CỤC ĐĂNG KIỂM VIỆT NAM
VIETNAM REGISTER

ĐỊA CHỈ: 18 PHẠM HÙNG, HÀ NỘI
ADDRESS: 18 PHAM HUNG ROAD, HA NOI
ĐIỆN THOẠI/ TEL: +84 24 37684701
FAX: +84 24 37684779
EMAIL: vr-id@vr.org.vn
WEB SITE: www.vr.org.vn

THÔNG BÁO KỸ THUẬT TÀU BIỂN
TECHNICAL INFORMATION ON SEA-GOING SHIPS

Ngày 07 tháng 08 năm 2018
Số thông báo: 014TI/18TB

Nội dung: Quản lý rủi ro mạng hàng hải trong hệ thống quản lý an toàn tàu biển.

Kính gửi: Các chủ tàu/ công ty quản lý tàu biển
Các đơn vị đăng kiểm tàu biển

Hiện nay các tàu và các công ty quản lý tàu đang ngày càng sử dụng nhiều hơn các hệ thống dựa trên số hóa, tích hợp và tự động hóa, dẫn tới có nhiều rủi ro về truy cập trái phép hoặc các cuộc tấn công nguy hiểm cho hệ thống và mạng của tàu. Thực tế này yêu cầu phải quản lý rủi ro về an toàn và an ninh mạng trên tàu.

Ngày 16/6/2017, tại phiên họp lần thứ 98, Ủy ban An toàn hàng hải của Tổ chức Hàng hải quốc tế (IMO) đã thông qua nghị quyết MSC.428(98) về quản lý rủi ro mạng hàng hải trong hệ thống quản lý an toàn; trong đó "*Khẳng định một hệ thống quản lý an toàn được phê duyệt cần lưu ý đến việc quản lý rủi ro mạng phù hợp với các mục tiêu và yêu cầu chức năng của Bộ luật ISM.*"

Nghị quyết MSC.428(98) "*Khuyến khích các Chính quyền hàng hải đảm bảo rằng các rủi ro mạng được đề cập một cách thích hợp trong hệ thống quản lý an toàn không muộn hơn đợt thẩm tra hàng năm đầu tiên của Giấy chứng nhận phù hợp (DOC) của công ty sau ngày 01/01/2021.*"

Ngày 05/7/2017, IMO đã ban hành Thông tư MSC-FAL.1/Circ.3 về hướng dẫn quản lý rủi ro mạng hàng hải đưa ra các khuyến nghị về quản lý rủi ro mạng hàng hải để bảo vệ vận tải biển khỏi các rủi ro mạng và lỗ hổng hiện tại đang nổi lên, cũng như các yếu tố chức năng hỗ trợ quản lý rủi ro mạng hiệu quả.

Liên quan đến vấn đề nêu trên, chúng tôi xin gửi kèm theo Thông báo kỹ thuật tàu biển này văn bản số 3943/ĐKVN-VRQC ngày 02/7/2018 của Cục Đăng kiểm Việt Nam về việc quản lý rủi ro về an toàn và an ninh mạng trên tàu biển hoạt động tuyến quốc tế. Đề nghị các Quý Đơn vị lưu ý thực hiện việc quản lý rủi ro mạng hàng hải phù hợp với các hướng dẫn của IMO.

Thông báo kỹ thuật này được nêu trong mục: *Thông báo/ Thông báo KT Tàu biển* của trang tin điện tử của Cục Đăng kiểm Việt Nam: http://www.vr.org.vn.

Nếu Quý Đơn vị cần thêm thông tin về vấn đề nêu trên, đề nghị liên hệ:

Cục Đăng kiểm Việt Nam
Trung tâm Chứng nhận hệ thống quản lý chất lượng và an toàn
Địa chỉ: 18 Phạm Hùng, Phường Mỹ Đình 2, Quận Nam Từ Liêm, Hà Nội
Điện thoại: +84 24 37684701 (số máy lẻ: 451)
Fax: +84 24 37684720
Thư điện tử: vrqc@vr.org.vn; nhanth@vr.org.vn

Xin gửi đến các Quý Đơn vị lời chào trân trọng./.

Nơi nhận:
- Như trên;
- Phòng QP, TB, CN, HTQT;
- Trung tâm VRQC, TH;
- Các chi cục đăng kiểm;
- Lưu TB./.

BỘ GIAO THÔNG VẬN TẢI
CỤC ĐĂNG KIỂM VIỆT NAM

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Số: 3943/ĐKVN-VRQC

Hà Nội, ngày 02 tháng 7 năm 2018

V/v Quản lý rủi ro về an toàn và an ninh mạng trên tàu biển hoạt động tuyến quốc tế

Kính gửi: Các công ty vận tải biển quốc tế

Hiện nay các tàu và các công ty quản lý tàu đang ngày càng sử dụng nhiều hơn các hệ thống dựa trên số hóa, tích hợp và tự động hóa, dẫn tới có nhiều rủi ro về truy cập trái phép hoặc các cuộc tấn công nguy hiểm cho hệ thống và mạng của tàu. Thực tế này yêu cầu phải quản lý rủi ro về an toàn và an ninh mạng trên tàu.

Ngày 16/6/2017, tại phiên họp lần thứ 98, Ủy ban An toàn hàng hải của Tổ chức Hàng hải quốc tế (IMO) đã thông qua nghị quyết MSC.428(98) về quản lý rủi ro mạng hàng hải trong hệ thống quản lý an toàn; trong đó "*Khẳng định một hệ thống quản lý an toàn được phê duyệt cần lưu ý đến việc quản lý rủi ro mạng phù hợp với các mục tiêu và yêu cầu chức năng của Bộ luật ISM.*"

Khoản 1.2.2.2 của Bộ luật ISM quy định mục tiêu quản lý an toàn của công ty phải bao gồm việc đánh giá mọi rủi ro đã được xác định đối với tàu, con người và môi trường và thiết lập các biện pháp bảo vệ thích hợp.

Khoản 1.4.5 của Bộ luật ISM quy định mỗi công ty phải xây dựng, thực hiện và duy trì một hệ thống quản lý an toàn bao gồm các quy trình để chuẩn bị sẵn sàng và đối phó với các tình huống khẩn cấp.

Nghị quyết MSC.428(98) "*Khuyến khích các Chính quyền hàng hải đảm bảo rằng các rủi ro mạng được đề cập một cách thích hợp trong hệ thống quản lý an toàn không muộn hơn đợt thẩm tra hàng năm đầu tiên của Giấy chứng nhận phù hợp (DOC) của công ty sau ngày 01/01/2021.*"

Ngày 05/7/2017, IMO đã ban hành Thông tư MSC-FAL.1/Circ.3 về Hướng dẫn quản lý rủi ro mạng hàng hải. Thông tư này khuyến nghị việc tham khảo Hướng dẫn về an ninh mạng trên tàu được xây dựng và hỗ trợ bởi BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, OCIMF và IUMI.

Cục Đăng kiểm Việt Nam xin gửi đến các Quý Công ty các tài liệu sau đây (song ngữ Anh - Việt):

- Nghị quyết MSC.428(98) ngày 16/6/2017;
- Thông tư MSC-FAL.1/Circ.3 ngày 05/7/2017;
- Hướng dẫn về an ninh mạng trên tàu được xây dựng và hỗ trợ bởi BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, OCIMF và IUMI.

