Cyber Security and Data Protection

A cyber risk is a threat to infrastructure and communications systems, and the data within those systems, which form the framework of any business enterprise, including the marine transportation sector. Such a threat could result in loss of life, loss of or damage to property, financial loss and reputational damage. For the most severe cyber attacks, the effect on their recipients could be catastrophic.

A cyber incident could be caused by a targeted cyber attack, or arise from an unintentional threat as a result of infection by a virus such as malware, the accidental loss of data, or the mis-operation of an operating system for various reasons, including improper configuration or a conflict between software dependent systems.

The sheer number of cyber related incidents and attacks such as WannaCry and NotPetya, some of which have claimed high profile victims, and the number of phishing attempts experienced on a daily basis, demonstrate the importance of having a defence to prevent a major incident. Cyber security should be taken very seriously and should form a core part of a company’s safety and security policies.

A shipboard cyber threat is two-fold, categorised broadly as a threat to Information Technology (IT) and to Operational Technology (OT). The former includes storage and sharing of data (personal, operational, and commercially sensitive) and communications systems, while the latter is concerned with, among other things, navigation systems, propulsion control systems, and cargo control and monitoring systems. Companies now have regulatory obligations with respect to both IT and OT security, which are detailed below.

In both IT and OT infrastructure the vulnerability risk increases when these systems are interfaced with the internet. Some systems are also more vulnerable depending on the underlying software platform on which they operate and the availability of tools for disruption (some of which can be procured from the ‘dark web’). As are legacy systems that do not have any support available to render the systems resilient to continuously morphing cyber-attacks.

The traditional methods of anti-virus software and fire walls are not considered sufficient for an effective cyber defence and a more holistic approach is required. For new vessels this approach should be pursued from initial design through to installation, testing and operation. For existing vessels segregation of systems may need to be considered based on a risk assessment and vulnerability testing. Existing or planned features such as the integration of a ballast treatment system or an exhaust gas cleaning system should be taken into consideration when carrying out risk assessment.

Air gapping systems (a security measure whereby a computer or network is isolated to prevent it from connecting wirelessly or physically with any other computer or network device) are an effective way of segregating but there is the potential risk of introducing malware or other software corruption while routinely updating or maintaining the system or when infected portable or wireless enabled devices are plugged into it. Rigorous procedures for controls and checks will therefore be necessary.

The human aspect of vulnerability cannot be underestimated as it is estimated that 80% of cyber incidents feature an element of human error.

In training in privacy and security practices, control of access (through user ID and password policies) and account management, logging of events and security reviews will be required.

Cyber security regulatory framework

The International Maritime Organisation (IMO) has issued Resolution MSC 428(98) providing, as part of the International Safety Management Code (ISM Code), guidelines for Flag administrations to enforce a cyber security policy and procedure to be implemented before the 1st anniversary of the Document of Compliance (DoC) after 1st January 2021. MSC 428(98) further affirms that ships’ SMS should include cyber risk management that takes into consideration the various relevant elements of the ISM Code.

Linking the date to the DoC it is intended to require that the Cyber Security Management (CSM) is verified during companies’ annual audits and that implementation should be fleet wide and requiring a strong commitment from senior management.

As per the objectives of the ISM Code all risks to ship, personnel and environment should be assessed and appropriate safeguards should be established. Cyber risks should therefore be considered as one such risk and need to be addressed within the Safety Management System.

There are elements in the ISM Code that should be applied to cyber security management, such as the requirement for a risk assessment, policies on cyber resilience, work procedures, contingencies, maintenance of systems to ensure operational reliability, record keeping, verification and audit, designation of responsibility and training of personnel.

The IMO has provided high level guidelines for the implementation of cyber security management based on a risk assessment methodology. There are more detailed guidelines and publications that companies are encouraged to consult for the implementation of the CSM within their organisation. Some of these standards and publications are listed below:

- BIMCO – The Guidelines on Cyber Security Onboard Ships for the implementation of the IMO resolution MSC 428(98), which include elements from various industry recognised standards and the US NIST cyber security frame work.
- ISO/IEC Standards 27001.
- IEC 62443: Security Levels In Industrial Control Applications.
- IACS has published 9 of planned 12 recommendations for making vessel systems resilient and further a unified recommendation UR E22 for On Board Use and Application of Computer based systems.
- United Kingdom Code of Practice: Cyber Security for Ships.
- The OCIMF SIRE VIG 7.0 now includes under Section 7.0 the verification of the implementation of a Cyber Security Policy and Procedures as part of the ships’ SMS.
and verification that the company is actively promoting cyber security awareness.

- The Tanker Management Self-Assessment 3 has included implementation of cyber security policies and procedures as a key performance indicator under Element 13 and a further software management procedure under Element 7.
- It is also important to take due note of various local rules, regulations and reporting obligations that may be applicable such as the Network and Information System Directive of the European Union for essential services which includes the marine transport sector.
- Specific industry sector practices and threats will also need to be taken into consideration for the risk assessment and development of the safety procedures.
- A questionnaire in the Club's condition survey report has also now been included for the attending surveyor to verify the implementation of cyber security management on board vessels.

Cyber security and industry support

Some elements of cyber security management to be taken into consideration include:

- Risk assessment – safety, legal and financial based on known incidents, motives and threats
- Company policy – portable devices, software management, data privacy, access, vendor
- Vessel infrastructure interface and connectivity to Internet
- Vulnerability testing – penetration testing
- Vessel specific implementation
- Operational procedures
- Change management
- Logging events and detection
- Data protection
- Contingency planning – system and data recovery
- Training and awareness of personnel

Cyber vulnerabilities are continuously evolving and therefore information on risk events and the threats to cyber security is crucial. Sharing information on risk events is important for appropriate counter measures and also encourages companies to take corrective action.

