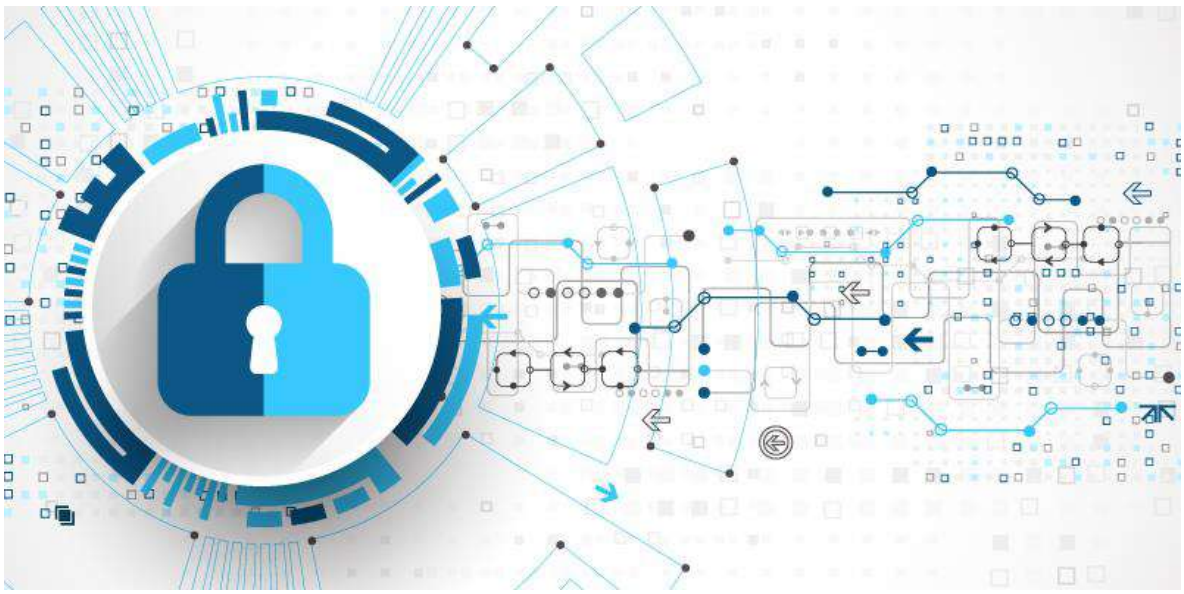
CYPRUS SHIPPING CHAMBER
Navigates Cyprus Worldwide

CYBER SECURITY CASE STUDY



(Version 1.1 – July 2017)

Published by
Cyprus Shipping Chamber
City Chambers, 1st Floor, Regas Fereos Str.
Limassol, Cyprus
www.csc-cy.org

Terms of Use

Table of Contents

1. Introduction

As the industry moves into a smart-shipping era, the risk of cyber threats is at an all-time high. Digitalised ships, increasing interconnectedness, the extended use of electronic data exchange and electronic navigation increases the likelihood of cyber-attacks in variety, frequency and sophistication. Cyber threats are one of the most serious economic and international security challenges facing the maritime industry today. The need for protection and security enforcements to mitigate the threats is more important today than ever. Guidelines to support secure cyber operations and contingency plans to be followed in a case of cyber incident have become necessary.

The Cyprus Shipping Chamber recognising the increasing concern of its Members with regards to the cyber security and their protection, developed this document with the intention to create awareness of the threat and provide guidance to its Members.

2. Aim and Scope

This case study was prepared to show a 'real life' snapshot of a company that is a Ship owner, Technical-Operations Manager, and Crew Manager and how they, in the early stages, are evaluating and implementing a program of cyber security for their ships with Online Connectivity.

We have posed several general questions to the company on general subjects to help scope how this company is initially viewing cyber security, and their efforts to organise internally by assigning responsibilities and allocating resources of staff and budget. Comments are made at a high level and are included under the section "Further Consideration". They have been purposely general in nature to help identify certain concepts that may be of help.

It should be recognised that this is not an all-inclusive guidance or evaluation, and does not critically assess their efforts. It is rather intended to contribute to the greater discussion of maritime cyber security by exposure to what is likely a typical case and find some value to their cyber security efforts.