Đề nghị các Quý Công ty :

- Xem rủi ro mạng là một loại rủi ro đã được xác định đối với tàu, con người và môi trường và phải có biện pháp bảo vệ thích hợp;
- Bổ sung các vấn đề về quản lý, đánh giá rủi ro mạng vào quy trình quản lý rủi ro hiện có trong hệ thống quản lý an toàn của công ty;
- Bổ sung vào quy trình ứng phó tình huống khẩn cấp hiện có trong hệ thống quản lý an toàn của công ty các tình huống khẩn cấp phát sinh từ sự cố mạng;
- Xem xét bổ sung vấn đề an ninh mạng vào kế hoạch an ninh của tàu;
- Tham khảo Thông tư MSC-FAL.1/Circ.3, khi bổ sung sửa đổi hệ thống quản lý an toàn;
- Trước khi yêu cầu thực hiện đánh giá lần đầu, hàng năm hoặc cấp mới Giấy chứng nhận phù hợp (DOC), công ty phải có bằng chứng đã triển khai thực hiện các nội dung nêu trên tối thiểu 03 tháng.

Từ sau ngày 01/01/2021, khi thực hiện đánh giá lần đầu, hàng năm hoặc cấp mới DOC đối với các công ty vận tải biển quốc tế, Cục Đăng kiểm Việt Nam sẽ xem xét vấn đề quản lý rủi ro mạng phù hợp với các hướng dẫn của IMO.

Cục Đăng kiểm Việt Nam trân trọng thông báo đến các Quý Công ty./.

Nơi nhận:
- Như trên;
- Cục trưởng (để b/c);
- Trung tâm VRQC; Phòng TB, QP, CN, CTB (để th/h);
- Các Chi cục Đăng kiểm tàu biển (để th/h);
- Lưu VP, CN.

KT. CỤC TRƯỞNG
PHÓ CỤC TRƯỞNG

CỘNG HOÀ X.H.C.N VIỆT NAM
CỤC ĐĂNG KIỂM VIỆT NAM
BỘ GIAO THÔNG VẬN TẢI

Nguyễn Vũ Hải

THE GUIDELINES ON
CYBER SECURITY ONBOARD SHIPS

HƯỚNG DẪN AN NINH MẠNG TRÊN TÀU

Produced and supported by
Được xây dựng và hỗ trợ bởi

BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, OCIMF and IUMI

Bản dịch tiếng Việt của Cục Đăng kiểm Việt Nam

Terms of use
Điều khoản sử dụng

The advice and information given in The Guidelines on Cyber Security Onboard Ships (the guidelines) is intended purely as guidance to be used at the user's own risk. No warranties or representations are given, nor is any duty of care or responsibility accepted by the Authors, their membership or employees of any person, firm, corporation or organisation (who or which has been in any way concerned with the furnishing of information or data, or the compilation or any translation, publishing, or supply of the guidelines) for the accuracy of any information or advice given in the guidelines; or any omission from the guidelines or for any consequence whatsoever resulting directly or indirectly from compliance with, adoption of or reliance on guidance contained in the guidelines, even if caused by a failure to exercise reasonable care on the part of any of the aforementioned parties.

Khuyến nghị và thông tin đưa ra trong Hướng dẫn an ninh mạng trên tàu (Hướng dẫn) được dự định hoàn toàn là chỉ dẫn, được sử dụng với rủi ro riêng của người dùng. Không có sự bảo đảm hay tuyên bố nào được đưa ra, cũng không phải là nghĩa vụ cẩn trọng hoặc trách nhiệm được chấp nhận bởi Tác giả, vai trò thành viên hoặc nhân viên của bất kỳ cá nhân, hãng, công ty hoặc tổ chức nào (ai hoặc cái gì có liên quan đến việc cung cấp thông tin hoặc dữ liệu, hoặc việc biên soạn hoặc bất kỳ bản dịch, xuất bản hoặc việc cung cấp Hướng dẫn nào) về tính chính xác của bất kỳ thông tin hoặc khuyến nghị nào được đưa ra trong Hướng dẫn; hoặc bất kỳ sự thiếu sót nào từ Hướng dẫn hoặc bất kỳ hậu quả nào trực tiếp hoặc gián tiếp từ việc tuân thủ, chấp nhận hoặc phụ thuộc vào chỉ dẫn có trong Hướng dẫn, ngay cả khi được gây ra bởi việc không thực hiện chăm sóc hợp lý đối với phần của bất kỳ bên nào nói trên.

.

Table of contents

Mục lục

Page/*Trang*

Introduction
Giới thiệu

Ships are increasingly using systems that rely on digitisation, integration, and automation, which calls for cyber risk management on board. As technology continues to develop, information technology (IT) and operational technology (OT) onboard ships are being networked together - and more frequently connected to the internet.

Tàu đang sử dụng ngày càng tăng các hệ thống dựa trên số hóa, tích hợp và tự động hóa, điều này yêu cầu phải quản lý rủi ro mạng trên tàu. Khi công nghệ tiếp tục phát triển, công nghệ thông tin (IP) và công nghệ hoạt động (OT) trên tàu được kết nối với nhau - và kết nối thường xuyên hơn với internet.

This brings the greater risk of unauthorised access or malicious attacks to ships' systems and networks. Risks may also occur from personnel accessing systems on board, for example by introducing malware via removable media.

Điều này tạo ra rủi ro lớn hơn về truy cập trái phép hoặc các cuộc tấn công nguy hiểm cho hệ thống và mạng của tàu. Rủi ro cũng có thể xảy ra từ những người truy cập vào các hệ thống trên tàu, ví dụ thông qua việc giới thiệu phần mềm độc hại qua phương tiện có thể tháo lắp được.

The safety, environmental and commercial consequences of not being prepared for a cyber incident may be significant. Responding to the increased cyber threat, a group of international shipping organisations, with support from a wide range of stakeholders (please refer to annex 4 for more details), have developed these guidelines, which are designed to assist companies develop resilient approaches to cyber security onboard ships.

Những hậu quả về an toàn, môi trường và thương mại của việc không chuẩn bị cho sự cố mạng có thể là đáng kể. Để đáp lại mối đe dọa mạng đang tăng lên, một nhóm các tổ chức vận tải biển quốc tế, với sự hỗ trợ từ nhiều bên liên quan (xem phụ lục 4 để biết thêm chi tiết), đã xây dựng Hướng dẫn này nhằm trợ giúp các công ty phát triển các cách tiếp cận có khả năng thích ứng đối với an ninh mạng trên tàu.

Approaches to cyber security will be company- and ship-specific, but should be guided by appropriate standards and the requirements of relevant national regulations. The guidelines provide a risk-based approach to identifying and responding to cyber threats. An important aspect is that relevant personnel should have training in identifying the typical modus operandi of cyber attacks.

Phương pháp tiếp cận an ninh mạng sẽ là cụ thể đối với công ty và đối với tàu, nhưng phải được định hướng bởi các tiêu chuẩn thích hợp và các yêu cầu của các quy định quốc gia có liên quan. Hướng dẫn này cung cấp phương pháp tiếp cận dựa trên rủi ro để xác định và ứng phó các mối đe dọa trên mạng. Một khía cạnh quan trọng là những người có liên quan phải được đào tạo trong việc xác định các cách thức tấn công mạng điển hình.

The International Maritime Organization (IMO) has developed guidelines (MSC-FAL.1/Circ.3 on Guidelines on maritime cyber risk management) that provide high-level recommendations on maritime cyber risk management to safeguard shipping from current and emerging cyber threats and vulnerabilities. The Guidelines on Cyber Security Onboard Ships are aligned with the IMO guidelines and provide practical recommendations on maritime cyber risk management covering both cyber security and cyber safety.

Tổ chức Hàng hải quốc tế (IMO) đã xây dựng hướng dẫn (Thông tư MSC-FAL.1/Circ.3 - Hướng dẫn quản lý rủi ro mạng) cung cấp các khuyến nghị cấp độ cao về quản lý rủi ro mạng hàng hải để bảo vệ ngành vận biển trước các mối đe dọa mạng và tính dễ bị tổn thương mạng hiện thời. Hướng dẫn về an ninh mạng trên tàu phù hợp với hướng dẫn của IMO và đưa ra các khuyến nghị thực tế về quản lý rủi ro mạng hàng hải bao gồm cả an ninh mạng và an toàn mạng.

