Risk Assessment - Key to Maritime Cyber risk management

Author Name(s): R. Srinivas (Principal Surveyor, Indian Register of Shipping)

Introduction

Maritime Industry keeping in line with the recent technology is moving from stand alone computer based systems to integrated computer systems. The new technologies are being adopted not only on board ship systems but also in maritime land installations. Be it a Dynamic position system, integrated platform management system on ships or a Container management system, Vessel traffic management system (VTMS) in port, critical process are getting automated and integrated. At the same time, the demand for ship to shore connectivity is increasing for better monitoring of ship systems, advice on route planning and maintenance.

Originally confined to large vessels and few critical port operations, the trend to integrate multiple systems is seen as requirement in present day offshore supply vessels, coastal vessels and in port critical operations. Use of such advanced systems is not without problems. Loss of network communication, external and internal Cyber attacks, hardware and software change management are some of critical issues which require organisation's continues attention. Critical systems are to be designed, installed, tested and maintained to mitigate the risks arising out of use of such technologies. Therefore evaluating the risks is essential for smooth operation of the control and information systems.

The present paper gives a brief insight on various aspects to be considered while carrying out the risk assessment due to cyber threats on critical systems. .

1. Cyber Risk Terminology

1.1 Cyber system

Cyber system is any combination of facilities, equipment, personnel, procedures and communications integrated to provide cyber services which can include control systems, business systems and personnel information system.
Cyber equipment includes physical hardware, networks, associated application software and networking software and can be an amalgamation of information technology (IT) systems and operational technology (OT) systems. While dealing with cyber issues a clear understanding and distinction between Information Technology and Operation Technology systems, is essential. Information technology can be regarded as the systems where the data is used for information purposes, whereas the operation technology systems can be regarded as systems where data is used to control and monitor physical systems.

1.2 Cyber Attacks

It is a deliberate attempt by a malicious actor to destroy or compromise a computer based system.

Types of cyber attack

In general, there are two categories of cyber attacks which may affect, ships and

land installations (herein after called organisations):
Untargeted attacks, where an organisation or a ship's systems and data are one of many potential targets;
Targeted attacks, where an organisation or a ship's systems and data, are the intended target.

Untargeted attacks are likely to use tools and techniques available on the internet which can be used to locate known vulnerabilities in a company and onboard a ship.

Targeted attacks may be more sophisticated and use tools and techniques specifically created for targeting a particular company or ship. E.g. Spear Phishing is an example

1.3 Attack Route

The most likely route of cyber attack can be through:

- USB or removable media
- Connection of crew or maintenance laptop, mobile device
- Remote connectivity
- Wi-Fi connection
- Through smart phones
- Physical interference with system

1.4 Consequences

In order to assess the risk of threat, the consequence for each threat is to be analysed and documented. For example, loss of router in one segment of integrated propulsion system control network could have effect on safety of the vessel, on the other hand, the same network device when used in ship administrative network, the consequences are less severe. However in a port, an IT network when used for container handling system, if compromised, could severely effect the port operations. Therefore the same network device when compromised will have different consequences depending on the organisation and the system it supports.

1.5 Cyber Threat

Several terms such as threat, threat source, and cyber incident are used in cyber risk management process. The basic concepts behind these terms are closely inter-related.

National Institute if Standards and Technology (NIST) defines threat as *any* circumstance or event which may adversely impact operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. The guide identifies four types threat sources as adversarial, accidental, structural, and environmental effects/actions, of which adversarial attacks are generally considered. as part of cyber security risk assessment. However the accidental threats also play an important role in cyber safety and needs to be considered. Structural effects address aging of equipment, equipment breakdown etc in a maritime context especially for ship are taken care through rules /regulatory requirements through equipment redundancy and installation requirements, maintenance procedures etc. For example through standby generators, pumps, standby systems such as follow up, non follow up steering, arrangement of equipment below main deck and above main deck, fire zones etc.
The consequences of threat of a particular system, in a specific condition, could be

higher when compared with systems with same threat in a different operating condition. Typical example of *sources of threat* could be, but not limited to

- Hackers
- Third party service providers
- Terrorists
- Dissatisfied staff
- Accidental
- Inadequately trained staff

As seen from above threats can originate from an internal source or from an external source.

