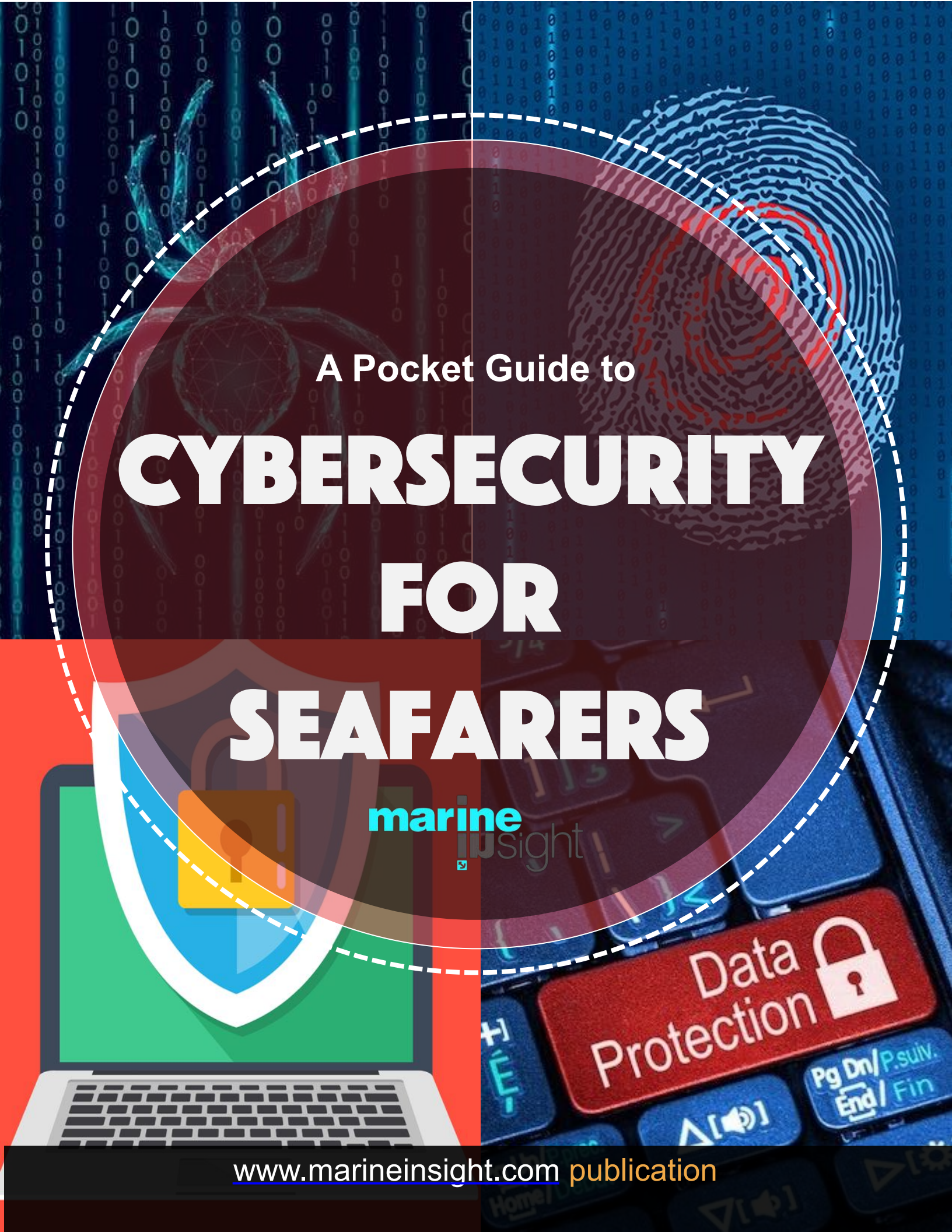


www.marineinsight.com publication

Marine Insight©

A Pocket Guide to Cybersecurity for Seafarers

Publication date: December- 2018
Author: Raunek Kantharia

Published by: Marine Insight
www.marineinsight.com

Graphic Design: Marine Insight Graphics Dept.