Comments are encouraged to the Cyprus Shipping Chamber to improve this document and to better prepare for future case studies on this subject.

3. Company Description

Question: Describe your company in terms of fleet size, ship types, number of employees, and number of offices worldwide.

Company comment:

"We own and/or operate over 100 ships which include tankers, bulkers, and container ships. We employ directly over 3,000 employees in seven offices worldwide. The company operates as an owner and technical operator, including crewing services".

4. Motivation

Question: Why is your company implementing cyber security?

Company comment:

"Driving this shipping company's cyber security initiatives is the increasing awareness of the invasive nature of cyber-criminal activity in the shipping industry. Cyber threat has imposed an elevated cyber security related risk awareness from ship owners, the company board of directors, cargo owners, and legal / regulatory bodies such as TMSA, IMO and USCG to name some, as well as P&I club coverage".

Further Consideration:

4.1 "Reducing the risk should be the main deliverable of the company's cyber security strategy and outcome of the risk assessment decided by senior management. At a technical level, this would include the necessary actions to be implemented to establish and maintain an agreed level of cyber security." 1

4.2 Ships entering / leaving management pose added challenge to maintaining a uniform application of a cyber security program as each ship differs in communication systems, ship technology, and operations budget. Efforts to establish a fleet wide standard cyber security strategy is an efficient way to maintain a consistent and effective level of defense and response across a fleet. "A further complexity is that shipping lines operate a mix of vessels which they either own or charter for a short period of time…".2

4.3 Company employees, port agents, service vendors, equipment manufacturers, and crewing services do introduce a significant cyber security risk for a ship's commercial operations due to the large number of persons routinely visiting the ship or joining as crew. These ship visitors are often routine in nature and are left minimally monitored while they complete their tasks onboard. There is no company cyber security policy in place for ship related services that use the ships network.

4.4 Knowing who is using your ship network and for what purpose is important and a real concern relating to cyber security. Discovering early malicious intent, unintentional mistakes, or poor cyber security practices are a risk that needs to be addressed. Ship network monitoring and analysis is one way to have this capability.

4.5 There is a need to have a clear policy and practical procedures for all crew and visitors who use the ship's network in the cyber security policy and proper use expectations.

4.6 Cyber Incident insurance coverage will grow in importance as a part of a company's risk management strategy. Underwriters will require certain cyber security standards and routine audits for

1 "Guidelines on Cyber Security onboard Ships" (BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO) pg. 12

2 "Threat Assessment: The cyber threat against the maritime sector" Centre for Cyber Security (Denmark), March 2017, pg. 2

coverage. Using their assessment and audit standards is a good start and should be reviewed for applicability to your cyber security strategy and for possible future insurance coverage.

5. Driving Cyber Security for the Fleet

Question: Why is your company implementing cyber security in its fleet?

Company comment:

"Currently, the company is undergoing a transition from the current Fleet Broadband communication services to a higher broadband capable VSAT system. This 'open to the internet' situation will drive the company towards more vigilance and the need for a Cyber security program to be put in place".

Further Consideration:

5.1 "The rapid development in maritime broadband satellite coverage combined with the introduction of highly sophisticated equipment, such as computer controlled engine systems, has changed the structural risks to maritime vessels. Ships are no longer protected by an air-gap from external systems. Today, an estimated 30,000 vessels globally have equipment providing them with constant internet access, which is an increase from only 6,000 in 2008. Even if networks on board are separated between systems for ship operation, crew welfare and remote access to suppliers, separations can over time be compromised by ad hoc interventions by the crew or suppliers, for instance in connection to maintenance…".3

5.2 "Cyber security refers to the security of information networks and control systems and the equipment and systems that communicate, store and act on data. Cyber security encompasses systems, ships and offshore assets, but includes third parties – subcontractors, technicians, suppliers – and external components such as sensors and analytic systems that interface with networks and data systems. This includes human interaction of crews and other Company personnel, customers and potential threat players. In such a dynamic system, cyber security is an evolving set of capabilities inside the Company, developing and adapting as technology and threats evolve." 4

6. Moving to VSAT from Fleet Broadband (FBB)

Question: How does VSAT broadband change your view of ship cyber security?