NIST framework
Khuôn khổ NIST

The National Institute of Standards and Technology, US Department of Commerce (NIST) framework has been used during the development of these guidelines. NIST aims to help understand, manage and express cyber security risks both internally and externally, for example within a ship's organisation. It can help to identify and prioritise actions for reducing cyber security risks. It is also a tool for aligning policy, business and technological approaches to manage the risks.

Khuôn khổ NIST (Viện Tiêu chuẩn và Công nghệ quốc gia (NIST), Bộ Thương mại Hoa Kỳ) đã được sử dụng trong quá trình xây dựng Hướng dẫn này. NIST nhằm mục đích giúp hiểu, quản lý và diễn đạt các rủi ro an ninh mạng cả bên trong và bên ngoài, ví dụ như trong tổ chức của một tàu. Nó có thể giúp xác định và ưu tiên các hành động để giảm rủi ro an ninh mạng. Nó cũng là một công cụ để điều chỉnh chính sách, kinh doanh và cách tiếp cận công nghệ để quản lý rủi ro.

1. Cyber security and safety management
Quản lý an toàn và an ninh mạng

Cyber safety is as significant as cyber security. Both have equal potential to affect the safety of onboard personnel, ships, and cargo. Cyber security is concerned with the protection of IT, OT and data from unauthorised access, manipulation and disruption. Cyber safety covers the risks from the loss of availability or integrity of safety critical data and OT.

An toàn mạng cũng quan trọng như an ninh mạng. Cả hai đều có khả năng tương đương để ảnh hưởng đến sự an toàn của người trên tàu, tàu và hàng hóa. An ninh mạng có liên quan đến việc bảo vệ IT, OT và dữ liệu khỏi truy cập trái phép, thao túng và gián đoạn. An toàn mạng bao gồm các rủi ro do mất tính khả dụng hoặc tính toàn vẹn của dữ liệu quan trọng về an toàn và OT.

Cyber safety incidents can arise as the result of:
Sự cố an toàn trên mạng có thể phát sinh do:

- A cyber security incident, which affects the availability and integrity of OT, for example corruption of chart data held in an Electronic Chart Display and Information System (ECDIS);

  Sự cố an ninh mạng, ảnh hưởng đến tính khả dụng và tính toàn vẹn của OT, ví dụ như sự sửa đổi làm sai lệch dữ liệu hải đồ được lưu giữ trong Hệ thống thông tin và hiển thị hải đồ điện tử (ECDIS);

- A failure occurring during software maintenance and patching;
  Sự cố xảy ra trong quá trình bảo trì và vá lỗi phần mềm;

- Loss of or manipulation of external sensor data, critical for the operation of a ship. This includes but is not limited to Global Navigation Satellite Systems (GNSS).

  Mất hoặc thao túng dữ liệu cảm biến bên ngoài quan trọng cho hoạt động của tàu. Điều này bao gồm, nhưng không giới hạn, đối với Hệ thống vệ tinh dẫn đường toàn cầu (GNSS).

Whilst the causes of a cyber safety incident may be different from a cyber security incident, an effective response to both is based upon training and awareness of appropriate company policies and procedures. So, this document aims to provide essential guidance on managing cyber safety and cyber security risks.

Trong khi nguyên nhân của sự cố an toàn mạng có thể khác với sự cố an ninh mạng, thì sự đối phó hiệu quả đối với cả hai đều dựa trên việc đào tạo và nhận thức về các chính sách và quy trình phù hợp của công ty. Vì vậy, tài liệu này nhằm mục đích cung cấp chỉ dẫn cần thiết về quản lý rủi ro an toàn mạng và an ninh mạng.

1.1 Plans and procedures
Kế hoạch và quy trình

Company plans and procedures for cyber risk management should be complementary to the existing security and safety risk management requirements contained in the ISM Code and ISPS Code. Cyber security should be considered at all levels of the company, from senior management ashore to onboard personnel, as an inherent part of the safety and security culture necessary for the safe and efficient operation of the ship.

Các kế hoạch và quy trình của công ty về quản lý rủi ro mạng phải được bổ sung cho các yêu cầu quản lý rủi ro an toàn và an ninh hiện có được quy định trong trong Bộ luật ISM và Bộ luật ISPS. An ninh mạng nên được xem xét ở mọi cấp độ của công ty, từ quản lý cấp cao trên

bờ tới những người trên tàu, như là một phần cố hữu của văn hóa an toàn và an ninh cần thiết đối với hoạt động an toàn và hiệu quả của tàu.

In accordance with chapter 8 of the ISPS Code, the ship is obliged to conduct a security assessment, which should include all operations that are important to protect. The assessment should address radio and telecommunication systems, including computer systems and networks (part B, paragraph 8.3 of the ISPS Code). This calls for controlling and monitoring "the ship to shore" path of the internet connection, which is important owing to the fast adoption of sophisticated and digitalised onboard OT systems that in many cases have not been designed to be cyber resilient.

Theo chương 8 của Bộ luật ISPS, tàu phải tiến hành đánh giá an ninh, bao gồm tất cả các hoạt động quan trọng để bảo vệ. Việc đánh giá phải đề cấp đến các hệ thống vô tuyến và viễn thông, bao gồm các hệ thống và mạng máy tính (phần B, mục 8.3 của Bộ luật ISPS). Điều này đòi hỏi phải kiểm soát và giám sát đường dẫn kết nối internet "tàu tới bờ", điều này rất quan trọng do việc áp dụng nhanh chóng các hệ thống OT số hóa phức tạp trên tàu nên trong nhiều trường hợp chưa được thiết kế để có khả năng thích ứng mạng.

The objective of the company's Safety Management System (SMS) is to provide a safe working environment by establishing appropriate safe practices and procedures based on an assessment of all identified risks to the ship, onboard personnel and the environment. In the context of ship operations, cyber incidents are anticipated to result in physical effects and potential safety and/or pollution incidents. This means that the company needs to assess risks arising from the use of IT and OT onboard ships and establish appropriate safeguards against cyber incidents.

Mục tiêu của Hệ thống quản lý an toàn (SMS) của công ty là cung cấp môi trường làm việc an toàn bằng cách thiết lập các quy trình và thực tiễn an toàn phù hợp dựa trên đánh giá tất cả các rủi ro đã xác định đối với tàu, người trên tàu và môi trường. Trong bối cảnh hoạt động của tàu, sự cố mạng được dự đoán sẽ dẫn đến các hiệu ứng vật lý và sự cố an toàn và/hoặc ô nhiễm tiềm tàng. Điều đó có nghĩa là công ty cần phải đánh giá các rủi ro phát sinh từ việc sử dụng IT và OT trên tàu và thiết lập các biện pháp bảo vệ thích hợp chống lại sự cố mạng.

The SMS should include instructions and procedures to ensure the safe operation of ships and protection of the environment in compliance with relevant international and flag state legislation. These instructions and procedures should consider risks arising from the use of IT and OT on board, as appropriate, taking into account applicable codes, guidelines and recommended standards.

SMS nên bao gồm các hướng dẫn và quy trình để đảm bảo hoạt động an toàn của tàu và bảo vệ môi trường phù hợp với pháp luật quốc tế và pháp luật quốc gia tàu mang cờ có liên quan. Các hướng dẫn và quy trình này nên xem xét các rủi ro phát sinh từ việc sử dụng IT và OT trên tàu, nếu thích hợp, lưu ý đến các bộ luật, hướng dẫn có thể áp dụng và tiêu chuẩn khuyến nghị.