1.6 Data & Information

Data can be simple facts or figures . when such data is processed and organised to present them in a meaningful or useful way , becomes information. In an organisation data and or information in digital form is used for various purposes. Example of such data or information can be but not limited to, administrative data (employee personnel information), financial data, operational data, data flowing between various control and monitoring devices in a ship or port trust etc. when data/ information in an organisation is compromised due to intentional or unintentional means it can lead to disruption/adverse actions on

- Processes(power generation, access control , traffic monitoring etc, plate cutting machine in a ship yard, etc)
- Organisation assets
- Individuals
- Other organisations
- Nations

1.8 Vulnerability

Vulnerability is the weakness in the system which can be exploited by the threat resulting into a cyber incident. The vulnerabilities may be present as an inherent weakness in the hardware or software itself or may arise due to lack of proper policies and procedures.

An example could be lack of policy for remote login which can result in successful attack from a hostile person from a remote location. Similarly lack of proper procedure for timely update of software patches can lead to cyber attack. The ransomware is a typical example where windows software patches were not applied in time resulting in huge financial losses to many organisations. From a ship point of view, as more and more operations are computerised, the systems which can become vulnerable increase.

IMO in their cyber risk management guidelines in FAL 1 Circ.3 2017 identified following systems, but not limited to, which can vulnerable to cyber risks

- Navigation systems
- Propulsion systems
- Passenger safety systems
- Communication systems
- Auxiliary machinery systems
- Cargo control systems

2. Cyber risks

2.1 Cyber risks can be defined as those risks that arise from the loss of confidentiality, integrity or availability of information in IT and OT systems the consequences of which can severely impact an organisation /or ship critical operations.

National institute of standards and technology (NIST) of US defines risk as a measure of the extent to which an entity is threatened by a potential circumstance or event. Risk therefore is a function of:

- Adverse impacts that would arise if the circumstance or event occurs
- Likelihood of occurrence.

2.2 The Three Dimensions of Cyber risk

ISO 27000, the established standard for information security identifies the following as the key dimensions to be addressed during risk assessment process.

Confidentiality: Information is not made available or disclosed to unauthorized individuals, entities, or processes

Integrity: Information and assets are accurate and complete.

Availability: Information and assets are accessible and usable upon demand by an authorized entity.

The impact due to loss of confidentiality, integrity, availability (CIA) would depend on the type of system i.e control system or information system.

The order of priority for protection of data in IT is generally Confidentiality, integrity and availability, where as for control systems, the availability is important and is given highest priority. It is followed by integrity and confidentiality

2.3 Attack surface

An attack surface is typically the exposed area for cyber attack and depends on the extent to which the system can be accessed either from locally or from another location. For example open USB ports on the PC give an easy access for the intended or unintended user to plug in a corrupted USB stick with virus. Similarly when the system has provision for remote login then the chances of attack increase as the asset can be connected from shore.

The extent of attack surface available to the threat to exploit the vulnerability will determine the likelihood of cyber attack on a particular equipment /system.

2.4 Likelihood of attack

Risk can be seen as the probability of a threat exploiting a vulnerability which can lead to undesired results /consequences.

The likelihood of a threat to exploit for an equipment /system is an important step in risk assessment . It depends on extent to which a cyber threat can be present at the location where the equipment/system is installed, and can exploit the vulnerability.

The extent of connectivity the system has with other systems plays a crucial part in risk assessment. For example a PC in bridge has lower likelihood of unauthorised local access than a PC in deck office. Similarly the threat due to attack on a standalone system has lesser consequence than an integrated system.

2.5 Impact

Impact is the summation of all of losses incurred on the asset, due to loss of confidentiality, integrity or availability of the information.

3. Risk assessment Approach

3.1 Objective

The objective of carrying out a facility risk assessment is to

- Identify the risks
- Evaluate and estimate the risk
- Prioritise the risk

Above steps would help the organisation in identifying suitable controls to mitigate the identified risks

Risk assessment is an essential prerequisite for the definition of a secure architecture. A risk matrix is to be prepared where each threat on a particular system and its consequence on safety, Risks can be graded as High, Medium or low based on the severity of consequences

Risk assessment provides decision-makers and responsible parties with an improved understanding of risks that could affect achievement of objectives, and the adequacy and effectiveness of existing controls. The assessment result provides a basis for decisions on the most appropriate approach to be used to treat the risks. The output of risk assessment is an input to the decision-making processes of the organization.

The risk assessment is to be carried out to assess the health safety, environmental risks (HSE) and business risks, due to cyber-attack. It is to be ensured that appropriate security measures are selected and the systems are protected in proportion to Organisation's risk. If HSE risks are to be assessed from statutory point of view , organisation reputation and operational risks are important from an organisational point of view.

Business risk will vary between different sectors and also within specific operations of the same Organisation.

3.2 Risk Levels

Risk assessment can be carried out at three levels of an organisation.