Company comment:

"The VSAT broadband ability allows ships to have direct connection to the Internet, therefore exposing them to its dangers. As a result of this, and because of the increasing cyber-attack incidents around the world, this is motivating this company to be more vigilant on this matter".

Further Considerations:

6.1 It needs to be noted that FBB and VSAT have in-common cyber security vulnerabilities as each is connected to the internet. FBB is likely a risk as the systems protecting the network are commonly older firewalls that are left with the default configuration and have never been updated. Compounding the risk

3 "Threat Assessment: The cyber threat against the maritime sector" Centre for Cyber Security (Denmark), March 2017, pg. 2

4 GUIDE FOR CYBER SECURITY IMPLEMENTATION FOR THE MARINE AND OFFSHORE INDUSTRIES, ABS CyberSafetyTM VOLUME 2, September 20, 2016, pg.ii

is the prevalent infrequently updated antivirus and out of date operating systems on computers. Cyber threats will most likely come from within the ships network from a vendor or the crews use of personal computers from virus emails, phishing, improper content downloads, to name just few threats. The ships network needs to be mapped and all critical systems need to be assessed for vulnerabilities. Penetration tests are a good check on the existence of vulnerabilities so that corrective actions can be prioritised.

6.2 When malware is introduced into a computer or ship system connected to the network, a common action of the malware is to establish a covert command communication outward. The result is possible system encryption, exfiltration of data, and a number of other serious exploits. These types of communications are potentially not identified by antivirus or ISP scanning as a threat.

7. Ship Cyber Security Company Administration

Question: How is your company addressing ship cyber security policies and procedures? Is it part of your ISM and Quality System - for example?

Company comment:

"A cyber security committee has been established, and is in the process of creating ship and office procedures with regards to cyber security. This will be an ongoing and constantly updated procedure".

Further Consideration:

7.1 In this case the Board of Directors (BoD) has made cyber security a priority for the office and fleet and tasked the management to formulate a strategy starting with a Cyber security Committee to communicate with the BoD, study cyber security 'best practices', provide recommendations, and implement approved actions.

7.2 It is a good start that the ship and office are working together as there is a common threat risk from one to the other. It is a challenge if there is the passing on of cyber security to an unprepared crew without reasonable guidance, assigned responsibility, and at least basic knowledge of the ships networks and hardware.

7.3 When implementing 'best practices', cyber security policy and procedures it should be incorporated into the Quality and Safety Management system to ensure ongoing improvement.

7.4 Cyber security implementation on ships, not supported by clear and understandable policy, procedures, and audit will lessen the effectiveness of the cyber security program. Assigning responsibility and direct communication channels is essential.

7.5 A clear message of the company policy and expectations from senior management to all of the company staff and crews and especially its vendors and suppliers is critical to set an acceptable level of cyber security companywide. The risk is that over time the trap of a lethargic message will lead to a weak cyber security culture.

7.6 Approval of a strategy and a budget are a must and should be addressed at the highest management level of the company.

7.7 "Company plans and procedures for cyber risk management should be seen as complementary to existing security and safety risk management requirements contained in the International Safety Management Code (ISM) Code1 and the International Ship and Port Facility Security (ISPS) Code2. Cyber

security should be considered at all levels of the company, from senior management ashore to crew on board, as an inherent part of the safety and security culture necessary for safe and efficient ship operations." 5

8. Ship Cyber Security Threat Prevention and Defense

Question: What are your general thoughts, and what are you doing towards cyber security prevention and defense onboard?

Company comment:

"Part of our philosophy is to be proactive; therefore, we have in place a few preventative/security measures. These are firewalls, internet filtering (for vessels that already have internet access), standalone PCs which contain sensitive information, and security software that locks the PCs requiring passwords to unlock them (as well as antivirus)".

Further Considerations:

8.1 Ships' Captains and officers have basic knowledge of cyber security from their experiences off the ship. Many are relatively knowledgeable and can be of a great assistance when needed if given the proper instruction, and responsibility to assist the shoreside person responsible for cyber security. However, there are many Captains and officers that do not have this knowledge and require assistance to gain the confidence and understanding of what you will expect of them.