When incorporating cyber risk management into the company SMS, consideration should be given to whether, in addition to a generic risk assessment of the ships it operates, a particular ship needs a specific risk assessment. The company should consider the need for a specific risk assessment based on whether a particular ship is unique within their fleet. This should consider factors, including but not limited to the extent to which IT and OT is used on board, the complexity of system integration and the nature of operations.

Khi tích hợp quản lý rủi ro mạng vào SMS của công ty, cần xem xét xem, liệu ngoài việc đánh giá rủi ro chung đối với các tàu mà công ty đang quản lý, có cần đánh giá rủi ro riêng biệt đối với một tàu cụ thể hay không. Công ty nên xem xét sự cần thiết cho việc đánh giá rủi ro riêng biệt dựa trên việc một tàu cụ thể là duy nhất trong đội tàu của công ty. Điều này nên xem xét

các yếu tố, bao gồm nhưng không giới hạn ở mức độ mà IT và OT được sử dụng trên tàu, tính phức tạp của việc tích hợp hệ thống và bản chất của hoạt động.

Cyber risk management should:
Quản lý rủi ro mạng nên

- identify the roles and responsibilities of users, key personnel, and management both ashore and on board;

  Xác định vai trò và trách nhiệm của người dùng, nhân sự chủ chốt và quản lý cả trên bờ và trên tàu;

- identify the systems, assets, data and capabilities, which if disrupted, could pose risks to the ship's operations and safety;

  Xác định các hệ thống, tài sản, dữ liệu và khả năng, nếu bị gián đoạn, có thể gây ra rủi ro cho hoạt động và an toàn của tàu;

- implement technical measures to protect against a cyber incident and ensure continuity of operations. This may include configuration of networks, access control to networks and systems, communication and boundary defence and the use of protection and detection software;

  Thực hiện các biện pháp kỹ thuật để bảo vệ chống lại sự cố mạng và đảm bảo tính liên tục của các hoạt động. Điều này có thể bao gồm cấu hình mạng, kiểm soát truy cập vào mạng và hệ thống, trao đổi thông tin, bảo vệ ranh giới và sử dụng phần mềm bảo vệ, phát hiện;

- implement activities and plans (procedural protection measures) to provide resilience against cyber incidents. This may include training and awareness, software maintenance, remote and local access, access privileges, use of removable media and equipment disposal;

  Thực hiện các hoạt động và kế hoạch (các biện pháp bảo vệ theo quy trình) để cung cấp khả năng phục hồi chống lại sự cố mạng. Điều này có thể bao gồm đào tạo và nhận thức, bảo trì phần mềm, truy cập từ xa và tại chỗ, đặc quyền truy cập, sử dụng phương tiện tháo lắp được và sử dụng thiết bị;

- implement activities to prepare for and respond to cyber incidents.
  Thực hiện các hoạt động để chuẩn bị và ứng phó với các sự cố mạng.

In recognising that some aspects of work to include cyber risk management in safety management systems may include commercially sensitive or confidential information, companies should consider protecting this information appropriately. As far as possible, policies and procedures included in a safety management system should not include sensitive information like this.

Thừa nhận rằng một số khía cạnh của công việc bao gồm quản lý rủi ro mạng trong các hệ thống quản lý an toàn có thể bao gồm thông tin nhạy cảm hoặc bí mật về mặt thương mại, các công ty nên xem xét việc bảo vệ thông tin này một cách thích hợp. Đến mức thực tế có thể được, các chính sách và quy trình được bao gồm trong hệ thống quản lý an toàn không nên bao gồm các thông tin nhạy cảm như vậy.

The development, understanding and awareness of key aspects of cyber security and safety as found in these guidelines are highlighted in figure 1.

Sự phát triển, hiểu biết và nhận thức về các khía cạnh quan trọng của an ninh và an toàn mạng trong Hướng dẫn này được mô tả trong hình 1.

Figure 1. Cyber security approach as set out in the guidelines
Hình 1. Cách tiếp cận an ninh mạng được nêu trong Hướng dẫn này

1.2 Defence in depth and in breadth
Bảo vệ theo chiều rộng và chiều sâu

Using more than one technical or procedural protection measure is recommended. It is essential to protect critical systems and data with multiple layers of protection measures which take into account the role of personnel, procedures and technology to:

Nên sử dụng nhiều hơn một biện pháp bảo vệ bằng kỹ thuật hoặc quy trình. Điều cốt yếu là bảo vệ các hệ thống và dữ liệu quan trọng bằng nhiều lớp biện pháp bảo vệ, lưu ý đến vai trò của con người, quy trình và công nghệ đối với:

- increase the probability that a cyber incident is detected;
  Tăng cường khả năng phát hiện sự cố mạng;
- increase the effort and resources required to protect information, data or the availability of IT and OT systems.

  Tăng cường nỗ lực và nguồn lực cần thiết để bảo vệ thông tin, dữ liệu hoặc tính khả dụng của các hệ thống IT và OT.

This defence in depth approach encourages a combination of:
Bảo vệ trong cách tiếp cận theo chiều sâu khuyến khích sự kết hợp của:

- physical security of the ship in accordance with the ship security plan (SSP);
  An ninh vật lý của tàu phù hợp với kế hoạch an ninh tàu (SSP);
- protection of networks, including effective segmentation;
  Bảo vệ mạng, bao gồm việc phân đoạn hiệu quả;
- intrusion detection;
  Phát hiện xâm nhập;
- software whitelisting;
  Lập danh sách trắng phần mềm;
- access and user controls;
  Kiểm soát truy cập và người dùng;
- appropriate procedures regarding the use of removable media and password policies
  Các quy trình thích hợp liên quan đến việc sử dụng các chính sách về mật khẩu và phương tiện tháo lắp được;
- personnel's awareness of the risk and familiarity with appropriate procedures.
  Nhận thức của nhân viên về rủi ro và sự thành thạo với các quy trình thích hợp.

Company policies and procedures should ensure that cyber security is considered within the overall approach to safety and security risk management. The complexity and potential persistence of cyber threats means that a "defence in depth" approach should be considered. Equipment and data protected by layers of protection measures are more resilient to cyber attacks.

Các chính sách và quy trình của công ty phải đảm bảo rằng an ninh mạng được xem xét trong tiếp cận tổng thể để quản lý rủi ro an toàn và an ninh. Sự phức tạp và khả năng tồn tại tiềm tàng của các mối đe dọa mạng có nghĩa là cần phải xem xét cách tiếp cận "bảo vệ sâu". Thiết bị và dữ liệu được bảo vệ bởi các lớp biện pháp bảo vệ có khả năng thích ứng hơn trước các tấn công mạng.

However, onboard ships where levels of integration between cyber systems may be high, defence in depth only works if technical and procedural protection measures are applied in layers across all vulnerable and integrated systems. This is "defence in breadth" and it is used to prevent any vulnerabilities in one system being used to circumvent protection measures of another system.

Tuy nhiên, trên tàu có mức độ tích hợp giữa các hệ thống mạng có thể cao, việc bảo vệ theo chiều sâu chỉ hoạt động nếu các biện pháp bảo vệ kỹ thuật và theo quy trình được áp dụng trong các lớp trên tất cả các hệ thống tích hợp và dễ bị tổn thương. Đây là "bảo vệ rộng" và nó được sử dụng để ngăn chặn bất kỳ lỗ hổng nào trong một hệ thống được sử dụng để phá vỡ các biện pháp bảo vệ của hệ thống khác.

Defence in depth and defence in breadth are complementary approaches which, when implemented together, provide the foundation of a holistic response to the management of cyber risks.

Bảo vệ sâu và rộng là cách tiếp cận bổ sung, khi được thực hiện cùng nhau, tạo ra nền tảng cho các biện pháp toàn diện đối với việc quản lý rủi ro mạng.

