The lowdown on cyber security

More and more ships are being digitalised and connected to the worldwide web. That means cyber security should concern everybody on board – even if they are not computer experts. All seafarers can make a difference – here’s how

Protecting a ship’s computers can be compared to protecting your home. A fence keeps strangers out, just as a computer is protected by a firewall. If your fence breaks, you must mend it. Your firewall must be kept up to date to prevent malware from getting in.

On the other hand, there need to be gaps in the fence to allow wanted visitors in. We must be able to welcome friends and family while assessing the risk of inviting in a stranger. Some guests are granted access to every room in the house, while the delivery guy might just be allowed into the hallway. But even if you offer your aunt unrestricted access to your home, you may still decide to keep your valuables in a locked safe. In other words, you are in full control.

When it comes to life onboard ship, officers must take control to make sure they know who has access to what data, and who is allowed in rooms containing key technical equipment.

Industry guidelines

In January 2016, a group of industry organisations including BIMCO published new Guidelines on Cyber Security Onboard Ships. These can be downloaded for free from www.bimco.org. There is a quick link at http://bit.ly/1O09X9g. The guidelines are designed to develop understanding and awareness of key aspects of cyber security. They do not focus on the technical aspects of cyber security.

Cyber security should start at the senior management level of the company ashore. You cannot protect a ship 100% against cyber incidents (a cyber incident is anything that may adversely affect an onboard system, network and computer or the information it handles). So it is important to have contingency plans ready for when something goes wrong.

Senior management has the strategic responsibility to decide on how best to protect the ship. For example, a barge trading in inland waters will be protected differently from a 15,000 TEU container ship trading worldwide. Cyber security is related to business processes and crew training, as well as technical systems. It is not just a matter for the IT department.

Cyber security has both safety and security aspects. So all plans and procedures for cyber risk management should be seen as complementary to the existing security and safety risk management requirements contained in the International Safety Management Code (ISM) Code and the International Ship and Port Facility Security (ISPS) Code.

Both information technology (IT) and operational technology (OT) might be vulnerable to cyber threats.

Cyber security onboard ships protects:

> operational technology against the unintended consequences of a cyber incident;

> information and communications systems and the information they contain from damage, unauthorised use or modification, or exploitation; and/or

> against interception of information when communicating and using the internet.

Identifying a threat

Firstly, you need to understand the specific threats to which the ship and its operations are exposed. For example, if a container is very valuable, there may be criminals who want to steal the contents. In order to do so, they need to know the location of the container and ship. So this information must be restricted to as few people as possible.

In general, there are two categories of cyber attacks, which might affect companies and ships:

> Untargeted attacks, where a company’s or a ship’s systems and data are one of many potential targets; or
Targeted attacks, where a company’s or a ship’s systems and data are the intended target. Untargeted attacks are likely to use tools and techniques available on the internet to locate known vulnerabilities in a company and onboard a ship. For example, to try to locate the container, the criminals may check if a valuable container is mentioned on social media. This method is called social engineering.

Targeted attacks may be more sophisticated and use tools and techniques specifically created for targeting a particular company or ship. To locate a container, for example, they may send a personal email to someone who knows which ship the container has been loaded on. This email may contain malicious software or links that automatically download malicious software. Such software will then send the information to the criminals, thereby enabling them to intercept the container.

Vulnerabilities
There are a number of onboard systems which may be exposed to cyber risks. It is important to identify these systems and their vulnerabilities. They could include:

- Cargo management systems
- Bridge systems. Even bridge systems that are not connected to other networks may be vulnerable, as removable media are often used to update such systems from other onboard networks
- Propulsion and machinery management and power control systems
- Access control systems e.g. for the accommodation and cargo control rooms
- Passenger servicing and management systems
- Public networks for passengers
- Administrative and crew welfare systems. These are particularly vulnerable when they provide internet access and email. They should not be connected to any safety critical systems on board
- Communication systems

Risk assessment
A risk assessment will help find out how vulnerable and how exposed the different systems are. The Industry Guidelines outline two risk assessment methods used by the crew or by a third party. When doing it yourself, elements of a Ship Security Assessment can be used to physically test and assess the IT and OT systems on board.

1. Identify existing technical and procedural controls to protect the onboard IT and OT systems. Is there unused or defective software, or are systems outdated or unpatched?
2. Identify specific vulnerabilities in IT and OT systems, including human factors, and the policies and procedures governing the use of these systems. Do you use passwords, are personal profiles changed regularly, etc?
3. Identify and evaluate key shipboard operations that are vulnerable to cyber attacks. For example, who is allowed access to what systems and what are they allowed to do?
4. Identify possible cyber incidents and their impact on key shipboard operations, and the likelihood of their occurrence. For example, what to do if the communication to the shoreside has been compromised?

Training and awareness
You can reduce the risk of cyber incidents by procedural controls, focussing on how seafarers use the onboard systems. Plans and procedures that contain sensitive information should be kept confidential and handled according to company policies. In many cases, a cyber incident is started by personnel working in the company. Personnel, even with the best of intentions, can be careless, for example by using removable media to transfer data from one computer to another without taking precautions; and data can be mishandled and files disposed of incorrectly. To limit these risks, training and awareness should be developed for:

- Onboard personnel, including the Master, officers and seafarers; and
- Shoreside personnel who support the management and operation of the ship.

An awareness programme for seafarers should cover:

- Emails and how to behave in a safe manner;
- Internet usage, including social media, chat forums and cloud-based file storage where data movement is less controlled and monitored;
- Use of own devices;
- Risks related to installing and maintaining software on company hardware;
- Poor software and data security practices where no anti-virus checks or authenticity verifications are performed;
- Safeguarding user information, passwords and digital certificates;
- The physical presence of non-company personnel, for example where third-party technicians are left to work on equipment without supervision;
- Detecting suspicious activity and how to report if a possible cyber incident is in progress;
- The consequences or impact of cyber incidents to the safety and operations of the ship;
- Understanding how to implement preventative maintenance routines such as anti-virus and anti-malware, patching, backups, and incidence-response planning and testing; and
- Procedures for protecting against service providers’ removable media before they are connected to the ship’s systems.

Author: Aron Frank Sorensen, Chief Marine Technical Officer at the Baltic and International Maritime Council (BIMCO)