8.2 "Many systems are only capable of recognising and blocking known threats. Unfortunately, the pace of innovation in the malware world is increasing, zero day exploits are common, and a strategy that relies exclusively on a perimeter defense designed to filter out known threats will not be successful…" 6

8.3 Perform Ship Penetration Tests and Vulnerability Assessments routinely across a sample of ships in the fleet, rotating the ships being tested across the fleet. Combining your own assessments with the assessments by experienced external cyber security experts is a 'best practice' and will provide a more useful evaluation.

8.4 Define in simple terms policy, procedures, and the person responsible for Service/Vendor network access onboard. Make this known to your vendors for inclusion into their ship visit requirement. Identify in advance vendor's emergency contacts for all critical systems.

8.5 IT related investment towards hardware and software updates to the office and fleet is important to undertake as soon as possible. A 'set and forget' cyber security program based on hardware and software hardening has been proven ineffective in many industries worldwide giving a false sense of security. Cyber security is an evolving threat and requires flexibility and ongoing efforts.

8.6 A program of upgrading computer systems and networks onboard with hardware 'useful life' is generally absent for ships. Ships have notoriously outdated computers, containing unsupported operating systems and software. Additionally, unauthorised installed software is a recognised problem and is a major contributor to virus and malware system wide.

5 The Guidelines on Cyber Security onboard Ships, Ver. 1.1, Feb. 2016, Pg. 1 (Published by BIMCO)

6 Cyber Risks in the Marine Transportation System, The U.S. Coast Guard Approach https://www.uscg.mil/hq/cg5/cg544/docs/USCG_Paper_MTS_CyberRisks.pdf

8.7 Remove all unapproved software and hardware from a ship's PC and networks and perform scheduled periodic checks as part of the defense hardening and maintenance. As this is a difficult task there must be an identified member of the crew responsible for cyber security onboard with a clear process for reporting to the cyber security person in charge ashore.

8.8 Set clear and enforceable ramifications for failure to follow policy or a maliciously act, which should be part of the cyber security policy.

8.9 A ship management company has many different business relationships, types and scope of management. It would be recommended to have a cyber security standard that is offered to all ship owners/managers across fleets.

9. Ship Response

Question: Describe how a ship cyber security event may be handled? Who is the person ashore? Who has overall responsibility for the ship's cyber security?

Company comment:

"The Communication department will be responsible to handle a ship cyber security incident onboard the vessel and the subsequent actions taken will be dependent upon the nature of the event".

Further Consideration:

9.1 Company should have a comprehensive cyber security emergency response plan in place onboard and ashore. With all related response functions such as the emergency response team, initial contact procedures, and internal company management ownership.

9.2 Create a support team of 3rd party cyber security experts that understand how a ship network is structured and what critical systems are at risk. It is recommended to develop a relationship in advance, and to understand their capabilities and scope of service. It is prudent to establish service agreements in advance.

9.3 A ship cyber security officer should be nominated to perform as the 'person in charge' and responsible for initiating and supporting the response and remediation. It is not recommended that the Captain undertakes this responsibility as in such an event the Captain's duties are on ship safety matters and response and remediation requires continuous communications and focused attention. A candidate for this responsibility is the Ship Security Officer.

9.4 Develop a detailed emergency contingency process as part of the Cyber Security Incident Plan that includes the communication and coordination between the ship and office. Simulating an attack with a ship in a form of a cyber attack drill is something to consider.

10. Cyber Security Updates Onboard

Question: What are your thoughts and what are you doing to keep antivirus software, computer patches, and systems updated onboard?

Company comment:

"A system, in order to be as less vulnerable as possible, it needs to be as up-to-date as possible. For the time being not all our vessels have internet access, therefore we update our computers by sending CDs with updates, links with updates to next port agents, as well as during attendance by the Communication team members. Once a VSAT broadband solution has been installed on board, the updates will be pushed to the vessels from the Communication dept. via the internet".

Further Consideration:

10.1 It is important that antivirus updates and software patches across the fleet be performed frequently, routinely and tracked. Dependence on port agents and other unscheduled visits by the communication team creates the risk that some ships will be updated more frequently and some not at all. At the very least a schedule and tracking method needs to be in place to ensure that updates are completed.

10.2 Assigning a person to be responsible for the updates and reporting completion to the shore cyber security person in charge is a recommended minimum standard. In this current scenario it is likely that the Captain is given the updates and is the person relied upon to make the updates. It is not a good policy to place this added responsibility on the Captain and unfortunately this is exactly what is happening in many fleets.