2. Identify threats
Nhận biết các đe dọa

The cyber risk is specific to the company, ship, operation and/or trade. When assessing the risk, companies should be aware of any specific aspects of their operations that might increase their vulnerability to cyber incidents.

Rủi ro mạng mang tính cụ thể đối với công ty, tàu, hoạt động và/hoặc thương mại. Khi đánh giá rủi ro, các công ty nên nhận thức được bất kỳ khía cạnh cụ thể nào trong hoạt động của công ty có thể làm tăng tính dễ bị tổn thương của họ đối với sự cố mạng.

Unlike other areas of safety and security where historic evidence is available and reporting of incidents is required, cyber security is made more challenging by the absence of any definitive information about the incidents and their impact. Until this evidence is obtained, the scale and frequency of attacks will continue to be unknown.

Không giống như các lĩnh vực an toàn và an ninh khác, nơi có bằng chứng lịch sử và báo cáo sự cố được yêu cầu, an ninh mạng được thực hiện khó khăn hơn do không có bất kỳ thông tin dứt khoát nào về sự cố và tác động của chúng. Cho đến khi có bằng chứng này, quy mô và tần suất tấn công sẽ tiếp tục không rõ.

Experiences from other business sectors such as financial institutions, public administration and air transport have shown that successful cyber attacks might result in a significant loss of services, assets and even endanger human lives. Such events argue that the shipping industry should also work proactively to understand and mitigate cyber threats.

Kinh nghiệm từ các lĩnh vực kinh doanh khác như các tổ chức tài chính, hành chính công và vận tải hàng không đã cho thấy các cuộc tấn công mạng thành công có thể dẫn đến tổn thất đáng kể về dịch vụ, tài sản và thậm chí gây nguy hiểm cho sinh mạng con người. Những sự kiện như vậy cho thấy ngành vận tải biển cũng nên chủ động tìm hiểu và làm giảm thiểu các mối đe dọa mạng.

There are motives for organisations and individuals to exploit cyber vulnerabilities. The following examples give some indication of the threat posed and the potential consequences for companies and the ships they operate:

Có những động cơ cho các tổ chức và cá nhân khai thác lỗ hổng mạng (tính dễ bị tổn thương mạng). Các ví dụ sau đây đưa ra một số dấu hiệu của mối đe dọa đặt ra và những hậu quả tiềm tàng cho các công ty và các tàu mà họ khai thác:

Group ***Nhóm***	**Motivation** ***Động cơ***	**Objective** ***Mục đích***
Activists (including disgruntled employees) *Các nhà hoạt động (bao gồm cả các nhân viên bất mãn)*	• Reputational damage *Thiệt hại danh tiếng* • Disruption of operations *Gián đoạn hoạt động*	• Destruction of data *Tiêu hủy dữ liệu* • Publication of sensitive data *Công bố dữ liệu nhạy cảm* • Media attention *Gây sự chú ý của truyền thông* • Denial of access to the service or system targeted *Từ chối quyền truy cập vào dịch vụ hoặc hệ thống*

		được nhắm tới
Criminals *Tội phạm*	• Financial gain *Lợi ích tài chính* • Commercial espionage *Gián điệp thương mại* • Industrial espionage *Gián điệp công nghiệp*	• Selling stolen data *Bán dữ liệu đánh cắp* • Ransoming stolen data *Đòi tiền chuộc đối với dữ liệu bị đánh cắp* • Ransoming system operability *Đòi tiền chuộc đối với khả năng hoạt động của hệ thống* • Arranging fraudulent transportation of cargo *Bố trí vận chuyển hàng hóa gian lận* • Gathering intelligence for more sophisticated crime, exact cargo location, off vessel transportation and handling plans etc *Thu thập thông tin tình báo cho tội phạm tinh vi hơn, vị trí chính xác của hàng hóa, kế hoạch vận chuyển tàu và điều động tàu, ...*
Opportunists *Người cơ hội*	• The challenge *Các thách thức*	• Getting through cyber security defences *Vượt qua bảo vệ an ninh mạng* • Financial gain *Lợi ích tài chính*
States *Các quốc gia* State sponsored organisations *Các tổ chức được nhà nước tài trợ* Terrorists *Khủng bố*	• Political gain *Lợi ích chính trị* • Espionage *Gián điệp*	• Gaining knowledge *Đạt được kiến thức* • Disruption to economies and critical national infrastructure *Sự gián đoạn đối với nền kinh tế và cơ sở hạ tầng quốc gia quan trọng*

Table 1. Motivation and objectives
Bảng 1. Động cơ và mục đích

The groups in Table 1 are active and have the skills and resources to threaten the safety and security of ships, and a company's ability to conduct its business.

Các nhóm trong Bảng 1 đang hoạt động và có các kỹ năng, nguồn lực để đe dọa an toàn, an ninh của tàu và khả năng của công ty để tiến hành việc kinh doanh của mình.

In addition, there is the possibility that company personnel, on board and ashore, could compromise cyber systems and data. In general, the company should be prepared that this may be unintentional and caused by human error when operating and managing IT and OT systems or failure to respect technical and procedural protection measures. There is,

however, the possibility that actions may be malicious and are a deliberate attempt to damage the company and the ship that is by a disgruntled employee.

Ngoài ra, có khả năng nhân viên của công ty, trên tàu và trên bờ, có thể xâm phạm các hệ thống và dữ liệu trên mạng. Nói chung, công ty nên chuẩn bị là điều này có thể không chủ ý và gây ra bởi lỗi của con người khi vận hành, quản lý các hệ thống IT, OT hoặc không tôn trọng các biện pháp bảo vệ bằng kỹ thuật và bằng quy trình. Tuy nhiên, có khả năng các hành động có thể là hiểm độc và là một nỗ lực có chủ ý làm tổn hại công ty và tàu gây ra bởi nhân viên bất mãn.

Types of cyber attack
Các loại tấn công mạng

In general, there are two categories of cyber attacks, which may affect companies and ships:
Nói chung, có hai loại tấn công mạng, có thể ảnh hưởng đến các công ty và tàu:

- untargeted attacks, where a company or a ship's systems and data are one of many potential targets

  Các cuộc tấn công không nhắm mục tiêu, nơi mà hệ thống và dữ liệu của công ty hoặc của tàu là một trong nhiều mục tiêu tiềm năng

- targeted attacks, where a company or a ship's systems and data are the intended target.

  Các cuộc tấn công nhắm mục tiêu, nơi mà hệ thống và dữ liệu của công ty hoặc của tàu là mục tiêu dự định.

Untargeted attacks are likely to use tools and techniques available on the internet which can be used to locate, discover and exploit widespread vulnerabilities which may also exist in a company and onboard a ship. Examples of some tools and techniques that may be used in these circumstances include:

Các cuộc tấn công không nhắm mục tiêu có thể sử dụng các công cụ và kỹ thuật có sẵn trên internet có thể được sử dụng để định vị, phát hiện và khai thác các lỗ hổng phổ biến cũng có thể tồn tại tại công ty và trên tàu. Ví dụ về một số công cụ và kỹ thuật có thể được sử dụng trong những trường hợp này bao gồm:

- **Malware:** Malicious software which is designed to access or damage a computer without the knowledge of the owner. There are various types of malware including trojans, ransomware, spyware, viruses, and worms. Ransomware encrypts data on systems until a ransom has been paid. Malware may also exploit known deficiencies and problems in outdated/unpatched business software. The term exploit usually refers to the use of a software or code, which is designed to take advantage and manipulate a problem in another computer software or hardware. This problem can, for example, be a code bug, system vulnerability, improper design, hardware malfunction, and error in protocol implementation. These vulnerabilities may be exploited remotely or triggered locally. Locally, a piece of malicious code may often be executed by the user, sometimes via links distributed in email attachments or through malicious websites.

