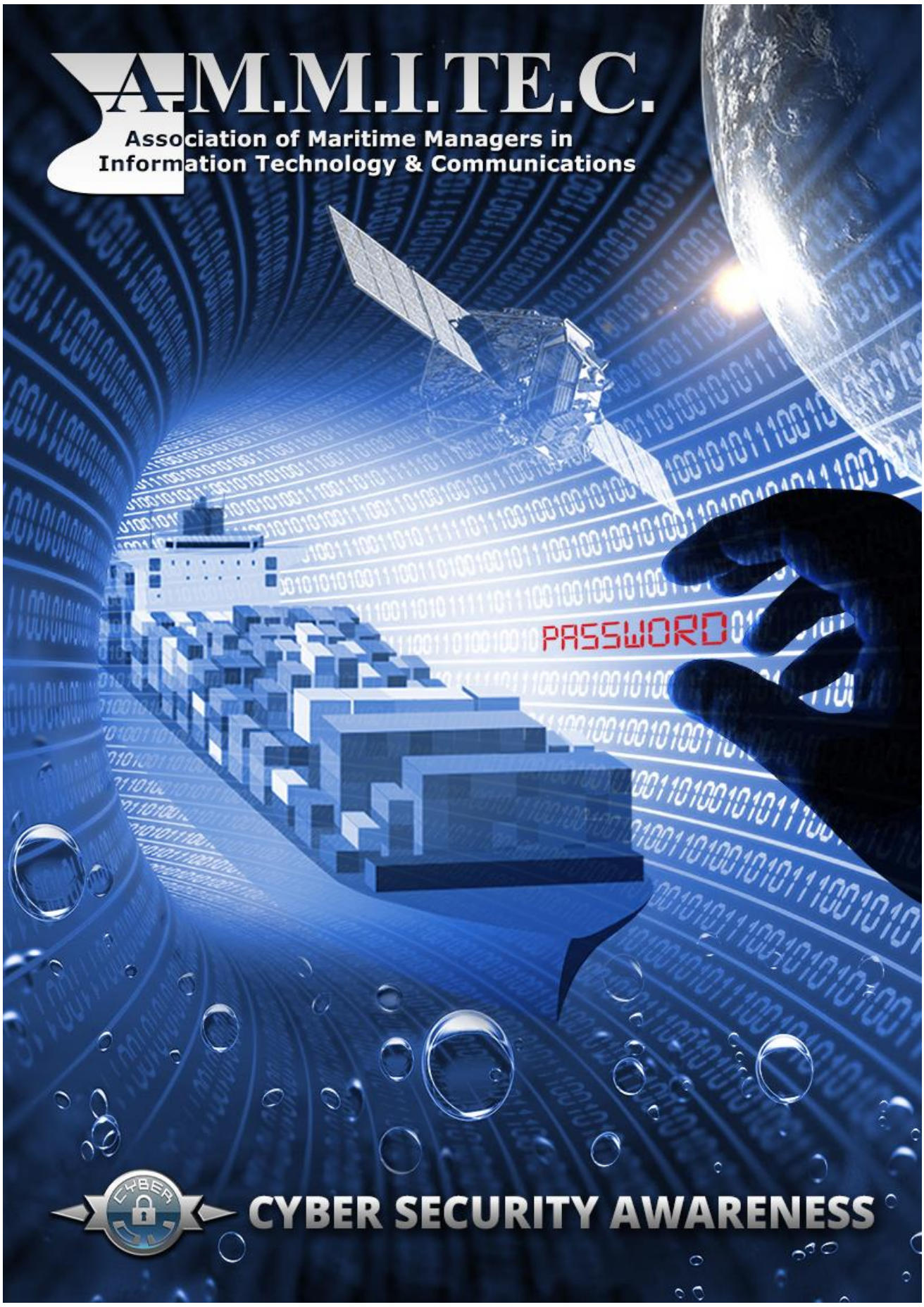
A.M.M.I.TE.C.
Association of Maritime Managers in
Information Technology & Communications
PASSWORD
CYBER SECURITY AWARENESS

Terms of Use

The information contained in the Cyber Security Awareness document is for general guidance purposes only. The information is provided by AMMITEC and while we endeavour to keep the information up to date and correct, we make no representations or warranties of any kind, express or implied, about the completeness, accuracy, reliability or suitability with respect to information contained in this document. In no event will we be liable for any loss or damage including without limitation, indirect or consequential loss or damage, or any loss or damage whatsoever arising from loss of data or profits arising out of, or in connection with, the use of this document. Any reliance you place on such information is therefore strictly at your own risk.

Cyber Security and Risks

An Introduction

As Shore and Satellite Communications continuously evolve over time, Internet access is a feature available to most vessels of our fleets and all office staff. Nowadays, more and more core ships' & office systems are networked together and connected to the public Internet.