TABLE OF CONTENTS

CHAPTER ONE

Introduction- Importance of Cybersecurity

Why Seafarers Needs a Hands on Training on Cyber Safety?

Introduction to Cybersecurity

In 2017, the world's largest container shipping company, Maersk suffered one of the worst kind of cyber attacks. The notorious NotPetya wiped off data from company's 4500 PCs, resulting in massive damages of up to $250- $300 million. For the recovery from the attack, the company had to install 4000 new servers, 45000 new PCs and 2500 applications, utilising an enormous amount of human and financial resources.

With ships acquiring new advanced technologies ever year for both engine room and bridge navigation, the issue of cyber attacks is more prevalent than ever as most new systems on ships are highly automated and extensively dependent on information technology and data exchange.

These technological advancements have become an easy target for hackers and cybercriminals to find their way into ship's systems, and from there, to various systems of on shore.

Cybersecurity for Seafarers

Needless to say, though the seafarers are more responsible for cyber safety when on a ship, the shipping companies are equally responsible for providing proper training and education to prevent cyber attacks.

The digitalisation of the maritime industry is happening at a rapid pace. It is essential for seafarers to not only understand and adopt these new technologies but also to become cautious and aware of how things can go wrong in a matter of few hours.

The main difference between a general maritime safety issue and a cyber safety issue is that the victim of a cyber attack is generally not aware of the threat and following consequences even after the attack, making the situation even more dangerous in terms of losses.

Many seafarers are highly experienced and skilful in their jobs but are equally novice when it comes to using information technology and other technological advancements as a majority of them have not received any specific training on the same from companies or shore-based institutes.

Cybersecurity for Seafarers

Also, with the increasing influence of social media and the facility of on-board internet ships, seafarers use at least one social media platforms while at sea. Other commonly used means of communicating with friends and family at sea are WhatsApp, WeChat, emails, SMS, phone calls etc.

SMS and phone calls do not require internet connections and therefore are the most preferred way to trap seafarers in the phishing net.

With ships acquiring new advanced technologies ever year for both engine room and bridge navigation, the issue of cyber attacks is more prevalent than ever as most new systems on ships are highly automated and extensively dependent on information technology and data exchange.

How does it start?

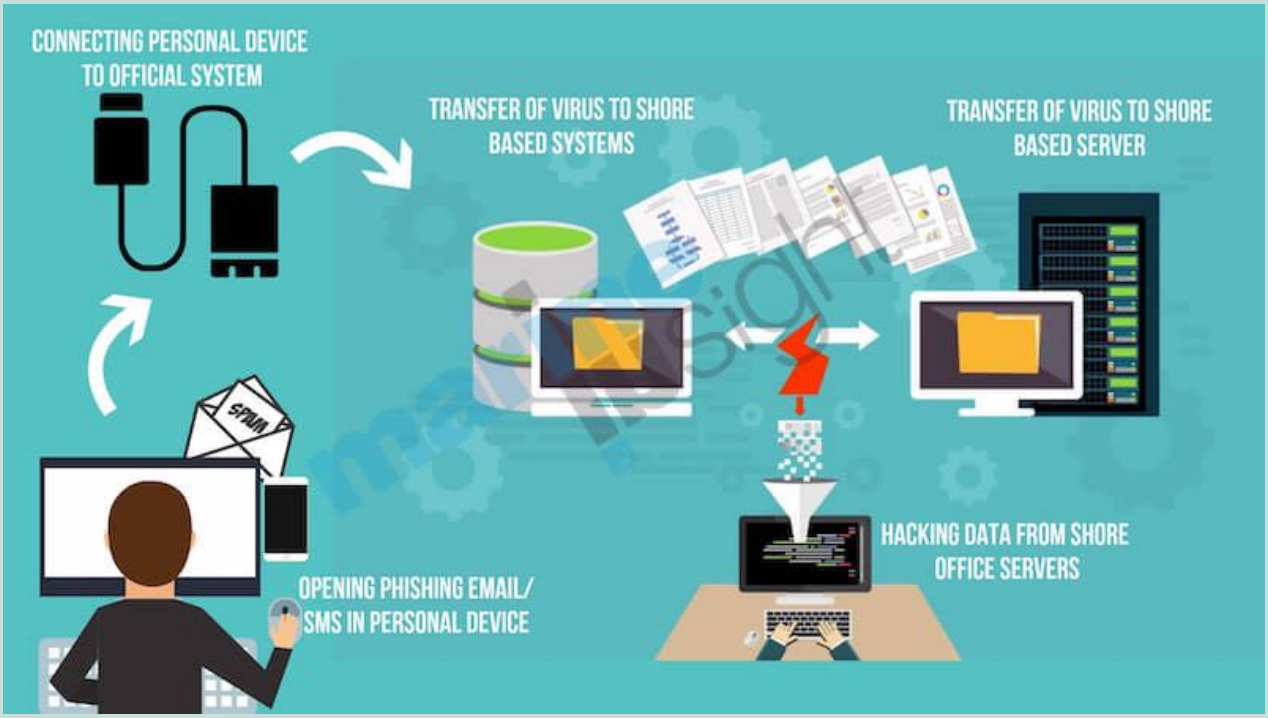
Any cybercriminal needs an access to a secured digital network having sensitive information, which can be utilised for monitory benefits, to commence a crime. Seafarers are an easy target for such criminals as the former are always looking for ways to connect to the world through various digital means from different parts of the world and often through untrusted systems / networks.

