Secure State Cyber: Crewmembers' responsibilities for maintaining security of IT systems on board

In this, the second FAQ article in the cyber risks series, Secure State Cyber highlight the responsibilities of crewmembers in maintaining the security of IT systems on board, safeguarding personal devices and identifying which equipment is most vulnerable on board.

What can crewmembers do to protect themselves and the vessel from a cyber-attack?

Crew members can take several actions to avoid their vessel becoming compromised:

- **Do not Jailbreak a device:** Ensure that the mobile device is updated regularly, and the device is not subject to 'rooting' or 'jailbreaking'. Rooting refers to a process that allows access to an Android device with 'root' or 'system' privilege, which in turn enables the user to install or make any modifications that they please. Jailbreaking refers to Apple products in the same way. The purpose of these actions is to remove restrictions imposed by the manufacturer or operator, e.g. to allow the installation of unauthorised software. Once a device is rooted or jailbroken, there is an increased chance that the device can have spyware, trojans, rootkits, or other forms of malware installed easily without the owner's knowledge.
- **Do not plug personal items into the ship's critical network:** Crew members that have access to or manage critical ship systems should not plug personal devices into any of the ports on these management systems or Human-Machine Interfaces (HMIs). It is imperative that devices used for accessing and/or managing ship systems are not utilised for web-browsing, social media, internet surfing or personal emails. Each device has a purpose, and their roles should be set out clearly and isolated from any other tasks.
- **Avoid clicking on phishing emails:** Phishing emails are emails sent by hackers with the intent to get unknowing users to click on malicious links or files. These emails are usually well built to look like a legitimate sender to confuse the recipient. Phishing attacks are one of the most successful and common attack methods for hackers as it saves them the effort of having to find another way through a firewall.

What equipment is most vulnerable on board?

The most vulnerable systems on board are typically the oldest and least up-to-date systems. These systems often run in a plaintext format or are using old protocols for management or operation, but not always. In addition, these systems often tend to be linked to managing

process control, safety and support functions such as Distributed Control Systems (DCS). DCS is a common term for systems that collect, process and forward data on board ships such as alarms, video, private telephone systems, engine controls and dynamic positioning among others.

The problem is amplified when the most vulnerable systems are also the most critical. A defence-in-depth strategy is vital when securing these vulnerable and critical systems. Defence-in-depth refers to the layering of protections to access critical systems therefore making it more difficult to bypass security to access the system (both for authorised and unauthorised personnel). The most critical systems and those programs that have access to or control these systems, are the most important and will require the highest level of redundancy and security measures.

How can crewmembers verify that equipment is safe to plug into the ship’s systems?

To reduce the risk associated with plugging equipment into lower security and higher security systems:

- Prohibit any uncontrolled devices from accessing the most critical systems. Any equipment or systems allowed to access these or the networks that contain these important systems, should be fully controlled and established policies and controls should exist that identify everything that is allowed, and more specifically what is not allowed.
- Ensure devices have a current and updated antivirus software installed. Before equipment is plugged into the systems either to patch an air gapped system (a system not directly connected to any network connected to the internet) or to transfer a file, file integrity checks and antivirus scans should be automatically performed (including third-party vendors and contractors).
- Verify the ability to install third party software or applications is completely controlled and restricted solely to system administrators.

Special Consideration: If Bring Your Own Device (BYOD) is allowed, Members need to implement a thorough asset loss aversion solution and policy. Devices that are allowed into the network should be controlled by an appropriate measure. If a BYOD device is lost or stolen, the IT team must be able to remotely wipe the device. The IT team also needs to be able to prevent unauthorised installs and downloads to these devices. The residual risk posed by BYOD devices must be fully understood before permitting crew to utilise these.

What special precuations should be taken for isolating networks on which the ship's communication equipment functions?

It is important to segment and separate networks into different areas of trust based on the criticality of the systems that operate on those networks. The key word here is network, any

system that is communicating with a critical system is also deemed to be critical, and hence part of the network.

However, it must be remembered that a network should not be over-secured to the point of compromising availability of critical systems. The purpose of security is to lower risk of the potential loss of an asset, not to reduce the availability of necessary services to authorised personnel.

This article is one in a series produced in partnership with cyber security specialists, Secure State Cyber.