When carried out at level 1 and level 2 the purpose would be to identify the high level risks, mostly on procedures, polices, governance. The assessment would also assist the management to get a reasonable idea on funding.

When the assessment is carried out at level 3 the objective is to identify the controls, authorisations, monitoring of the IT and OT systems up to field level.
To ensure a cyber safe installation the risk assessment is to be carried out through out the life cycle of the process e.g.

- System concept and design stage
- Implementation and commissioning stage
- Operation stage

The organisation shall be aware that any risk assessment, has some limitations arising out of assessment methods, techniques, data quality, interpretation of results and expertise of the individuals performing the risk assessment.

3.3 Risk assessment methodology

Multiple methods are available for carrying out the risk assessment and each industry over the last few years have come out with methods to suit their particular industry, for example for railways, power industries, nuclear plants etc. The methods suitable for an IT organisation may not be suitable for an organisation having Supervisory control and data acquisition (SCADA) systems.

Risk assessment methods can be broadly classed as per following factors

a)How the individual risks are measured *: Quantitative or qualitative*

Quantitative method requires data on known failure rates, frequency of attacks on a particular equipment, systems in different scenarios. As the cyber risk data especially in control systems in nascent stage, lack of authentic risk data, is a major drawback in evaluating risk quantitatively. On te other hand qualitative risks requires specialist knowledge of systems and risks are evaluated as high medium low etc.

b) How the risk identification process is structured, *Situation/ scenario based or asset based.*

The risk assessment can be device specific for example , ECIDS , power management systems, port data base server etc. Alternatively it can be situation/ scenario

based for example ship propulsion system, vessel traffic management system, container handling system etc. For an effective risk assessment integrating both methods is recommended, which considers both assets (which may comprise of devices, applications , data) and scenarios.

3.4 Risk assessment Process

The risk assessment process includes following steps

i)Establish the context

The scope of assessment (process, systems, equipment) are to be identified and documented prior to carrying out risk assessment.

The scope shall include the assets that support the operations of the vessel /organisation and potential impacts in case confidentiality, integrity or availability is compromised.

Simple questions such as what is the function of the systems, what kind of data does the system handles, how does the data flow between various sub systems, what are the interfaces etc. would help the assessor in identifying the vulnerable systems.

ii) Identify Threats

This phase involves identification of all possible threats which can be present in the given system environment and can exploit the equipment /system vulnerabilities. There are certain common threats and some threats are specific to equipment. As an example, unauthorised access to systems, data leakage , loss of systems etc. are common threats. Where as spoofing, jamming are specific threats to systems using communication such GPS, AIS etc. .

iii)Determine likelihood of attack.

The next step would be identify the likelihood of attack considering the existing controls. Generally the existing control include organisational risk policy, user access controls, physical access controls, remote login controls etc. When looking at security point of view the threats considered will be of adversarial type originating from individuals, groups or organizations seeking to exploit the vessel dependence on cyber resources.

iv) Evaluate Risk

The final step or last phase of risk assessment process involves evaluation of risk value. The risk evaluation is more or less a straight forward equation which states risk as a product of impact and likelihood. The impact can be assigned a number in 1 to 10 or alternatively can be classified as high, medium and low based on the severity of the impact. This value can form the basis for determining which risks are needed to be mitigated immediately. Due to lack of sufficient published risk data on industrial control systems, the qualitative procedures are generally applied.

The risk value also depends on the extent of connectivity For example a vessel fitted with performance monitoring system and remote maintenance for main engines has more connectivity than a vessel fitted with stand alone engine control system.

4 Risk analysis

4.1 Risk analysis is a complex process and based on the analysis decision to mitigate the risk or accept the risk is taken. The decision would be based on organisation risk tolerance level which is to be identified prior to commencement of process.

Identified Risks can be dealt in two ways. Either accept the risk or mitigate the risk.

Depending severity of identified risk a decision is made during risk analysis to accept the risk or mitigate the risk. Risk

prioritisation is also carried out in this stage of risk assessment.
Risks that are mitigated are those that typically have a medium to high impact on an organisation. Risks that are accepted should have little to low impact on the organisation. Cost of mitigating risk also plays a crucial role in decision making process.

There is a third alternative also i.e. to Defer a risk. Deferring a risk is generally not recommended as it would require a detailed assessment of the consequence, before taking a decision to defer it. Any wrong analysis can have serious consequences to safety and security of the asset.