Reporting incidents such as navigational interference, jamming or the spoofing of GPS and AIS to local authorities and service providers will help the agencies taking appropriate corrective action and also cascade information to others. Such efforts to collate data are important for assessing the impact on the maritime industry and making a realistic threat assessment.

Where external expert assistance is sought, it is important that the agencies offering such assistance are evaluated and their expertise and experience are verified before providing access to systems.

There are various hardware and software solutions on offer, some based on the principles of machine learning capable of autonomous safeguarding action or alerts for manual intervention.

Implications

Although P&I Club cover has no general exclusion of claims arising from cyber risks, owners, charterers, managers or operators of ships ought to be able to demonstrate that appropriate steps to identify and safeguard against cyber threats and vulnerabilities as required, including having a cyber risk policy and systems, to avoid any potential risk of cover being prejudiced.

BIMCO issued a cyber security clause in May 2019 'to raise awareness of cyber risks among owners, charterers and brokers...to provide a mechanism for ensuring that the parties to the contract have procedures and systems in place, in order to help minimize the risk of an incident occurring in the first place and, if it does occur, to mitigate the effects of such an incident'.

Early implementation of cyber security management is therefore encouraged.

Data protection

In addition to the threats to a company's operational systems, companies should also consider how best to look after the data they hold within those systems. There is now a raft of data protection legislation across the world for companies to comply with. Notably, in May 2018 the European Union brought into force the General Data Protection Regulation (GDPR).

The GDPR is concerned with the handling of personal data – any data that identifies an individual or relates to an identifiable individual. Its purpose is to give data subjects greater rights with respect to their personal data, and requires those handling personal data to be able to justify using and keeping them, and to have in place appropriate security to protect the personal data they hold.

Vessel owners and operators will process a wide variety of personal data, with respect to crew, passengers and staff. This may include medical information, passport details, or salary and job data.

The GDPR applies not only to European individuals and entities (wherever in the world they process data) but also to the processing of personal data:

- of data subjects who are in the EU by an entity or individual based outside the EU, where the processing activities relate to:
  a. the offering of goods or services to data subjects in the EU; or
  b. monitoring their behaviour as far as their behaviour takes place within the EU
- by an entity or individual not based in the EU, but in a place where Member State law applies by virtue of public international law

There are significant penalties for breaching the GDPR. For the most serious breaches, companies could face fines of up to (the greater of) 20 million Euros or 4% of worldwide group turnover. As well as this, the reputational damage to companies that suffer data leaks can be very substantial.

Companies should carry out a detailed audit of their data processing, among other things, assessing the types of data received, what they are used for, where and how they are stored, how long they are kept and who they may be sent to. Policies, procedures and practices that cover the use of personal data should be reviewed in light of the requirements of the GDPR and other applicable data protection legislation, and where appropriate combined with a company's cyber security measures.

Companies have an obligation at all times to minimise the data they collect, and to hold them only for as long as necessary. It is expected that companies will embed the principles of privacy by design (putting in place appropriate technical and organisational measures to implement the data
Protection principles and safeguard individuals’ right) and privacy by default (only processing personal data necessary for each specific processing purpose) into their procedures.

Protection of data is a key concern, and companies should ensure they have suitable electronic and physical security measures in place to look after the data in their own systems, and to make sure data is sent and received in a secure way. Although the GDPR is only concerned with personal data, the imposition of appropriate security measures will ensure that operational and commercially sensitive data is also more secure. These measures may include using appropriate security software, passwords and other user authentication measures, the anonymising of data, and the use of secure or encrypted email servers when transferring emails and attachments containing personal data.

Where personal data is held on devices that leave company premises (such as laptops, tablets, mobile phones or mass storage devices), or such devices are used by staff to remotely access company systems, it may be necessary to use encrypted and password protected devices, and to put in place robust guidelines covering the use and security of such devices.

Physical security considerations may include appropriate entry systems and locks for premises and internal storage facilities such as filing cabinets, and measures to ensure hard copy documents containing personal information are not left lying around.

Companies that process personal data should have in place suitable privacy notices, detailing the types of data they hold and how and why they process them. For companies subject to the GDPR whose core activities require the large scale, regular and systematic monitoring of individuals, a Data Protection Officer (DPO) must be appointed. Where the appointment of a DPO is not mandatory, having a DPO may nonetheless make it easier to properly manage one’s data protection obligations.

With the increase in data protection and cyber security obligations, it is good practice to ensure staff are given the necessary training with respect to their own and the company’s responsibilities. If staff are trained to handle personal data in an appropriate way and to be aware of cyber security threats such as phishing emails and malware, companies will minimise the human error risk inherent in all security procedures and ensure their data are protected and their OT and IT systems free from unwanted interference.

In terms of cyber security on board ships, members are encouraged to read the Guidelines on Cyber Security Onboard Ships – version 3 is available on the Steamship Mutual website.

Steamship has published two Circulars (L312 and L314) which give further background on the GDPR and consider various best practice ideas. These can be found on our website.

Members are also encouraged to view our film on the topic, Cyber Security, Smart, Safe Shipping.

Article by John Hamlyn
Legal Services Executive

and

Vijay Rao
Loss Prevention Executive