PREVENTION AT SEA

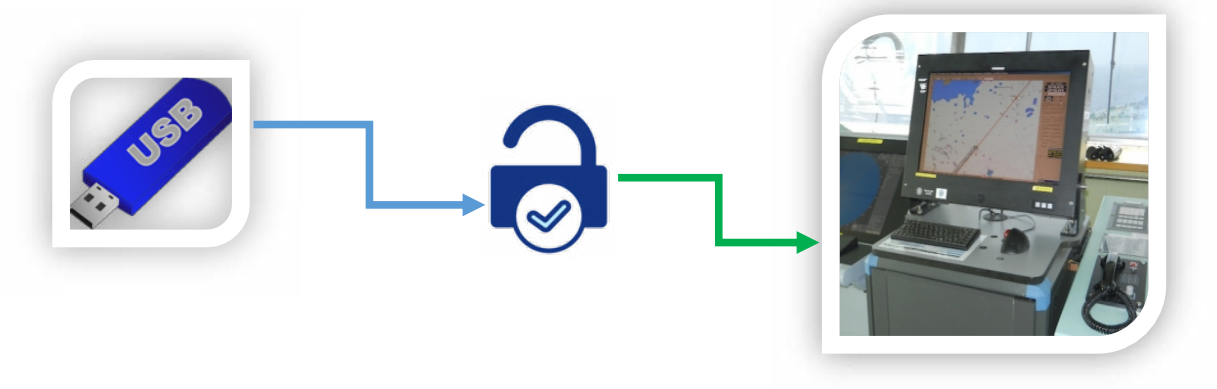
CIRCULAR 07/2018

SECURE YOUR ECDIS – PREVENT A CYBER ATTACK!

Don't Cure,
PREVENT

Secure your ECDIS – Prevent a Cyber attack!

Case Study: During a recent inspection on board a tanker vessel, the PaSea Marine Risk Auditor noticed that a USB drive was plugged into the ECDIS to install updates for the ENC's. The officer of the watch was complaining that the system was too slow and some false alerts popped up at the ECDIS computer, causing issues to the normal operation of the system. Finally, with the assistance of the Marine Risk Auditor and the Managing Company's IT department, it was evidenced that the ECDIS sensor data was manipulated with unreliable information displayed to the officer of the watch. Following the vessel's cyber security management procedures, the problem was effectively solved and the ECDIS system was properly restored, without causing further damage to the Nautical charts folio and to the ECDIS system in general.



Check USB connections or DVD drives, prior their connection to ECDIS system.

Import of electronic data such as updates to navigation systems and software, always implies risk of unauthorized or malicious data intrusion with potentially destructive consequences for the safety and security of shipboard systems. In extreme cases secondary damages are incalculable and may affect control over the ship at levels leading into catastrophic incidents.

Therefore, it is important that seafarers comply with **Company cyber security procedures**, that take into account industry guidelines and regulatory requirements addressing cyber security.

ECDIS specifically is sensitive to attacks that can cause serious cyber safety issues, ranging from a reduction in performance to a complete system failure potentially compromising safety of navigation.

ECDIS and associated sensors are vulnerable to attacks such as:

- malware attacks via computer viruses, worms, trojan horses or ransom ware
- spoofing attacks whereby data such as GPS positions is manipulated and falsified to mask the true position of the ship
- denial of service attacks taking the ECDIS offline and leaving the ship without means of safe navigation

To control the risks of attacks the Master and Navigation Officers should apply:

- ✔ **Restriction of use of the ECDIS** to trained and authorized personnel only;
- ✔ **Restriction of access to software component of the ECDIS**, including the computer operation system (OS), by password protection;
- ✔ **Restriction of access to the data interfaces of the ECDIS computer**, such as USB connections and DVD drives, to authorized persons only by keeping the computer in a cabinet under lock and key;
- ✔ **Frequent backing-up crucial data**, including passage plans, navigational data, and software;
- ✔ **Assurance that new software and updates to existing software for installation on the ECDIS is approved by the ECDIS maker and/or IT experts of the Company;**
- ✔ Assurance that the ECDIS software and operating system is kept up-to-date;
- ✔ Assurance that only software and data pertinent to the ECDIS is installed and that no other files such as music files, games, videos or pictures are installed; and
- ✔ **Assurance of availability and frequent training of adequate emergency response plans for the event of suspected cyber attacks and ECDIS failure**. The Master and Navigation Officers SHOULD know what to do in the event of equipment malfunction, whether due to a cyber-attack or for other reasons, in order to ensure continuance of safety of navigation in the event of ECDIS or sensor failure.

Prevention at Sea can undertake the compilation of ship specific and Company specific Cyber Security Management Plan in compliance with the Company's SMS procedures. Additionally, we can provide Company specific ECDIS Management Plan containing as a separate Appendix, Cyber security guidelines on ECDIS, always in compliance with the Company's existing cyber security procedures.

HELPFUL TIPS

TIP 1

Follow cyber hygiene practices, such as a strict device policy, whereby a dedicated – clearly marked - USB memory device is kept solely for use with the ECDIS and is scanned for viruses each time before inserting into the ECDIS; other USB devices are strictly prohibited for use with the ECDIS;

TIP 2

Connecting the ECDIS directly to a network, forms a serious risk of attack. A careful Risk Assessment must be carried out before connecting an ECDIS to a LAN or to the internet. This must assess whether adequate security protocols are in place, such as anti-virus software and a suitable firewall.

TIP 3

If an ECDIS is not protected with anti-virus software or use a not updated OS, the user SHOULD ensure that any media, particularly USB memory devices, are authorized and approved before connecting to the ECDIS.

Ref. BIMCO "The Guidelines on Cyber Security Onboard Ships, Version 2.0". These Guidelines were a joint effort by various shipping organizations, including Intercargo, International Chamber of Shipping, Cruise Lines International Association, OCIMF and Intertanko. Reference is also made to the IMO's Guidelines on Maritime Cyber Risk Management (MSC-FAL.1/Circ.3) of 5 July 2017.

PREVENTION AT SEA

DON'T CURE, PREVENT! FOR MORE INFORMATION, PLEASE DO NOT HESITATE TO CONTACT US.

Prevention at Sea Ltd
52 Arch. Makariou III Avenue,
Ydrogios Tower, CY 6017
Larnaca - Cyprus

Tel: +357 24819800
Fax: +357 24819881

Tel: +30 210 64 37 637

info@preventionatsea.com

www.preventionatsea.com

CIRCULAR 07/2018