a Strong Framework

The Cyber Risk Analysis subsequently informs the development of policy and procedures for a strong cyber risk mangement framework. Working closely with its clients, Bureau Veritas helps ensure that each framework is specifically tailored to the variety of assets in the owner's fleet.

Cyber Security Policy

Bureau Veritas provides methodological guidance and training to ship owners by developing company-wide cyber rules. A ship owner's Cyber Policy will be implemented across their fleet.

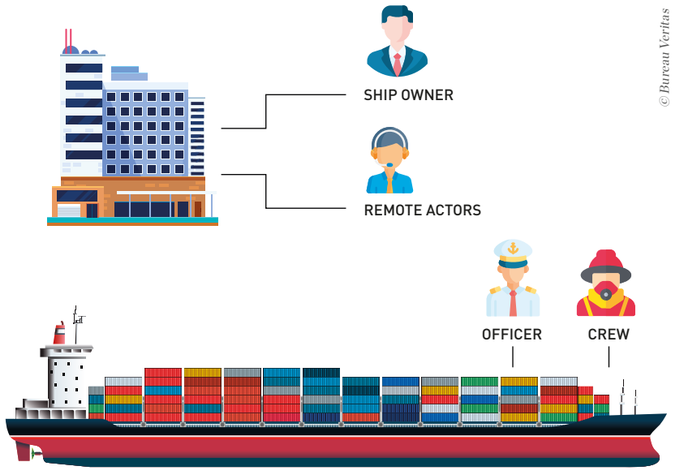
In line with IMO requirements, this policy focuses on defining:

- Cyber rules to be implemented onboard fleet vessels;
- Roles and responsibilities for cyber risk management;
- Crew training activities to ensure that all crew members are aware of their roles and responsibilities;
- Crisis management measures to guarantee efficient and effective actions are undertaken in the event of a cyber-related incident.

Cyber Handbook

The Cyber Handbook is customized to a ship and its equipment. Therefore it has to be stored and used onboard by relevant officers and crew.

Bureau Veritas supports ship owners in the development of a handbook that contains onboard procedures to enforce the Cyber Security Policy during operations and maintenance. It also provides crew with incident response procedures that meet cyber risk management standards set by the Cyber Security Policy.



© Bureau Veritas

CYBER MANAGED comprehensive cyber risk management approach covers all stakeholders onboard and on shore.

BUREAU VERITAS' CYBER SECURE

In April 2020, the International Association of Classification Societies (IACS) published a Recommendation on Cyber Resilience (No.166). The recommendation, "intends to ensure that design, integration and/or maintenance of computer-based systems support secure operation and provide means to protect against unauthorized access, misuse, modification, destruction or improper disclosure of the information generated, archived or used in onboard computer-based systems or transported in the networks connecting such systems."

In other words, IACS Recommendation No.166 encourages cyber security of ships by design. Through a provision of technical requirements, it aims to guide stakeholders toward the delivery of cyber resilient ships from the very beginning of their life cycle. A vessel's IT architecture, as well as all the systems that support it, are designed to be cyber resilient, leading to more effective management of cyber risks throughout the whole life cycle of the ship.

Bureau Veritas' CYBER SECURE offers the support ship owners need to follow IACS' technical requirements for their newbuild. Based on the same processes applied to in-service vessels under the CYBER MANAGED offer – Cyber Repository, Cyber Risk Analysis, Cyber Security Policy and Cyber Handbook – CYBER SECURE works with both shipyards and ship owners to add a 'secure by design' layer to each of these processes.

Secured Integration

To ensure that a vessel's IT infrastructure is cyber resilient, Bureau Veritas requires shipyards to identify, in the Cyber Repository, the security mechanisms put in place to handle cyber risk management.

Once the Cyber Repository, which includes cyber security mechanisms, has been developed, the shipyard needs to assess any potential vulnerability to cyber threats of the elements inventoried and evaluate the potential effects and impacts (the Design Assessment). Unlike for CYBER MANAGED, mitigation measures include the introduction of requirements for both equipment selection and on board integration, and critical equipment must be secured and approved by a classification society. Further, equipment must be installed and connected in compliance with the Rule Notation.