As per data, a majority of the cyber-attacks onboard are triggered accidentally by seafarers which can be due to the opening of phishing email attachments or hyperlinks or using infected removable media.

The ship system is an intranet system, i.e. there are computers installed at various locations and departments, which are all connected (Similar to those found in any other organisation or company). However, the same system is used by seafarers for both official and personal use, which makes the complete connected system vulnerable to cyber attacks. When seafarers use such infected mobile phones or storage drives to transfer

transfer data to a ship's computer, the virus spreads into all the ship's systems connected via intranet.

As the master connects the ship's system to the internet for sending or receiving files from the shore-based company office, this deadly virus can be transferred with other data without detection (unless screened by a good anti-virus software) and spreads to the land-based computer systems, leading to a major cyber-attack. The attack which started from a personal device is now transformed into a significant corporate cyber attack.



Considering an increase in cyber attack incidents in recent times, it is vital to train the seafarers on good practices of using information technology related systems, including social media and other personal means of communication.

Maritime authorities and governmental institutions should also provide additional training on information technology and cyber safety to the students of Maritime Training Institutes (MTI's) to increase awareness.

Cybersecurity for Seafarers

As per the Crew Connectivity 2018 Survey Report, 92% of seafarers now say that internet access “strongly influences” their decision on whether to work on a ship or not. This data itself indicates that we need more immersive and in-depth cyber safety training starting from the grassroots level.

It is the responsibility of the shipping company to train every crew member on “Cyber Safety” before getting them onboard ship. The probable consequences of a cyber attack on board ship are:

- Loss of network
- Loss of connectivity between various parts of control systems
- Gaining unauthorised access to control and IT systems
- Unauthorised change of critical system parameters
- Environmental Impact
- Safety Impact
- Effect on critical application /assignment of the ship

A majority of the cyber-attacks onboard are triggered accidentally by seafarers which can be due to the opening of phishing email attachments or hyperlinks or using infected removable media.

CHAPTER TWO

Common Ways for Cyber Attacks on Ships

Malware:

Malicious software and tools are the most common ways (malware) that are used to initiate a cyber attack. Viruses, spyware, Trojan horses, worms etc. are used to highjack, alter, steal, encrypt and delete sensitive data of a system without the knowledge or permission of the user.

A virus, once on a ship's system, spreads and infects all vulnerable programs and files whereas a worm can self-replicate and spread without any human interaction.

A Trojan horse is designed in a way to appear genuine and authentic tool, however once activated performs all malicious activities, for which, it is programmed from.

Spyware as the name suggests, spies on the user and collects sensitive information and data without the knowledge of the user.