  Phần mềm độc hại: *Phần mềm độc hại được thiết kế để truy cập hoặc làm hỏng máy tính mà người dùng không biết. Có nhiều loại phần mềm độc hại khác nhau bao gồm trojans, ransomware, spyware, viruses và worms. Phần mềm đòi tiềm chuộc (ransomware) mã hóa dữ liệu trên hệ thống cho đến khi khoản tiền chuộc được thanh toán. Phần mềm độc hại cũng có thể khai thác những thiếu sót và sự cố*

đã biết trong phần mềm doanh nghiệp đã lỗi thời/chưa được vá. Thuật ngữ khai thác thường đề cập đến việc sử dụng phần mềm hoặc mã, được thiết kế để tận dụng và xử lý sự cố trong phần mềm hoặc phần cứng máy tính khác. Ví dụ, vấn đề này có thể là lỗi mã, lỗ hổng hệ thống, thiết kế không đúng, lỗi phần cứng và lỗi trong triển khai giao thức. Các lỗ hổng này có thể được khai thác từ xa hoặc được kích hoạt cục bộ. Tại chỗ, một đoạn mã độc hại thường có thể được thực thi bởi người dùng, đôi khi thông qua các liên kết được phân phối trong tệp đính kèm email hoặc thông qua các trang web độc hại.

- **Social engineering:** A non-technical technique used by potential cyber attackers to manipulate insider individuals into breaking security procedures, normally, but not exclusively, through interaction via social media.

  Kỹ thuật xã hội: *Kỹ thuật phi kỹ thuật được các kẻ tấn công mạng tiềm năng sử dụng để thao túng các cá nhân nội bộ vào việc làm gián đoạn các quy trình an ninh, thông thường, nhưng không duy nhất, thông qua tương tác qua phương tiện truyền thông xã hội.*

- **Phishing:** Sending emails to a large number of potential targets asking for particular pieces of sensitive or confidential information. Such an email may also request that a person visits a fake website using a hyperlink included in the email.

  Lừa đảo: *Gửi email đến một số lượng lớn các mục tiêu tiềm năng yêu cầu các thông tin nhạy cảm hoặc bí mật cụ thể. Email như vậy cũng có thể yêu cầu một người truy cập trang web giả mạo bằng cách sử dụng siêu liên kết được bao gồm trong email.*

- **Water holing:** Establishing a fake website or compromising a genuine website to exploit visitors.

  Tạo lỗ nước (Water holing): *Thiết lập một trang web giả mạo hoặc xâm phạm một trang web chính hãng để khai thác khách truy cập.*

- **Scanning:** Attacking large portions of the internet at random.
  Quét: *Tấn công các phần lớn của internet một cách ngẫu nhiên.*

Targeted attacks may be more sophisticated and use tools and techniques specifically created for targeting a company or ship. Examples of tools and techniques which may be used in these circumstances include:

Các cuộc tấn công được nhắm mục tiêu có thể phức tạp hơn và sử dụng các công cụ và kỹ thuật được tạo cụ thể để nhắm mục tiêu là một công ty hoặc tàu. Ví dụ về các công cụ và kỹ thuật có thể được sử dụng trong những trường hợp này bao gồm:

- **Brute force:** An attack trying many passwords with the hope of eventually guessing correctly. The attacker systematically checks all possible passwords until the correct one is found.

  Lực lượng vũ phu: *Một cuộc tấn công thử nhiều mật khẩu với hy vọng cuối cùng cũng đoán đúng. Kẻ tấn công kiểm tra một cách hệ thống tất cả các mật khẩu có thể cho đến khi tìm thấy đúng mật khẩu.*

- **Denial of service (DoS):** prevents legitimate and authorised users from accessing information, usually by flooding a network with data. A distributed denial of service (DDoS) attack takes control of multiple computers and/or servers to implement a DoS attack.

Từ chối dịch vụ (DoS): *ngăn người dùng hợp pháp và được ủy quyền truy cập thông tin, thường là do làm tràn ngập mạng có dữ liệu. Một cuộc tấn công từ chối dịch vụ (DDoS) phân tán sẽ kiểm soát nhiều máy tính và/hoặc máy chủ để thực hiện một cuộc tấn công DoS.*

- **Spear-phishing:** Like phishing but the individuals are targeted with personal emails, often containing malicious software or links that automatically download malicious software.

  Spear-phishing: *Giống như lừa đảo nhưng các cá nhân được nhắm mục tiêu bằng email cá nhân, thường chứa phần mềm độc hại hoặc liên kết tự động tải xuống phần mềm độc hại.*

- **Subverting the supply chain:** Attacking a company or ship by compromising equipment, software or supporting services being delivered to the company or ship.

  Phá hoại chuỗi cung ứng: *Tấn công một công ty hoặc tàu bằng cách xâm phạm thiết bị, phần mềm hoặc dịch vụ hỗ trợ đang được giao cho công ty hoặc tàu đó.*

The above examples are not exhaustive. Other methods are evolving for example impersonating a legitimate shore based employee in a shipping company to obtain valuable information, which can be used for a further attack. The potential number and sophistication of tools and techniques used in cyber attacks continue to evolve and are limited only by the ingenuity of those organizations and individuals developing them.

Các ví dụ trên không phải là toàn diện. Các phương pháp khác đang phát triển ví dụ như mạo danh một nhân viên trên bờ hợp pháp trong một công ty vận tải biển để có được thông tin giá trị, có thể được sử dụng để tấn công tiếp theo. Số lượng tiềm năng và sự phức tạp của các công cụ và kỹ thuật được sử dụng trong các cuộc tấn công mạng tiếp tục phát triển và chỉ bị giới hạn bởi kỹ năng của các tổ chức đó và các cá nhân phát triển chúng.

Stages of a cyber attack
Các giai đoạn tấn công mạng

Cyber attacks are conducted in stages. The length of time taken to prepare a cyber attack can be determined by the motivations and objectives of the attacker, and the resilience of technical and procedural cyber security controls implemented by the company, including those onboard its ships. The four stages of an attack are:

Các cuộc tấn công mạng được thực hiện theo từng giai đoạn. Thời gian để chuẩn bị tấn công mạng có thể được xác định bởi động cơ và mục đích của kẻ tấn công, và khả năng phục hồi việc kiểm soát an ninh bằng kỹ thuật và quy trình do công ty thực hiện, bao gồm cả các nội dung liên quan trên tàu của công ty. Bốn giai đoạn của một cuộc tấn công là:

- **Survey/reconnaissance:** Open/public sources used to gain information about a company, ship or seafarer, which can be used to prepare for a cyber attack. Social media, technical forums and hidden properties in websites, documents and publications may be used to identify technical, procedural and physical vulnerabilities. The use of open/public sources may be complemented by monitoring (analysing - sniffing) the actual data flowing into and from a company or a ship.

  Khảo sát/trinh sát: *Các nguồn mở/công cộng được sử dụng để lấy thông tin về một công ty, tàu hoặc thuyền viên, có thể được sử dụng để chuẩn bị cho cuộc tấn công*

trên mạng. Phương tiện truyền thông xã hội, diễn đàn kỹ thuật và tài sản ẩn trong các trang web, tài liệu và ấn phẩm có thể được sử dụng để xác định các lỗ hổng về mặt kỹ thuật, quy trình và vật lý. Việc sử dụng các nguồn mở/công cộng có thể được bổ sung bằng cách giám sát (phân tích - nghe lén) dữ liệu thực tế vào và từ một công ty hoặc tàu.