In addition to rules for equipment and on board integration, CYBER SECURE introduces rules for cyber security supervision that are reflected in the Cyber Handbook. These existing procedures ensure the Security Policy is followed for operations, maintenance and incident response.

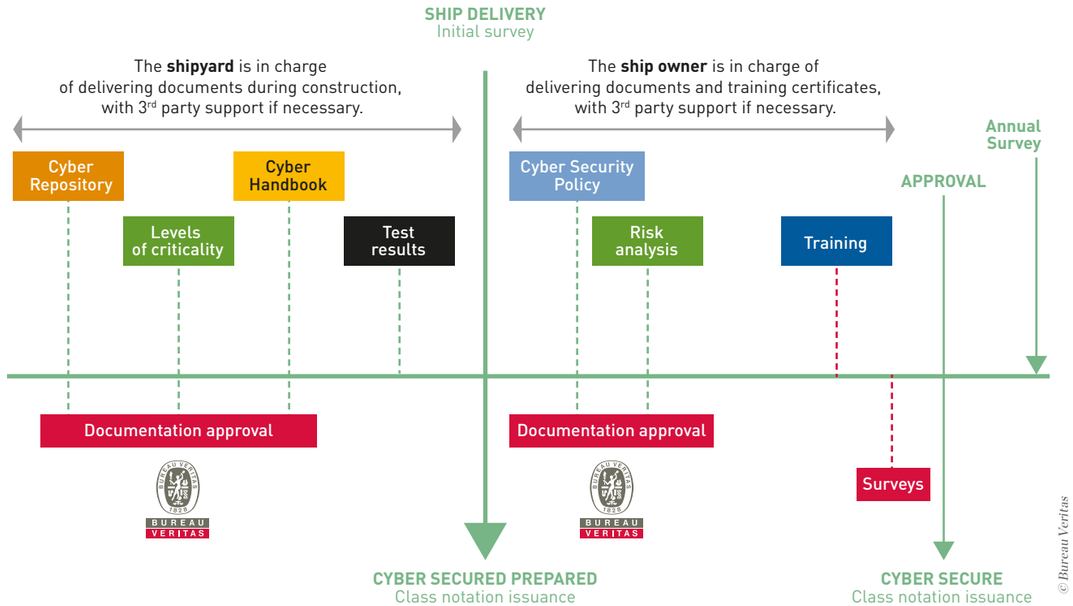
Finally, an additional layer of cyber risk management is added to the CYBER SECURE offer, as owners can request specific surveys, including penetration testing. Subsequently, subject to approval by Bureau Veritas, the CYBER SECURE notation is delivered to the ship owner.

Hardened Equipment

System hardening requires the application of best practices by the equipment supplier in order to reduce the vulnerabilities of the system. It applies to the operating system, network components, software, services, databases, virtual machine and firmware.

The core of system hardening relies on the reduction of the attack surface, by removing useless components such as applications, listening services, configuration files, hardware interfaces, files and process privileges. It also introduces active functions dedicated to activity monitoring, integrity monitoring and non-repudiation of actions.

Hardened systems dramatically reduce the odds of installation and execution of malware. They also discourage remote attackers as they provide few relevant paths of attack. Equipment hardening improves both cyber security and cyber safety, as it reduces the risk of system unavailability due to misconfiguration, process, storage or memory overload. Long-term maintenance and auditability are also greatly enhanced.