Ransomware is designed to encrypt the data of a system after infection. The criminals then ask a ransom in return of decrypting the data.

Phishing emails:

This is the most commonly used techniques to extract sensitive data from users illegally. Cybercriminals design and send emails (or use other communication channels) which appear to be sent from a legitimate and reputable company or a person. These messages contain malicious links or attachments which ask for victim's sensitive details such as login credentials, bank details etc.

Social Engineering:

Social engineering is a technique which deals with manipulating people to break security procedures for gaining access to a particular system or network.

This is a common trick used by hackers as it is easy to exploit a human weakness than to find a vulnerability in a system.

The attacker would often present themselves as a trusted individual from a reputed company or a person of high authority, in order to seek sensitive information from the desired organisation.

Email virus:

It is yet another very commonly used technique to infect the desired system with a virus. An email with malicious code is distributed through emails. When a vulnerable user clicks a link, opens an attachment or interacts in any other way, the code activates and infects the system with the virus.

Honey trap:

This is another method, in which, a seafarer plays an indirect role in implanting a virus in the ship's system. Seafarers are always eager to get shore leave and to socialise. There have been incidences in the past wherein a seafarer or shipping company representative while enjoying his free time in a social club meets a beautiful woman.

The conversation then leads to an exchange of emails and mobile numbers. Later on, the maritime professional, who was eagerly waiting for a message, receives an email containing a link, which when clicked, leads to unintentional downloading of virus. It was a well-planned cyber-attack plot.

Free gadgets:

In some past incidences, free pen-drives/flash drives were offered to seafarers by unknown people as gifts when crew members visited seafarer clubs. It is natural not to be suspicious in such places/institutions; however, seafarers have been taken advantage of during such visits.

SMS:

Short Messaging Service or SMS is also a popular way to infect the mobile device of seafarers. The message may contain a free or lucrative offer along with a link which will lure the reader to click it. Once the link is clicked, a malicious virus will get installed on the mobile phone.

If the same phone is connected to another device (e.g. seafarer's personal computer), it will get transferred to it; whereas, if the seafarer uses a pen drive to copy an important file to the ship's computer, the virus will get into the pen drive and then to the ship's computer without the seafarers knowing about it. As the SMS does not depend on the internet, this is one of the preferred methods of attack.

Free Wifi:

Free wifi in airports, public places, shipping ports etc. are not secure and can be accessed by anyone. There is always a danger of cyber attacks in such open and vulnerable systems.

CHAPTER THREE

How to Identify a Cyber Attack?

The chances are high that you can become a victim of cybercrime without knowing about it. However, there are a couple of signs that you should be aware of to find out if your system is compromised. Do note that you might not always be able to read these signs; however, watching out for these suspicious activities will help you to take immediate actions if you are on the verge of an attack.