10.3 A process to put in place the most current PC operating system software on all computers onboard is a critical need. Using outdated, possibly unlicensed, unsupported software is a known high cyber security risk that can be corrected with management policy and controls as part of the company Quality System.

10.4 It is recommended that a shipboard PC replacement policy be put in place where old and outdated hardware is replaced, based on the expected life of the hardware.

11. Monitoring of Log Files and Alerts

Question: Describe who will be responsible and will review vessel / office cyber security reports, log files, and alerts.

Company comment:

"The Communication dept. will be responsible for vessels, and will review security reports, log files and alerts. It will cooperate/liaise with the company's IT dept. and our Internet Service Providers (ISPs) if needed. The requirement of a 3rd party to assist in the analysis and threat potential and level, will require risk assessment coupled with financial impact both to pay for it and the impact as a result of an attack".

Further Considerations:

11.1 Reviewing security reports, log files and alerts is a specialised ability requiring a cyber security analyst to be most effective. The large number of false alerts and unidentified threats alerts can be significant. It is a risk that this daily task will likely result in the process not being done consistently, systematically, and dependably due to time and resource constraints of a small staff covering a large fleet.

11.2 Cyber security is far more reaching and 'holistic' in nature. Using best practices would include such functions as Security Information and Event Management (SEIM). It is recommended to seek third party assistance for monitoring and analysis to avoid a false sense of protection from cyber security threats as they emerge.

11.3 ISPs are not in the business of cyber security and generally depend on third party providers to provide this specialised service. Most ISP offer some scanning and content filtering but not a comprehensive cyber security service. Using an ISP is also susceptible to creating additional levels of separation between you and the problem for notification and correction.

12. Antivirus

Question: Describe how you will be using antivirus. Updating it from your office using USB, auto update from the AV provider or using an updating service?

Company comment:

"The antivirus solution will be updated automatically using auto update".

Further Considerations:

12.1 Antivirus can detect malware that is known but cannot detect a low volume (not wide spread) malware or a new form of malware attack.

12.2 Antivirus generally cannot detect covert channels often used by malware. To put this into perspective, with penetration tests antivirus rarely causes trouble meaning it doesn't detect the covert activity on the computer such as ransomware. Overall Antivirus will not protect you from the attack that matters most.

12.3 Consider when the antivirus has failed and has been compromised. Most current malware is set up to deactivate the Antivirus software. Additional monitoring protection is needed to know when antivirus has failed or deactivated.

12.4 The concept that Antivirus, firewalls, and ISP content filtering is a sufficient level of cyber security for ships is a misconceived notion that is prevalent in the maritime. Knowing how your network is used and learning what a normal activity is, is important. Monitoring and a deep level of analysis is a service that can contribute to improved cyber security.

13. Third Party Assessments

Question: You are, or are intending to use third party services. Which services are you looking to do this? Entirely with current IT and communication dept. staff?

Company comment:

"The Communication dept. has a member with a Master's Degree in Cyber security, while two of its members have earned their Certified Ethical Hacker (CEH) certification. We are planning to assess possible events using our currently 'Cyber-security aware' staff, whilst being open to third party assessments depending on findings".

Further Considerations:

13.1 Third party penetration and vulnerability testing should be part of the business process and is generally considered an industry best practice. It is prudent to use a few different providers to get a balanced assessment, as assessments can vary from provider to provider.

13.2 Cyber security to be effective needs to be internally and externally 3rd party tested. Corrective actions from these tests and audits needs to be in place.

13.3 "It is recommended that a shipping company initially performs an assessment of the potential threats that may realistically be faced. This should be followed by an assessment of the systems and procedures on board, in order to map their robustness to handle the current level of threat. These vulnerability assessments should then serve as the foundation for a senior management level discussion/workshop. It may be facilitated by internal experts or supported by external experts with knowledge of the maritime industry and its key processes, resulting in a strategy centered around the key risks."7

14. Cyber Security Hardware

Question: Describe what hardware you are intending to use. Purchase or lease, or obtain as a service.

Company comment:

"As mentioned earlier, the hardware that will be used are firewalls along with the provider assisted shore side URL filtering technology".