Prior to commencement of risk assessment the organisation as a minimum has to carry out following activities

- Establishes risk acceptance criterion
- Identifies and documents consequences of each threat on Vulnerable system
- Understands its legal responsibilities for the business it undertakes
- Identifies risk priorities based on severity of impact

The risk assessment process is to be periodically reviewed as per the organisational policy

4.3 Common Observations

Some of the common observations found during risk assessment of maritime industry are presented below

- Risk analysis does not consider all OT systems
- Business continuity plan does not address critical OT and IT systems.
- Inadequate network segregation , especially between IT and OT networks , leading to increased risk
- Low Cyber risk awareness for OT systems
- In a port the critical systems are located in different buildings spread over entire port area. Physical security levels of these assets accordingly would be different and would be based on operations they support.
- Applicable Govt of India regulatory requirements for cyber security need to be included in risk analysis

5. Cyber Risk Management Philosophy

Cyber risks cannot be totally eliminated through installation of fire walls, antivirus software. A holistic approach is required towards management of cyber security. A five functional approach method is recommended to manage the cyber risks. NIST frame work for critical infrastructure specifies a five functional approach to address cyber threats.
The five functions which form the basis for Cyber risk management are

a. *Identify*: Clear definition of roles and responsibilities involved in cyber risk management, identify typical assets which are vulnerable to attacks, identify risks, policies and procedures
b. *Protect*: formulate suitable technical and procedural control to mitigate the identified risks through Systems and procedures such as training, technical protection, controls etc.
c. *Detect*: develop and implement systems and procedures to detect a Cyber incident like intrusion detection systems, analyzing anomalies etc.

d. *Respond:* Define and implement the various process involved in responding to a cyber event. The policies and procedures of the organisation to respond to a cyber incident. Ex communication, response planning etc. is to be formulated and implemented.
e. *Recover*: Organisation has to measures through policies and procedures for recovery of critical data, backup philosophy etc., in the event of cyber attack.

The objective of the whole process would to identify controls to prevent the risk and identify suitable mitigation measures to reduce the risk level

6 Cyber Risk Management, Statutory Requirement

Noting the criticality of cyber risks in maritime field IMO has adopted following resolutions/ circulars

- Guidelines on Cyber risk management vide MSC- FAL.1 /Circ.3 2017
- Res. MSC.428 (98) on Maritime Cyber Risk Management in Safety
- Management Systems requiring Cyber risks being appropriately addressed in safety management systems no later than the first annual verification of the company's Document of Compliance after 1st January 2021.

The guidelines define cyber risk management as the process of identifying, analysing, 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.

For Indian flag vessels DG shipping vide their Engineering circular 06 of 2017 further specified that Cyber-risk management procedures are to be included in the SMS manuals. Circular 06 of 2017 specifies procedures for compliances through ISM as under

- All new DOC applicants requesting for initial DOC audit on or after 1st January 2018
- All other existing DOC holders wishing to demonstrate compliance prior to 1st January 2021

7. IRS initiatives for a Cyber safe Installation

To assist Indian maritime Industry in identification of cyber risks and design a suitable cyber risk management system, IRS has developed Maritime cyber safety Guidelines. The guidelines have been prepared based on IMO guidelines, NIST, IEC 27001, and IEC 62443. Notation for ships can be assigned by IRS when the facility complies with the specified requirements. Training is an important aspect in controlling cyber incidents and our cyber risk management training programs are designed to help the industry in identifying and designing suitable control towards an effective cyber risk management.

8. Conclusion

Risk assessment forms fundamental and important step in addressing cyber risks. A holistic approach addressing various threat actors, threat paths are to be considered along with overall impact on the vessel safety and environment when the subject system is compromised.

Leaving some of the crucial factors can lead to ineffective system as the barriers implemented to prevent risk depend on the risks cause and their path. In the event the threat materialises to an event, the objective should be to control the damage to extent possible before the undesired consequences are realised. It is therefore very important that the person/group responsible for carrying out the assessment has clear understanding of information and operation technology systems of the installation, their interdependencies and can clearly visualise the total/ partial degradation of performance of critical systems and its effect on overall organisation.

Reference

- IMO guidelines on cyber risk management
- ISO/IEC 27001 standard on Information technology – Security techniques
- ISO/IEC27032-Guidelines for Cyber security
- United States National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Security (the NIST Framework).
- Code of Practice - Cyber security for ships by Department of Transport UK
- IEC 62433-2-1 Establishing an Industrial automation and control system security program
- IEC 62443-3-3 Industrial Communication Networks - Network and System Security - Part 3-3: System Security Requirements Security Levels
- NIST Special Publication 800-30
- ISO 31000 – Risk Management-Principles and Guidelines