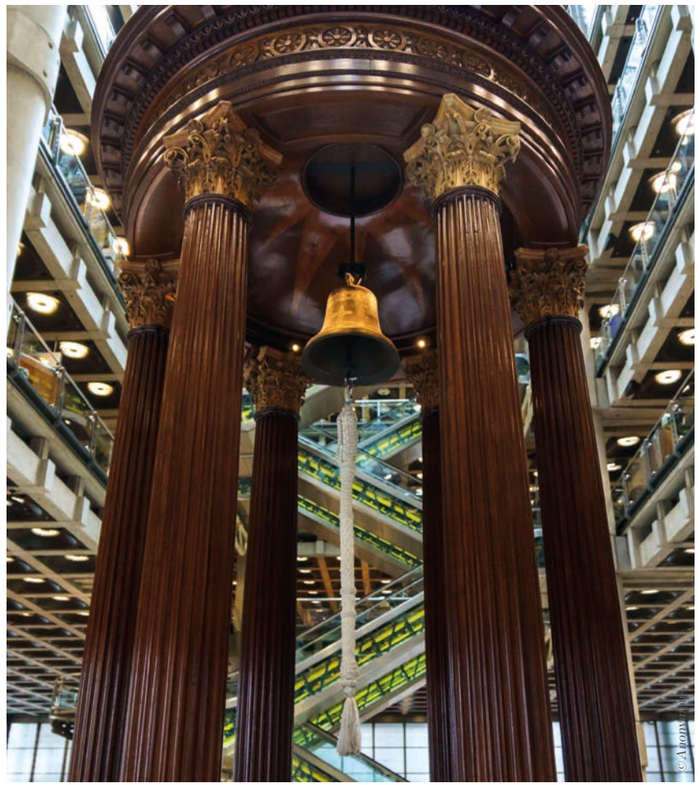
© Bureau Veritas

Cyber Secure approach

CYBER RISK MANAGEMENT & INSURANCE – A MATTHEWSDANIEL PERSPECTIVE

Hanging in the rostrum of Lloyds' of London's Underwriting Room, framed by darkened carved wood, is the Lutine Bell. Recovered from HMS Lutine on July 17, 1858 following its sinking in October 1799, the Lutine Bell came to be used by the renowned insurance and reinsurance market to inform all brokers and underwriters simultaneously when news of an overdue ship arrived in the market. It was struck once when a ship was known to have been lost, and twice for news of a safe arrival.

Although the bell has not been struck in over three decades due to a crack in the bell itself– it last heralded the return of an overdue ship in 1989 – it remains a strong symbol of risk in the Marine insurance market. At a time when shipping and insurance are increasingly reliant on data and technology, the Lutine Bell, being perhaps the most basic form of communication, acts as a reminder to all that the same maritime perils remain and that prevention and preparation are as relevant as ever to both shipping safety and insurance when cyber risks threaten potential losses.



The Lutine Bell used to be struck to signal news of an overdue ship - it remains a strong symbol of risk in the marine insurance market.

Yet, within the insurance market there is a perception that the shipping industry has perhaps been slow, in relation to other industries, in addressing exposure to cyber-related crime. This may partly be due to a lack of high profile cyber incidents having caused physical damage (PD). It is however more likely that the numerous pressing issues the shipping industry has had to navigate in recent years – from freight rates, oil prices and miss-declared dangerous cargoes, to ballast water conventions and Sulphur Cap regulations – have led to onboard cyber security risks being relegated to the bottom of the potential list of exposures for some stakeholders.

The impending deadline for the implementation of IMO's 2021 resolution comes a year after the London insurance market looked to address 'Silent Cyber', a term used to define cyber risk in existing property and liability policies that were not specifically designed to cover cyber risk – including traditional Hull and Machinery (H&M) policies in the Marine Insurance market, where the lack of clarity over the inclusion or exclusion of cyber risk leaves a certain degree of ambiguity.

MatthewsDaniel – a Bureau Veritas Group Company

Since being founded in 1962, MatthewsDaniel has been a trusted partner in the risk transfer arena. Its team of dedicated experts provides a broad range of pre- and post-risk solutions to the energy, petrochemical, marine, mining, utilities and heavy engineering industries.

Over six decades, MatthewsDaniel has innovated to continue responding to the changing needs of industry and its insurers. From geographic and technological frontiers to new insurance products and markets, the company has helped its clients meet these challenges, building trust at every step.

In an effort to unpack what 'cyber risk' may include, a number of standalone cyber policies have been developed by insurance brokers designed to affirmatively cover hull and machinery damage, loss of income and loss of hire, and crisis management expenses in the event of a cyber-related incident.

Additionally, research carried out by insurance broker Aon also highlights the fact that 50% of all cyber incidents are, whether accidentally or deliberately, caused by people. While not news per se, this finding demonstrates that technical monitoring of a breach alone will not prevent a ship-based cyber incident – the weakest part of any security regime being the human element.