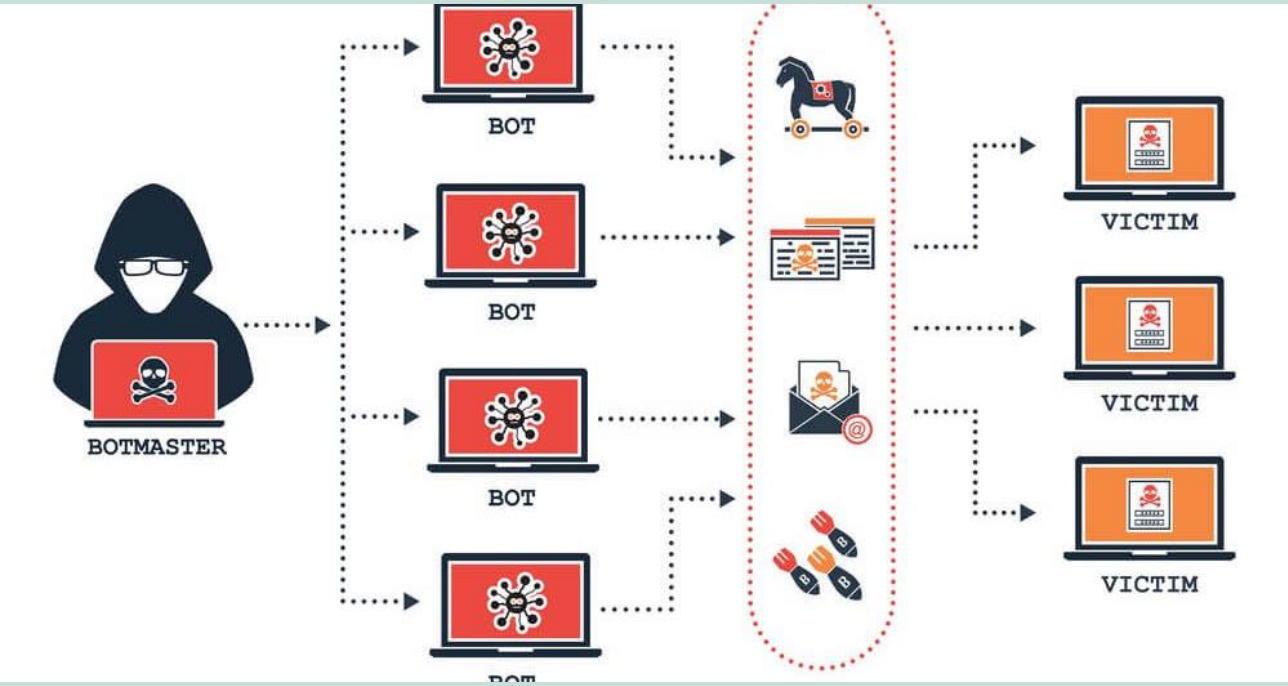
Check primary recourses and unusual activities

A virus (or a form of malware) will create problems by over utilising the resources of your system. If the virus infection is already activated, it will slow down the system by putting the CPU at full use or consuming too much of RAM even if you are not performing any operation.

In such cases check the Task Manager if you are using windows or Activity monitor if you are using MAC. Kill any process that looks suspicious. Though, cybercriminals are now smarter to name the virus in executable file format to make it look like a legit and essential system file. In such cases, kill all processes that are consuming a large amount of resources. Always remember that the path of the virus executable file will still be different than the system file.

Another thing you can check is the file size and the bandwidth usage. Sometimes virus utilises a large amount of disc space while creating several hidden files in system directories. Also, if the virus is designed to transfer your data to a remote server, then there will be a lot of usage of network bandwidth. Makes sure you kill such processes immediately.

If there is a denial of service (DoS) attack, which usually takes place over the internet, there are very slim chances you will be able to prevent it. As the attacker will open several connections to your computer at a very high speed, utilising plenty of resources before crashing it, the system will become too slow to monitor what has gone wrong.



Hence, to detect if the system is attacked by a malware or virus, following things to be noticed:

•Unexpected errors in programs, including failure to run correctly or programs running unexpectedly

•Unexpected password changes or authorised users being locked out of a system

- A slow and unresponsive system
- Sudden changes in available disk space or memory
- Emails returned suddenly
- Unexpected network connectivity difficulties
- Frequent system crashes
- Abnormal hard drive or processor activity
- Unexpected changes to browser, software or user settings, including permissions

Physical signs of compromised ship's network

Sometimes it will be too late to take action against cybercrime.\ The attacker would have already perpetrated the systems and attained the desired results. Though it would be difficult to find out which system has been affected, some of the common targeted systems of ships are :

- Automated identification system & ECDIS - Interfering with GPS signal using spoofing device, blocking signals, jamming alarms
- Cargo tracking system - taking control over computer systems to identify valuable cargo, removing containers with illegal items from the system to go undetected

Cybersecurity for Seafarers

- Marine navigation and radar system - misleading vessel's direction, shutting down one or all navigation systems
- Satellite communication system - diverting funds, gaining sensitive data, hijacking email and other modes of communication
- Security systems - infiltrating ports security system to allow entry to unauthorised people

It is widely proven that most of the cyberattacks rely on human errors. It is therefore important to identify all vulnerabilities and take necessary protection and detection measures.