Further Considerations:

14.1 Care should be taken with the selection of a firewall as not all are created equal and commercial grade 'next generation' firewalls is a must. Notably, there is a wide margin of mistakes with firewall initial settings and the ongoing updating of configurations as new threats appear. It requires specialised knowledge when configuring firewalls.

14.2 Timely fleet wide firewall configurations are a must. Firewall updates across a fleet can be problematic when different models and brands are used. It is recommended that selection of hardware across the fleet be standardised.

14.3 A reasonable level of security that is a 'best practice' is 3rd party monitoring, analysis and alert processing should be on the SIEM using data streams from the firewall and IDS.

14.4 There is often a false notion that cyber security can be entirely handled adequately 'in-house'. This can be a hidden risk as it has been proven that internal teams often resist transparency over time. It is necessary that the company Cyber security Committee' seek out, vet and contract 3rd Party Cyber security expertise to conduct audits of the cyber security systems.

15. Satellite Communication / ISP Services

Question: Are you looking to use the satellite communication / ISP provider as your cyber security provider? If partially to what extent?

7 "Guidelines on Cyber Security onboard Ships" (BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO) pg. 7

Company comment:

'Our satellite communications providers will take part in enforcing our cyber security policy, by blocking specified senders/domains, providing email filters, filtering websites, etc.'

Further Considerations:

15.1 Ensure that the alert communication procedure and reporting is as direct as possible and in accordance with your response expectations.

15.2 ISP filtering is an automated process and its effectiveness is susceptible to exploits newer than the latest update. It is reliable but not infallible especially when the exploit originates onboard.

15.3 Be especially careful with an ISP providing cyber security and to what scope it provides support. Commonly an ISP will use a 3rd party cloud based cyber security provider contracted to them. Notification of routine and serious alerts will likely be separated from you by several degrees where the 3rd party provider notifies the ISP who notifies you. Your questions and requested actions can be delayed. Additional charges for the 3rd Party provider services are likely. Additional service support should be clarified in advance.

16. Crew Online Behavior

Question: How does your company address controlling and monitoring of safe crew internet use?

Company comment:

"The internet usage and access will be controlled and supervised by our ISP according to our policies whether the crew are paying for these services or not. In the interest of our company's security and integrity, we will decide what access they have. Crew access to the internet is a privilege not a right (at the moment)".

Further Considerations:

16.1 An ISP can provide filtering and scanning of the data stream. They can assist in blocking access to known malicious sites; however, they cannot effectively monitor user activities onboard.

16.2 Training the crew on good cyber security practices and cyber security awareness is recommended.

16.3 Corrective actions are a key aspect of cyber security. Proactive advice needs to be part of your strategy.

17. Ship Network Design as it applies to Cyber Security

Question: How are you limiting critical system access? Such as Network isolation etc.?

Company comment:

"There will be two separate networks that will have no access to each other. One will be the crew and the other will be the business network. Moreover, standalone PCs are currently being used to prevent access/infection in case of a compromised network".

Further Considerations:

17.1 When determining that networks are separated it is very often a false assumption. Only a penetration test will prove that getting from one network to the other is not possible. Cyber attackers

think very differently than IT people and know how to exploit the most thoughtful effort for network isolation.

18. Training

Question: How are you addressing cyber security training?

Company comment:

"The Communication officers attended the CEH (Certified Ethical Hacker) training and received their CEH certificates. Seminars and forums are attended in order to keep updated and gain further knowledge. The Captains are informed and instructed during briefings and vessel visits regarding cyber threats, phishing, and other techniques used with malicious intent."

Further Consideration:

18.1 "Communication or Connected - Crew Connectivity Survey. Only 12% of crew had received any form of cyber security training. In addition, only 43% of crew were aware of any cyber-safe policy or cyber hygiene guidelines provided by their company for personal web-browsing or the use of removable media (USB memory sticks etc.). Perhaps unsurprisingly, given the above statistics, 43% of crew reported that they had sailed on a vessel that had become infected with a virus or malware."8

18.2 Provide Cyber security training and network and hardware familiarisation for the person in charge of cyber security onboard. As the representative onboard confusion can be avoided and quicker restoration can be achieved.