- Bridge Navigation
- Communications
- Propulsion and machinery management
- Power control
- Ships Security
- Cargo Management Systems
- Crew Welfare (Crew Lan, Wi-Fi hotspots, Internet browsing etc.)
- Crew personal mobile devices connected to ship's network

Although this includes many benefits, it also contains some major risks. Considering this, some major Organizations like Bimco, Clia , ICS, Intercargo and Intertanko have begun to develop Cyber Security Guidelines in order to raise awareness of the safety, security and commercial risks for shipping companies.

AMMITEC, the Association of Maritime Managers in Information Technology and Communications www.ammitec.org, has created a team of ICT Professionals which aims in Maritime Cyber Security Awareness. In this document you may find useful guidelines which aim to provide general information and knowledge in Cyber Security. Next step is to initiate a risk assessment on this area, expose threats and vulnerabilities and finally enhance security and protection of our Offices and Fleet Networks.

«Any information from your side that will help raise awareness in cyber security and risk matters is most welcome». Please send your enquiries and suggestions to info@ammitec.org

Best Regards,
AMMITEC BoD

Terminology

Cybersecurity is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access.

Elements of cybersecurity include:

- Application security
- Information security
- Network security
- Disaster recovery / business continuity planning
- End-user education

Why worry?

The increased use of Computer Network Systems from navigation to container inspection has enhanced mariners' and vessels' safety at sea.

However, the more we leverage on Internet for these activities, the more vulnerable we become.

Vessels are now vulnerable to Cyber Attacks, as those systems were designed to meet the needs of the 20th century rather than the threats of the 21st.

Important systems with high risk such as:

- E-navigation and integrated Automatic Identification Systems (AIS) to supplement marine radar, the main method of vessel detection, positioning and collision avoidance
- GPS / dGPS, Electronic Chart Display and Information Systems that are often integrated with company's AIS

Gaining access to these systems could allow criminals to disable one or multiple ships transiting strategically important waterways, greatly impacting world trade.

What can I do?

Email Use

Think twice before you click “Send”!

- Corporate e-mail is a tool intended for business related work. Personal use should be limited
- Corporate infrastructure should not be used for private purposes.
- Double-check that your e-mail is being sent only to the intended recipients, don’t forget to check the replied addresses
- Do not forward business e-mail messages to your personal e-mail account
- Do not open emails and attachments from unknown senders
- Remember that every e-mail you send will be saved on a computer server somewhere, even if you delete it on your laptop or other device

What can I do?

Protect Removable Media

Examples of removable media include, but are not limited to:

- USB flash drives - memory sticks
- External hard drives
- Memory cards (e.g. SD cards from digital cameras or cell phones)
- DVDs and CDs

How can I protect my media?

- Use only company approved removable media
- Before you open removable media, scan it for malicious software
- Use removable media only as a temporary data store, for a minimum possible duration, and not in place of network storage
- Securely store removable media or keep it in your possession
- Do not share any device containing confidential information with unauthorized individuals
- If possible, use a dedicated machine to exchange removable media with third parties (i.e. vendors, agents, auditors, etc.)

What can I do?

Beware of Social Engineering

- Social engineering is a technique used to trick you into disclosing valuable information. Social engineering usually occurs through a personal interaction, such as a telephone call or face-to-face encounter, or through the use of computer systems
- Be certain of a person's identity and their right to ask for information before providing it. Be suspicious of unsolicited requests for personal or corporate information
- Do not provide personal details or financial information about yourself, your colleagues or clients to someone you don't know, especially over the telephone or via e-mail
- Beware of any e-mail that claims to activate or suspend a financial account, change a password or payment technique, or that prompts for personal or banking details
- If in doubt, consult with your manager or partner
- Report the incident immediately to your ICT department

What can I do?

Social Media

When using social media, it is important that you protect confidentiality of corporate information.

- Be careful when using social media
- Carefully review and select privacy settings
- Don't make posts or comments that may be considered defamatory, obscene, libellous, threatening, harassing or embarrassing to others
- Do not exchange or store work documents or messages
- Do not discuss details of your work activities
- Be cautious when downloading applications from social networking sites

Remember:

- Everything you post is at risk of disclosure
- Everything you post stays there forever

How ICT will keep the Business Secure

Identify

- Identify Risk Areas & assign “Risk Owners”
- Perform internal Risk Assessment

Protect

- Review Access control Processes
- Secure Network perimeter
- Build a “security culture” in your organization

Detect

- Conduct Independent Security Assessment
- Encourage users to be actively involved in the security of sensitive data they work with
- Establish incident alert thresholds

Respond

- Prepare and implement a response plan
- Report & categorize all cyber incidents

Recover - Prepare for the Worst

- Keep an updated Business continuity plan
- Keep an updated IT Recovery plan
- Execute Drills based on the response plan

The above awareness has been developed by AMMITEC, the Association of Maritime Managers in Information Technology and Communications.