ALPHA MARINE
CONSULTING P.C.

MARINE CONSULTANTS & SURVEYORS
T: +30 211 888 1000, F: +30 211 8881039
mail@alphamrn.com | www.alphamrn.com

DIAPLOUS
Cyber

MARITIME CYBER RISK REDUCER
T: +30 216 600 7557, F: +30 210 410 1070
info@diaplous-cyber.com | www.diaplous-ms.com

WEBINAR – 04.02.2021

CYBER SECURITY IN THE MARITIME ENVIRONMENT

Questions & Answers (Q&A)

1. Do companies need to keep IT/OT inventory?

According to the relevant IMO Resolution "*Information technology and operational technology systems should be considered. The protection of information and data exchange within the IT/OT systems should also be considered... Every Company must* ***identify*** *the systems, assets, data and capabilities that, when disrupted, pose risks to ship operations".*

Furthermore, according to the instructions issued by both the Classification Society and various other industry organizations, the existence and maintenance of detailed IT/OT inventories is an important requirement. Every company must prepare a hardware inventory on its IT and OT systems and develop and maintain a register of all critical system hardware on board, including authorized and unauthorized devices on company-controlled networks. The SMS should include procedures for maintaining this inventory throughout the operational life of the ship. The company must also develop a Software inventory and maintain a register of all authorized and unauthorized software running on company-controlled software, including version and update status.

Taking this into account we consider that IT/OT inventories should not only be established but also constantly updated, in order to reflect any changes occurred to fleet and Company's systems and software.

2. How useful and necessary is penetration testing?

Penetration testing is a simulated real-time attack on a network, application, or system that identifies vulnerabilities and weaknesses. Penetration tests (pen tests) are in fact the only way to identify and quantify the relevant risks. They 'exploit' vulnerabilities and weaknesses in a Company's infrastructure, applications, people and processes.

We believe that this is exactly the main challenge i.e., to assess all identified risks to ships, personnel and the environment and establish appropriate safeguards.

Every Company should undertake a pen test to its own systems ashore (head office) and onboard with the aim to acquire a proper and trustworthy risk assessment, focusing separately on each system in order to indicate specific vulnerabilities at the input/output data level, without compromising the smooth and uninterrupted Company's operations.

Based on its results, the Company must identify and adopt the necessary corrective actions in order to successfully address the vulnerabilities identified and thus ensure cyber resilience.

The penetration test must be repeated at regular intervals in order to confirm the continuous effectiveness of the corrective actions taken.

It should be noted that Charterers, and especially some Oil Majors, now require penetration testing and this was identified as an Observation in the latest TMSA Office Audits.

3. What is the situation with insurance companies and underwriters? Is Cyber Security covered by the existing insurance policies?

Current insurance schemes as far as the cyber security is concerned cannot be considered as final. It is certain that new requirements will emerge.

Yet, it can be also considered as certain that Shipping Companies will have to enact due diligence in order to be insured. Insurers will need to become aware of the Company's operation procedures, the applied protection measures and whether it has adequate procedures and mechanisms to effectively deal with a cyber-attack. In this respect, the relevant insurance premium will be adjusted based on the above principles.

4. Do charterers require the implementation of specific terms in charter party agreements?

Discussions at BIMCO regarding the requirements that will be included in the charter parties are still ongoing. So far though, some Oil Majors have started to provide special Cyber Security related terms in their proposed charter party agreements. These terms refer to the conduct of penetration test ashore and onboard, enhanced procedures on Cyber Security and handling of cyber-attack incidents, as well as the obligation to immediately inform the charterer and the competent authorities, Flag etc.

Based on the above, we could say that soon all charter party agreements will include such new requirements.

5. What is the role of the IT Department, whether it is in house or not? What is its connection with the other departments of the Company?

We believe that companies are still struggling to make cybersecurity a vibrant, proactive part of strategy, operations, and culture. The root cause is twofold: (1) Cybersecurity is treated as a back-office job and (2) most cyber leaders are ill-equipped to exert strategic influence.

Historically, companies have expected IT Officer to focus on technical tasks — and haven't expected more of them. Cyber leaders have the monstrous and all-important goal of securing a business, but when companies make big, strategic decisions — about business models, digital strategy, etc. — cybersecurity is an afterthought. That means companies are losing out on the value that the function can provide. This approach was acceptable in the past, when threats were slower and less complex, but it is no longer sufficient. Today's cyber leaders must be able to embed security throughout the company's operations, rapidly respond to threats, and influence fellow senior leaders. In short, they must be able to lead.

IT Department role must be enhanced, connected with all other Company's departments and ships and actively participate in the decision-making process. If a Company wants to adjust to this new reality, the Company's Top Management must understand the new era and invest money and resources to cyber security. Preserving Cyber Security is not a technical issue any more; it is a central process directly linked with company's and fleet's business continuity.

On the other hand, though, IT department personnel must also realize the new challenges, act beyond the purely technical/supportive role and adopt a "holistic" approach and ability. They must promote a new culture through practices and procedures, which should be embedded across the Company, accepted by all staff and interconnected with all other existing procedures.

Cyber Security must become part of the day-to-day operation of the Company and be integrated into the Company's Safety Management System. This requires the "commitment" from the Company's Management.