18.3 Making an informed and responsible assignment of ship related cyber security responsibilities is of particular importance. The Captain is on the path to be the default person responsible for cyber security policy enforcement and incident response. This is risky as the Captain is overall responsible and he is now being assigned with one more responsibility mandate without time to manage it properly. Assign and train an appropriate Ship Cyber Security Officer with this responsibility.

18.4 Crew cyber security awareness and good cyber practice training needs to be part of the company training program. Use of eLearning and classroom cyber security awareness training of the crew is prudent as it is especially common for crew to bring their own devices onboard thus raising the risk of introducing malware.

18.5 An important part of any cyber security program is awareness training ashore and onboard. Additionally more advanced training needs to be provided for the persons with cyber security responsibilities. It is not effective if only the shore staff has such training. It is very important that the ship officers have practical and responsible training.

18.6 Use company sponsored information programs such as company newsletters and posting of awareness materials in common areas of the ship to help contribute to building an ongoing company culture of cyber security awareness.

18.7 Make 'good cyber security practices' a clearly understood responsibility for all new employees of the company and for all new crew joining a ship.

8 Futurenautics.com, "Communication or Connected - Crew Connectivity Survey" This article appeared in the October 2015 issue of Futurenautics.

19. Ship Cyber Security Incident Plan

Question: Describe what your cyber security response plan includes e.g. Initial action, Response, Media crisis, support vendors.

Company comment:

"Once the Communication team is notified, the vessel is contacted to assess the situation/damage. At the same time, the vessel's airtime provider is contacted and kept in the loop. Depending on the situation, we will advise the vessel accordingly. Actions may include remote/phone support, or attendance if needed. The company is in the process of developing a quick response plan".

Further Consideration:

19.1 Broadband offers the opportunity for remote incident response including but not limited to in situ system forensics and remote remediation. This process needs to be outlined in a "Ship Cyber security Response Plan" and prepared for in advance.

19.2 The Ship Cyber security Incident Plan needs to identify 3rd party support and these resources need to be prearranged and the ship's network details need to be pre-prepared and available for use.

19.3 A Company Cyber security Incident Plan needs to be in place for the company to respond to multiple scenarios where the ship is experiencing operational and critical data system exploits.

19.4 Each ship should have all vendors that have critical data dependent systems identified and their emergency contact information for response and restoration.

19.5 Companywide and fleet wide cyber security response planning and drills need to be in place and part of the company's emergency planning. Critical to this is media communication to provide a clear and appropriate message for the commercial relationships and the public.

20. Recovery

Question: Describe how you would backup and restore the ship network?

Company comment:

"Important data located on the vessels' network and the captains' PCs is backed-up once per week on an external hard drive that is kept safe by the captain. If needed the data can be restored using the external hard disk. The company's communication department has experience with frequent network failure for many different reasons, the procedures they have in place to get a vessel up and running will be paired to a Cyber Security issue. The restoration process will be customised to suit such a situation".

Further Consideration:

20.1 Captains often use their private laptops rather than the ships designated computer which raises the question 'Is ship data and records being transported off the ship?'. Policy needs to be clear about use and storage of sensitive data control.

20.2 There should be a defined person responsible for maintaining these backups and a procedure for frequency of the backup, and policy and procedure for the backup.

20.3 Since this portable backup drive can potentially contain sensitive information it should be protected by encryption and kept in designated secure locked location.

Continuously connected external drives can be exploited by malware. It would be prudent to use a secure backup system for all ship network systems to address this risk.

21. 3rd Party Assessments

Question: Describe if you are or intend to use third party vulnerability assessments onboard.

Company comment:

"As we said before we will do a vulnerability assessment by ourselves and if it is needed we will consider the possibility also use a third party vulnerability assessment. The cost and risk assessment will ultimately be decided upon by our senior management and CFO, based on the advice given by the Cyber Security committee".

Further Consideration:

21.1 Having security controls assessed on each ship and validated by a third party is accepted as a 'best practice' for cyber security.

21.2 Cyber security risk should be assessed in advance by management and included in the cyber security strategy. There is a risk that a company or ship originating exploit may carry over to each network undetected.

21.3 Internal testing is used to determine resiliency to specific types of exploit or attack however the system as a whole should be penetration tested by an outside 3rd party who thinks differently than the company internal team. Self-assessment without audit is a flawed approach which can result in unwanted bias or underreporting of the results.