- **Delivery:** Attackers may attempt to access company and ship systems and data. This may be done from either within the company or ship or remotely through connectivity with the internet. Examples of methods used to obtain access include:

  Phân phát: *Những kẻ tấn công có thể cố gắng truy cập vào hệ thống và dữ liệu của công ty và tàu. Điều này có thể được thực hiện từ bên trong công ty hoặc tàu hoặc từ xa thông qua kết nối với internet. Ví dụ về các phương pháp được sử dụng để có được quyền truy cập bao gồm:*

  - company online services, including cargo or consignment tracking systems;

    Các dịch vụ trực tuyến của công ty, bao gồm hệ thống theo dõi hàng hóa hoặc lô hàng ký gửi;

  - sending emails containing malicious files or links to malicious websites to personnel;

    Gửi email chứa các tệp độc hại hoặc liên kết đến các trang web độc hại tới nhân viên;

  - providing infected removable media, for example as part of a software update to an onboard system;

    Cung cấp phương tiện tháo lắp được bị nhiễm độc, ví dụ như một phần của bản cập nhật phần mềm cho hệ thống trên tàu;

  - creating false or misleading websites which encourage the disclosure of user account information by personnel.

    Tạo các trang web giả mạo hoặc gây hiểu lầm khuyến khích tiết lộ thông tin tài khoản người dùng của nhân viên.

- **Breach:** The extent to which an attacker can breach a company or ship system will depend on the significance of the vulnerability found by an attacker and the method chosen to deliver an attack. It should be noted that a breach might not result in any obvious changes to the status of the equipment. Depending on the significance of the breach, an attacker may be able to:

  Vi phạm: *Mức độ mà kẻ tấn công có thể vi phạm một công ty hoặc hệ thống tàu sẽ phụ thuộc vào tầm quan trọng của lỗ hổng do kẻ tấn công tìm thấy và phương pháp được chọn để cung cấp một cuộc tấn công. Cần lưu ý rằng một sự vi phạm có thể không dẫn đến bất kỳ thay đổi rõ ràng nào về trạng thái của thiết bị. Tùy thuộc vào tầm quan trọng của vi phạm, kẻ tấn công có thể:*

  - make changes that affect the system's operation, for example interrupt or manipulate information used by navigation equipment;

    Thực hiện các thay đổi ảnh hưởng đến hoạt động của hệ thống, ví dụ như làm gián đoạn hoặc thao túng thông tin được sử dụng bởi thiết bị hành hải;

  - gain access to commercially sensitive data such as cargo manifests and/or crew and passenger lists;

    Truy cập vào các dữ liệu nhạy cảm về mặt thương mại như các bản kê khai hàng hóa và/hoặc danh sách thuyền viên và hành khách;

- achieve full control of a system, for example a machinery management system.

  Đạt được toàn quyền kiểm soát hệ thống, ví dụ như hệ thống quản lý máy móc.

- **Effect:** The motivation and objectives of the attacker will determine what effect they have on the company or ship system and data. An attacker may explore systems, expand access and/or ensure that they are able to return to the system in order to:

  Hiệu ứng: *Động cơ và mục đích của kẻ tấn công sẽ xác định hiệu ứng của chúng trên hệ thống hoặc dữ liệu của công ty hoặc tàu. Kẻ tấn công có thể khám phá hệ thống, mở rộng quyền truy cập và/hoặc đảm bảo rằng họ có thể quay lại hệ thống để:*

  - access commercially sensitive or confidential data about cargo, crew and passengers to which they would otherwise not have access;

    Truy cập dữ liệu nhạy cảm về mặt thương mại hoặc bí mật về hàng hóa, thuyền viên và hành khách mà họ không có quyền truy cập;

  - manipulate crew or passenger lists, or cargo manifests. This may be used to allow the fraudulent transport of illegal cargo, or facilitate thefts;

    Thao túng danh sách thuyền viên hoặc hành khách, hoặc bản kê khai hàng hóa. Điều này có thể được sử dụng để cho phép vận chuyển hàng giả bất hợp pháp, hoặc tạo điều kiện cho việc trộm cắp;

  - cause complete denial of service on business systems;

    Gây ra sự từ chối dịch vụ hoàn toàn trên các hệ thống kinh doanh;

  - enable other forms of crime for example piracy, theft and fraud;

    Cho phép các hình thức tội phạm khác ví dụ như cướp biển, trộm cắp và gian lận;

  - disrupt normal operation of the company and ship systems, for example by deleting critical pre-arrival information or overloading company systems.

    Làm gián đoạn hoạt động bình thường của hệ thống công ty và tàu, ví dụ bằng cách xóa thông tin trước khi tàu đến quan trọng hoặc làm cho hệ thống của công ty quá tải.

It is crucial that users of IT systems onboard ships are aware of the potential cyber security risks, and are trained to identify and mitigate such risks.

Điều quan trọng là người dùng hệ thống IT trên tàu phải biết về các rủi ro an ninh mạng tiềm ẩn và được đào tạo để xác định và làm giảm thiểu các rủi ro đó.

3. Identify vulnerabilities
Nhận biết các lỗ hổng (tính dễn bị tổn thương)

It is recommended that a shipping company initially performs an assessment of the potential threats that may realistically be faced. This should be followed by an assessment of the systems and onboard procedures to map their robustness to handle the current level of threat. These vulnerability assessments should then serve as the foundation for a senior management level discussion/workshop. It may be facilitated by internal experts or supported by external experts with knowledge of the maritime industry and its key processes, resulting in a strategy centred around the key risks. The distinction between IT and OT systems should be considered. IT systems focus on the use of data as information whilst OT systems focus on the use of data to control or monitor physical processes.

Khuyến nghị công ty vận tải biển ban đầu thực hiện việc đánh giá về các mối đe dọa tiềm năng mà thực tế có thể phải đối mặt. Điều này nên được theo sau bằng việc đánh giá các hệ thống và các quy trình trên tàu để vạch ra giải pháp thiết thực nhằm xử lý mức độ mối đe dọa hiện tại. Việc đánh giá lỗ hổng (tính dễ bị tổn thương) này tiếp theo tạo ra nền tảng cho việc thảo luận/hội thảo của cấp quản lý cấp cao. Công việc này có thể được tạo điều kiện thuận lợi bởi các chuyên gia nội bộ hoặc được hỗ trợ bởi các chuyên gia bên ngoài với kiến thức về ngành hàng hải và các quá trình chính của nó, dẫn đến một chiến lược tập trung vào những rủi ro chính. Sự khác biệt giữa các hệ thống IT và OT nên được xem xét. Các hệ thống IT tập trung vào việc sử dụng dữ liệu như thông tin, trong khi các hệ thống OT tập trung vào việc sử dụng dữ liệu để kiểm soát hoặc theo dõi các quá trình vật lý.

Stand-alone systems will be less vulnerable to external cyber attacks compared to those attached to uncontrolled networks or directly to the internet. Network design and network segregation will be explained in more detail in annex 2. Care should be taken to understand how critical shipboard systems might be connected to uncontrolled networks. When doing so, the human element should be taken into consideration, as many incidents are initiated by personnel's actions. Onboard systems could include:

Các hệ thống độc lập sẽ ít bị tổn thương hơn bởi các cuộc tấn công mạng bên ngoài so với các hệ thống được kết nối với các mạng không được kiểm soát hoặc trực tiếp lên internet. Thiết kế mạng và cách ly mạng sẽ được giải thích chi tiết hơn trong phụ lục 2. Cần chú ý để hiểu các hệ thống trên tàu quan trọng có thể được kết nối với các mạng không được kiểm soát như thế nào. Khi làm như vậy, yếu tố con người nên được xem xét, vì nhiều sự cố được khởi xướng bởi các hành động của nhân viên. Các hệ thống trên tàu có thể bao gồm:

- **Cargo management systems**: Digital systems used for the management and control of cargo, including hazardous cargo, may interface with a variety of systems ashore. Such systems may include shipment-tracking tools available to shippers via the internet. Interfaces of this kind make cargo management systems and data in cargo manifests vulnerable to cyber attacks.