Cyber threats may have been a real threat to shipping for some time, but the reality of the extent of their impact on the whole maritime industry is just starting to sink in. The looming deadline of January 1, 2021, when companies will have to produce a Document of Compliance in line with IMO 2021 resolution requirements, no longer leaves any room for delays or ambiguities. Maritime stakeholders such as insurers and leading shipping companies have already been stepping up to the challenge of addressing cyber risk management. While this may lead the way, the task of understanding the full spectrum of cyber risks in a whole fleet, and elaborating adequate mitigation measures, may remain daunting for a large number of maritime stakeholders.

In this respect, Bureau Veritas' CYBER MANAGED and CYBER SECURE are more than class notations offering verification that "cyber risks are appropriately addressed in Safety Management Systems" by ship operators. By supporting ship owners in the development of a cyber security management system, which includes a definition of roles and responsibilities for cyber risk management onboard as well as crew training to ensure performance in these roles, Bureau Veritas goes beyond IMO's 2021 resolution. In fact, CYBER MANAGED and CYBER SECURE are in line with IACS' recommendation No.166, which requires continuous crew training on cyber-related security.

With these class notations, Bureau Veritas supports ship owners and operators in taking the steps necessary to fully understand and address potential cyber risks onboard fleet vessels, and training crew to ensure that all determined mitigation measures will be applied appropriately. Reviewed and approved procedures for incident response may also prove critical in the event of an insurance claim resulting from a cyber incident.

Once they have received CYBER MANAGED and/or CYBER SECURE notations, ship owners are able to demonstrate that they have gone beyond minimum standards – beyond compliance for compliance's sake – and are effectively cyber resilient. This proactive step in mitigating cyber risk, supported by new Class notations, will also assist ship owners in presenting their Risk to both H&M and Cyber Insurers by demonstrating compliance with the best industry standards.

"No one-size-fits-all approach can be applied when adopting a cyber risk management strategy. Bureau Veritas' CYBER MANAGED and CYBER SECURE support ship owners in going beyond the minimum IMO 2021 requirements to protect their assets and their crew. For the insurance market, such practice demonstrates compliance with the best industry standards."

Jim Clark
Associate Director/Marine Manager, MatthewsDaniel

MOVING BEYOND COMPLIANCE

It can at times be difficult to fully grasp everything the notion of 'cyber', and cyber security, encompass. Cyber matters do not merely refer to hardware, software and information systems; the networks cyber systems rely on to function make them inherently intricate, and the consequences of a breach far-reaching.

The progressive development of IoT in the maritime world has brought about the expansion of complex networks facilitating the real-time transfer of data, both onboard ships and between ships and shore. In practice, this means that interactions with these networks are no longer limited to crew members or port authorities – they now include a wide variety of people and social interactions that go well beyond familiar immediate circles.

Similarly, IT and OT systems onboard are only the end of a much wider value chain. The number of systems necessary for the production of large volumes of data, and for the transfer of such data, involves a large eco-system of companies – and therefore people – that each have their own intricacies and vulnerabilities.

Such complexity in an ever changing environment means that cyber security is not about zero risk, but risk mitigation. There is no one-size-fits-all model because each ship or port has its own network and eco-system. To be efficient, cyber risk management needs to be specifically tailored to each ship owner, operator and ship type.

Bureau Veritas works closely with clients to propose solutions that go beyond compliance with IMO 2021. CYBER MANAGED and CYBER SECURE provide support to shipyards and ship owners to understand and address the complexity of their cyber systems – and the eco-system within. These two class notations verify that a ship owner has developed a full picture of the systems onboard and the eco-system of their value-chain, and that they have sought the best risk-mitigation measures to address critical vulnerabilities therein. Regular checks on the ability of ship owners and crews to efficiently implement cyber risk management practices – during annual surveys – demonstrate that Bureau Veritas also accompanies its clients through the years in addressing evolving threats.

Bureau Veritas will continue to work closely with the International Association of Classification Societies (IACS), using its practical experience to enhance cyber resilience on our own future fleets. This will be ever more relevant as we see Maritime Autonomous Surface Ships (MASS) progressively increase in our clients' fleets. Together with clients and other class societies, Bureau Veritas seeks to move beyond compliance to help save time, money, and reputational damage across the shipping industry.

BUREAU VERITAS
MARINE & OFFSHORE
8 Cours du Triangle
92937 Paris-La Défense, France