21.4 Rotating outside penetration testers is also a good idea as it exposes the systems being tested to a more robust variety of attack methodologies. This will expose more weaknesses over time and result in an increasing security posture over time.

22. GDPR – EU General Data Protection Regulation

When implementing cyber security on ships it is prudent to include the requirements of the GDPR. Although not part of this case study's questions particular care must be taken to address cyber security systems to avoid investing time and resources into a cyber security strategy that does not address the requirements of GDPR . The GDPR comes into force May 2018 and the regulation strengthens local European legislation for data protection and aligns regulators under one authority. Maritime companies

must follow the GDPR when collecting, processing and managing personal information and data. Companies which breach any of these areas risk fines of up to €20 million or 4% of global turnover and data processing bans.

As it relates to crew and personnel data collection, data retention and data compromise must be addressed. It specifically identifies a Crisis Management Plan and a responsible level of cyber security to protect, detect breaches, and to discover and report quickly which covered data has been compromised and which data has been ex-filtrated. GDPR regulates every company worldwide that provides services to and / or handles personal information of EU data subjects (within the EU). Non-compliance can result in big penalties.

23. Summary

The process of interviewing the company for this case study was a useful exercise in that it helped to understand generally how the Ship owner, Technical-Operations Manager, and Crew Manager is addressing cyber security in his offices and aboard his ships. From this 'snapshot' during the early months of 2017, it can be seen that good progress has been made to understand and address the issues. However, it also creates a further discussion leading to improvements that would not normally be known and considered at this early stage. Cyber security is evolving quickly worldwide but lags the efforts of the professional criminal attacker. The company strategy should be to keep up to date on the evolving regulations and standards, move toward cyber security 'best practice', strive to create a cyber security culture with individual responsibility, prepare for incidents and crisis, and have a system that can improve over time.

Key Elements

1. BoD – Senior Management Oversigh
2. 3rd Party Assessments and Audits
3. Senior Management Budgeting
4. Practical Policy / Sensible Procedures
5. Hardware replacement and Software update policy
6. Designated onboard Cyber security Officer
7. Penetration and Vulnerability Testing
8. Cyber security Awareness Training
9. Cyber security Incident Plan
10. Pre-established Cyber security expert and service Agreements
11. Threat Monitoring, Analysis, and Alert Reporting
12. Assessment of critical ship systems
13. Remediation and Restoration
14. Forensics of cyber breach
15. GDPR – EU General Data Protection Regulation

24. Contributors

The Cyprus Shipping Chamber wish to thank Capt. Lance Savaria of our Member company, EPSCO (Cyprus) Ltd, for his valuable contribution in drafting this paper. Appreciation is also extended to the members of the ICT Sub-Committee of the Chamber for their input.

25. References:

The Guidelines on CYBER Security ONBOARD SHIPS, Produced and supported by BIMCO, CLIA, INTERCARGO, And INTERTANKO, (Version 1.1 – February 2016)

GUIDE FOR CYBER SECURITY IMPLEMENTATION FOR THE MARINE AND OFFSHORE INDUSTRIES
ABS CyberSafety™ VOLUME 2, September 20, 2016

EPSCO-RA (Cyprus) Ltd. "Maritime Cyber Security Solutions", www.epsco-ra.com

"Threat Assessment: The cyber threat against the maritime sector" Centre for Cyber Security (Denmark), March 2017

Cyber Risks in the Marine Transportation System, The U.S. Coast Guard Approach
https://www.uscg.mil/hq/cg5/cg544/docs/USCG_Paper_MTS_CyberRisks.pdf

Futurenautics.com, "Communication or Connected - Crew Connectivity Survey" This article appeared in the October 2015 issue of Futurenautics.

Maritime cyber security using ISPS and ISM codes. Alejandro Gómez Bermejo, Cyber security Manager and Consultant www.erawat.es

The EU General Data Protection Regulation (GDPR). http://www.eugdpr.org

Maritime Alert: USCG Clarifies Cyber Incident Reporting Requirements, JANUARY 19, 2017
http://mariners.coastguard.dodlive.mil/2017/01/17/cyber-reporting-updated-coast-guard-policy-reporting-suspicious-activity-breaches-security/