CHAPTER FOUR

Security Against Cyber Crime

Cybersecurity for Seafarers

How can a seafarer ensure his or her security against cyber crimes?

Keep Your Passwords Strong: As cliché as this may sound, this is one of the most common vulnerabilities across users. Most people have a habit of keeping the same password across all apps and websites for their convenience. This is highly risky.

Keep different passwords for different websites. Use a combination of capital and small letters, special characters, and numbers to make your password stronger. It is normal for a seafarer to use public systems at cafes, seamen's club, hotels etc. to access emails, banking accounts and other similar websites requiring their personal details. Make sure whatever methods you are using are adequately secured and from a trusted organisation. Do not share your passwords or any other sensitive information with anyone.

Be aware of phishing emails: Sometimes phishing emails are too difficult to differentiate from genuine emails.

Cybersecurity for Seafarers

Avoid opening any links or attachments from suspicious emails especially if you are opening them on a ship's system or network. In case of doubt about the authenticity of the mail, mark them and then open them when you are on a secured network, which is not connected to any of the ship's system or network.

Use Free Wifi Hot-spots with caution: While travelling to new places, seafarers are often looking for free wifi hot-spots. Though this a highly useful service, free public wifi hotspots are a breeding ground for hacking activities. Ensure you do not access any account which requires putting sensitive credentials.

Avoid Becoming an SMS Victim: As mentioned earlier, this is a favourite tactic among hackers to gain personal information from victims. It works similar to a phishing mail. As seafarers often use different SIM cards to get the best calling and data rates, a hacker would send a phishing SMS with a link to get the cheapest offers on calling and data plans. Once the link is clicked, it will either download malware to the phone without the user's knowledge or open a webpage or application which looks reputable or trustworthy, asking sensitive information.

Avoid using unidentified disk, pen drives: If you are not aware of the condition of pen/flash drive given to you by your colleague or another person, avoid using it. Keep a separate pen drive/ hard disk for personal use and another for office/ship use.

As explained in the earlier point, you will never know when your phone is attacked by malware if it's intent is to attack your ship's or company's network. Do not connect your phone directly to the ship's computer network for data transfer or charging. If you need to transfer any documents from your phone to ship's system, first transfer it to your personal computer and ensure your personal computer have a good antivirus, and the file has been approved by it, before forwarding it to ship's network.

Cybersecurity for Seafarers

One common practice of seafarers is to keep all important documents in the email or cloud drive or on the computer as a soft copy. However, if any of this gets hacked, the bad guys will have all the sensitive details. Similar cases have been registered wherein sensitive details of seafarers were used to make forged documents or to gain access to companies' system by hackers/ smugglers.

In this age of FB posts and tweets, we humans are so excited all the time to tell the world what we are doing or will be doing next. We have seen many posts from the seafarers that give details about their whereabouts and even mention the ETA of their ships and next port of call.

Many intelligence and security agencies have proved that the pirates scan social media for such updates. Learn and know the privacy settings or your post (and the social network) so that only your trusted friends can see the profile and post details.

How can shipping company ensure ship's security against cyber crimes?

Training

The human element is one of the most significant factors in the cyber safety problem on board ships. Training the crew and the shore staff who are directly involved with the ship operation is essential. The training program provided by the company should cover three main areas:

1. Ways to prevent the attack

2. Ways to identify the malware or virus within the system or a potential suspicious software or file

3. How to cure the attacked system and back up requirements

The training should be provided to the crew of all levels and must include the preventive maintenance routines such as updating of anti-virus and anti-malware software, taking backups of essential files, incidence-response planning and testing.

Regulated and strong access control

The company needs to set up the system on a ship which is highly regulated and requires authorisation at different levels. The Master and other management level officers of all department need to be trained regarding the hierarchy of the online system that needs to be followed.

Management level officers such as chief officer, 2nd engineer, chief engineer and Master are the first line of defence in implementing cyber safety on ships and training the junior officers and ratings.

Inspection

The shipping company needs to regularly inspect the information technology system installed on the ship, including the status of anti-virus software and condition of the system, i.e. if they are virus-free or not, as the crew working on board may never know in case the ship system is affected.