Based on the above, we believe that the role of the IT Department and the Information Security Officer (ISO) of each Company should be strengthened. Employees' duties and responsibilities must be also reconsidered, with emphasis on risk and crisis management. Respective tasks – linked with cyber security - must be assigned to all employees (emergency response team, etc.), so that all participants can successfully perform their duties, aiming to deal with any relevant incident with the least possible adverse implications and the rapid recovery to reality.

6. What are the requirements of the various Port State Control Authorities and the US Coast Guard regarding the implementation of Cyber Security procedures?

The USCG has recently published the cyber security requirements which will be checked onboard all vessels calling US ports during the USCG inspections.

USCG considers the proper implementation of the cyber security procedures as one of the criteria of the ship's seaworthiness. Vulnerabilities can be created by accessing, interconnecting or networking numerous systems critical to the safety and security of shipping and protection of the environment - these can lead to cyber risks which should be addressed. Cyber vulnerabilities can have an impact on Safety and Environment and Cyber risks can affect seaworthiness.

In this respect a ship that does not comply with the Cyber Security regulations will not be considered as seaworthy. This means that for the purposes of the Port State Control requirements, Cyber Security is emerging as a basic and mandatory requirement, equivalent to SOLAS, MARPOL, etc.

7. Do we expect Flag States instructions for implementing cyber regulations?

The majority of Flag States will issue or have already issued their guidelines on cyber security. These guidelines aim at what we call "compliance". However, the most important requirements will come from the charterers/Oil Majors and the insurance market.

Finally, we must not forget that increased requirements have already been included not only in the TMSA, but also in the DryBMS for Bulk Carriers.

8. How should a cyber incident be handled? Is there a similarity with the typical "marine incident"?

The modern Company's Safety Management Systems categorize the various emergencies based on their severity and consequences. Each category of incidents leads to specific actions to be undertaken within specific time frame. For high-risk incidents the Company must notify the ship's flag, coastal states, and other competent authorities as well as charterers.

The same principle needs to be followed for the Cyber Security incidents. The Company's Cyber Response Plan must be aligned with the existing Emergency Response Plan.

An effective incident response plan ultimately relies on executive sponsorship. Given the impact of recent breaches, we expect incident response to move higher on the executive agenda. Putting the development of a robust plan on the fast track is imperative. When a successful cyber-attack occurs and the scale and impact of the breach comes to light, the first question customers, shareholders, and regulators will ask is, "What did this company do to prepare?"

With cyber criminals successfully targeting organizations of all sizes across all industry sectors, organizations need to be prepared to respond to the inevitable data breach. A response should be guided by a response plan

that aims to manage a cyber security incident in such a way as to limit damage, increase the confidence of external stakeholders, and reduce recovery time and costs.

Many companies do have response plans but don't truly operationalize them. Often, the documentation prescribing how to act in the event of a cyber breach is out of date, inaccessible to key decision makers, generic, unhelpful for guiding specific activities, or some combination of the above. In many cases response plans aren't integrated across business units. Developing individual plans in silos inhibits the sharing of critical information and best practices This may lead to lack of coordination during large response efforts.

Furthermore, too many plans sit idle. Organizations that are highly conscientious about practicing fire drills fail to rehearse the steps they would take in the event of a data breach.

Moreover, in order for a Company to ensure personnel familiarity with the newly developed procedures, it is required to perform drills and readiness exercises which can be combined with the existing drills and exercises. It goes without saying that the effective handling of a cyberattack is dependent on company's personnel awareness and preparedness to respond.

9. What are the advantages provided by the cooperation of DIAPLOUS-CYBER with ALPHA MARINE CONSULTING?

From the early stages of our involvement in this area we understood that our industry needs a holistic approach which can be summarized in the 5 main pillars described in the relevant IMO Circular i.e., to:

1. Identify
2. Protect
3. Detect
4. Respond, and
5. Recover

Our cooperation aims exactly in providing a holistic solution of Cyber Security issues, and combines the ingrained experience of each Company in their respective expertise fields, thereby allowing us to deliver high quality services by providing the requisite advanced methodology to implement risk management measures, to establish robust cyber protection management system procedures, as well as a well-secured risk assessment framework, in order to ensure enhanced protection against cyber risks.

In case of a malfunction or threat, the customized procedures and operations shaped according to each Company's technological infrastructure and needs, guarantee Business Continuity by:

- Responding to the cyber incident
- Recovering the Company's systems
- Restoring normal operations
- Ensuring Company's assets (including personal data) and operational integrity
- Protecting Company's business continuity and reputation, and
- Establishing an effective Cyber Risk Management, Cyber Incident and Crisis Management.

Contact

For more information about DIAPLOUS-CYBER, please:

- Visit our website and subscribe our newsletter at https://diaplous-ms.com/index.php/cyber- security/
- E-mail us at info@diaplous-cyber.com
- Call us at +30 216 600 7500 (standard working hours, UTC+2)

For more information about ALPHA MARINE CONSULTING, please:

- Visit our website: https://alphamrn.com/
- Email us at: mail@alphamrn.com
- Call us at: Tel: +30 211 888 1000 (standard working hours, UTC+2)