There are classification societies and third parties which aid in implementing cyber inspections of the ship.

Segregation

The seafarers staying on board the ship may access the ship's computer from different locations for both work and personal usage. A company can make a simple provision by keeping the ship's systems connected on a different network and the computers/ system used for training or personal usage on a separate one. The management level officers must ensure no personal drives, USB, CDs etc. are used without prior permission on a ship's network.

It is possible that a visitor (port personnel, agent, PSC inspector etc.) may require computer or printer access. For such cases, an independent computer not connected to the ship's controlled networks must be used. To avoid unauthorised access, removable media blockers should be used on all other physically accessible computers and network ports.

Use of the latest antivirus system

Anti-Virus is a computer program which is installed to detect, respond and remove any malicious software with viruses or malware. The anti-virus functions include blocking the user access to any such infected files or system, cleaning of such system, and giving an early warning of the infected system to the user. The company must also ensure that the connected systems are provided with firewalls and updated anti-virus tools, and are implemented on the servers as well as at the end user level

Implement Cybersafety in SMS

There is already a resolution by Maritime Safety Committee (MSC) to add MARITIME CYBER RISK MANAGEMENT IN SAFETY MANAGEMENT SYSTEMS which states that "Administrations to ensure that cyber risks are appropriately addressed in safety management systems no later than the first annual verification of the company's Document of Compliance after 1st January 2021". All companies should try to implement it in the SMS as soon as possible as the threat is real and can happen at any time.

Administrator privileges, allowing full access to system configuration settings and all data, should be given only to selected people, who are appropriately trained for the usage.

CHAPTER FIVE

Responding to Cyber Attack

Cybersecurity for Seafarers

Most companies and maritime professionals won't come to know for several days if there has been a cyber attack until some physical signs come to their notice regarding the malicious activity.

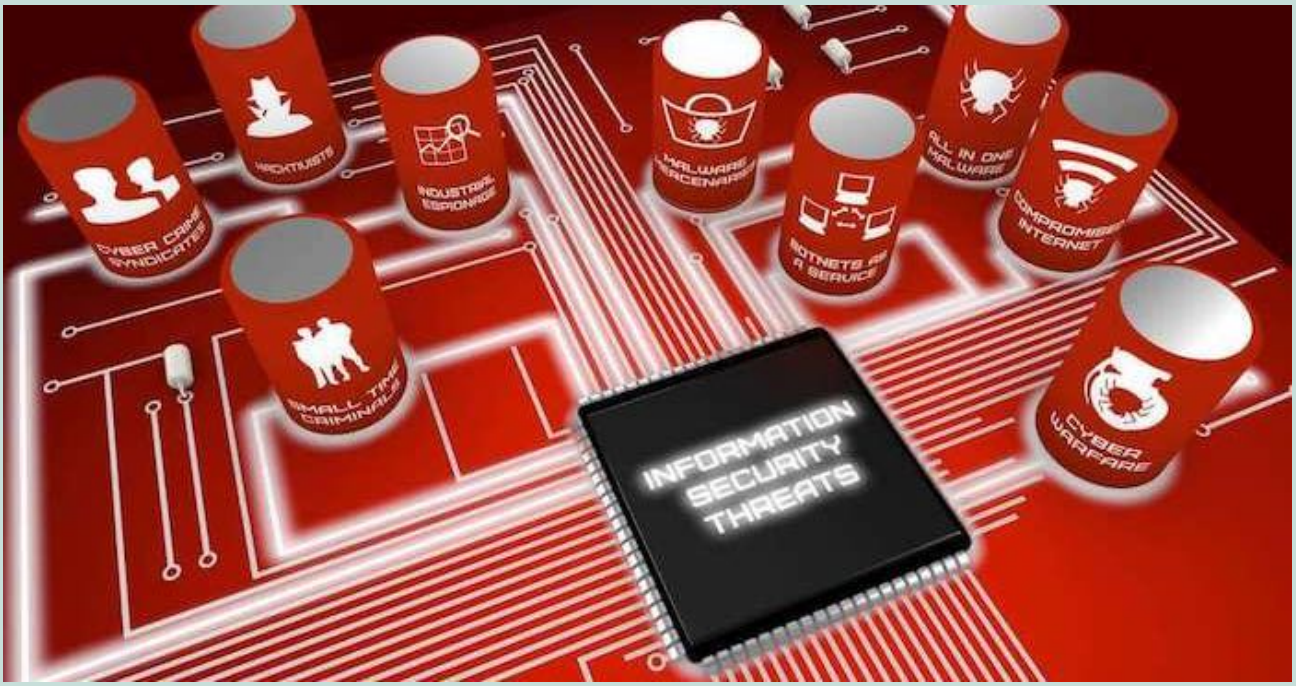
Being prepared with a recovery plan and acting quickly will help in bouncing back as soon as possible from a cyber attack. The first and most important step would be to inform the company and the authority about the breach. Maritime professionals can then take the following steps to recover from the attack:

1. Identify the problem through assessment

If there is a specialised team of IT experts provided, try and identify -

•What were the reasons for the incident

•What is the type of attack and level of threat



- Until what extent the data is affected

2. Recover and restore the data

If possible, IT department should act quickly to restore IT and OT data by separating the sensitive data from the network, removing affected files, reinstalling removed files, putting security patches etc. The priority at this stage would be to bring the system back to operational condition.

A data recovery capability with software backups is crucial on ships. It is understood that most of the times there would be no expertise at sea to deal with such situations and in such cases help should to taken from shore technical support and efforts should be made to reach port safety to get further help from IT engineers.

3. Preventing reoccurrence of attacks

For ships, recovering from an attack is not enough. Steps to prevent any future attacks must be taken by carrying out a proper investigation to understand the causes and consequences by bringing in experts.

People working on ships should be made aware of the results of the investigation and related vulnerability that can lead to such incidents in future.

The shipping company must implement a proper recovery and prevention plan to mitigate and minimise the effects of such attacks in future.

CHAPTER SIX

Security Measures and Contingency plan

Cybersecurity for Seafarers

Preventive planning by the shipping company is highly important to prevent any cybersecurity threat to the ship.

According to IMO guidelines, a five functional approach to cyber risk management needs to be adopted, following the instructions mentioned in all sections. The five functions of Cyber risk management are as follows:

1.Identify: Identify the systems, policies, and procedures that are vulnerable to attacks

2.Protect: Implement protection methods such as training, technical protection, controls etc.

3.Detect: Systems and processes to detect a Cyber incident like intrusion detection systems, analysing anomalies etc.

4.Respond: The organization's plan to respond to a cyberattacks. For e.g. communication, response planning etc.

5.Recover: Procedures for recovery of critical data, backup systems etc.

Digital services increasingly rely on external factors. Security must broaden its scope and imagine how to ensure a 'known and consistent' risk level with in-house and outsourced means. Referring to value chain is one of the keys

Cyber-safety and security management plan

This document should contain the following information/details:

•Description of various essential safety systems/equipment

•Policies and procedures to be followed

•Roles and responsibilities of each crew member

•Vulnerability analysis (systems and procedures for all intended operations of the vessel/shore support facility)

•Risk assessment process and report

•Risk register including risk tolerance and risk management

- Third party risk assessment procedure
- Method for sharing cyber safety information.
- Process Review methodology

Cyber-safety Implementation plan

The cyber-safety and security plan is to incorporate the following details:

- Operations and Maintenance plan to be followed
- Registry of control and information system equipment

- Software Registry and software updates
- Reports on the vulnerability test
- Records of cyber incidents and event logs where applicable
- Full details of remote logins
- Software configuration management plan and policy
- Network diagrams for IT and OT systems
- Information on vulnerable software and hardware assets
- Test procedures and test records for every change in software and hardware assets of both IT and OT systems

Exhaustive prevention is an illusion. Company can't secure misconfiguration, shadow IT, third parties, human error, former employee etc. Focus on what matters more and be ready to react.