  Hệ thống quản lý hàng hóa: *Các hệ thống kỹ thuật số được sử dụng để quản lý và kiểm soát hàng hóa, bao gồm hàng hóa nguy hiểm, có thể giao tiếp với nhiều hệ thống khác nhau trên bờ. Các hệ thống này có thể bao gồm các công cụ theo dõi lô hàng có sẵn cho các người gửi hàng thông qua internet. Giao diện của loại này làm cho hệ thống quản lý hàng hóa và dữ liệu trongbản kê hàng hóa biểu hiện dễ bị tổn thương do tấn công mạng.*

- **Bridge systems:** The increasing use of digital, network navigation systems, with interfaces to shoreside networks for update and provision of services, make such systems vulnerable to cyber attacks. Bridge systems that are not connected to other networks may be equally vulnerable, as removable media are often used to update such systems from other controlled or uncontrolled networks. A cyber incident can extend to service denial or manipulation, and therefore may affect all systems associated with navigation, including ECDIS, GNSS, AIS, VDR and Radar/ARPA.

  Hệ thống buồng lái: Việc sử dụng ngày càng tăng các hệ thống hành hải mạng kỹ thuật số, với giao diện với các mạng trên bờ để cập nhật và cung cấp dịch vụ, làm cho các hệ thống như vậy dễ bị tổn thương do tấn công mạng. Các hệ thống buồng lái không được kết nối với các mạng khác có thể dễ bị tổn thương tương đương, vì các phương tiện di động (tháo lắp được) thường được sử dụng để cập nhật cho các hệ thống như vậy từ các mạng được kiểm soát hoặc không được kiểm soát khác. Một sự cố mạng có thể mở rộng để từ chối dịch vụ hoặc thao túng, và do đó có thể ảnh hưởng đến tất cả các hệ thống liên kết với hành hải, bao gồm ECDIS, GNSS, AIS, VDR và Radar/ARPA.

- **Propulsion and machinery management and power control systems:** The use of digital systems to monitor and control onboard machinery, propulsion and steering make such systems vulnerable to cyber attacks. The vulnerability of these systems can increase when they are used in conjunction with remote condition-based monitoring and/or are integrated with navigation and communications equipment on ships using integrated bridge systems.

  Quản lý máy móc, thiết bị đẩy tàu và hệ thống kiểm soát năng lượng: *Việc sử dụng các hệ thống kỹ thuật số để giám sát và kiểm soát máy móc, thiết bị đẩy và thiết bị lái trên tàu khiến các hệ thống này dễ bị tổn thương do tấn công mạng. Tính dễ bị tổn thương của các hệ thống này có thể tăng lên khi chúng được sử dụng kết hợp với giám sát dựa trên điều kiện từ xa và/hoặc được tích hợp với thiết bị hành hải và thông tin liên lạc trên tàu sử dụng hệ thống buồng lái tích hợp.*

- **Access control systems:** Digital systems used to support access control to ensure physical security and safety of a ship and its cargo, including surveillance, shipboard security alarm, and electronic “personnel-on-board” systems.

  Hệ thống kiểm soát tiếp cận: *Các hệ thống kỹ thuật số được sử dụng để hỗ trợ kiểm soát tiếp cận để đảm bảo an toàn, an ninh vật lý của tàu và hàng hóa, bao gồm giám sát, báo động an ninh trên tàu và hệ thống "nhân sự trên tàu" điện tử.*

- **Passenger servicing and management systems:** Digital systems used for property management, boarding and access control may hold valuable passenger related data. Intelligent devices (tablets, handheld scanners etc.) are themselves an attack vector as ultimately the collected data is passed on to other systems.

  Các hệ thống phục vụ và quản lý hành khách: *Các hệ thống kỹ thuật số được sử dụng để quản lý tài sản, kiểm soát việc tiếp cận và lên tàu có thể chứa dữ liệu có liên quan đến hành khách có giá trị. Bản thân các thiết bị thông minh (máy tính bảng, máy quét cầm tay, ...) là vật thể tấn công vì cuối cùng, dữ liệu thu thập được chuyển sang các hệ thống khác.*

- **Passenger facing public networks:** Fixed or wireless networks connected to the internet, installed on board for the benefit of passengers, for example guest entertainment systems. These systems should be considered uncontrolled and should not be connected to any safety critical system on board.

  Mạng công cộng dùng cho hành khách: *Mạng cố định hoặc không dây kết nối với internet, được lắp đặt trên tàu dành cho hành khách, ví dụ như hệ thống giải trí cho khách. Các hệ thống này nên được coi là không kiểm soát được và không được kết nối với bất kỳ hệ thống an toàn quan trọng nào trên tàu.*

- **Administrative and crew welfare systems:** Onboard computer networks used for administration of the ship or the welfare of the crew are particularly vulnerable when they provide internet access and email. They can be exploited by cyber attackers to gain access to onboard systems and data. These systems should be considered uncontrolled and should not be connected to any safety critical system on board. Software provided by ship management companies or owners is also included in this category.

  Hệ thống hành chính và phúc lợi cho thyền viên: *Các mạng máy tính trên tàu được sử dụng cho công việc hành chính trên tàu hoặc phúc lợi cho thuyền viên đặc biệt dễ bị tổn thương khi chúng cung cấp truy cập internet và email. Chúng có thể được khai thác bởi những kẻ tấn công mạng để truy cập vào các hệ thống và dữ liệu trên tàu. Các hệ thống này nên được coi là không kiểm soát được và không được kết nối với bất kỳ hệ thống an toàn quan trọng nào trên tàu. Phần mềm do các công ty quản lý tàu hoặc chủ tàu cung cấp cũng được bao gồm trong danh mục này.*

- **Communication systems:** Availability of internet connectivity via satellite and/or other wireless communication can increase the vulnerability of ships. The cyber defence mechanisms implemented by the service provider should be carefully considered but should not be solely relied upon to secure every shipboard systems and data.

  Hệ thống thông tin liên lạc: *Khả năng kết nối internet thông qua vệ tinh và/hoặc thông tin liên lạc không dây khác có thể làm tăng tính dễ bị tổn thương của tàu. Các cơ chế bảo vệ mạng được thực hiện bởi nhà cung cấp dịch vụ nên được xem xét cẩn thận nhưng không nên chỉ dựa vào đó để bảo vệ mọi hệ thống và dữ liệu của tàu.*

The above-mentioned onboard systems consist of potentially vulnerable equipment which should be reviewed during the assessment. More detail can be found in annex 1 of these guidelines.

Các hệ thống trên tàu nói trên bao gồm các thiết bị dễ bị tổn thương tiềm tàng cần được xem xét trong quá trình đánh giá. Chi tiết hơn có thể được tìm thấy trong phụ lục 1 của Hướng dẫn này.

3.1 Ship to shore interface
Giao diện tàu đến bờ

Ships are becoming more and more integrated with shoreside operations because digital communication is being used to conduct business, manage operations, and stay in touch with head office. Further, critical ship systems essential to the safety of navigation, power and cargo management have been increasingly digitalised and connected to the internet to perform a wide variety of legitimate functions such as:

Các tàu ngày càng trở nên tích hợp hơn với các hoạt động trên bờ vì thông tin liên lạc kỹ thuật số đang được sử dụng để tiến hành kinh doanh, quản lý hoạt động và giữ liên lạc với trụ sở chính. Hơn nữa, các hệ thống tàu quan trọng cần thiết cho an toàn hành hải, quản lý hàng hóa và năng lượng ngày càng được số hoá và kết nối với internet để thực hiện nhiều chức năng hợp pháp như:

- engine performance monitoring;
  Giám sát việc thực hiện chức năng của động cơ;
- maintenance and spare parts management;
  Bảo trì và quản lý phụ tùng;
- cargo, crane and pump management;
  Quản lý hàng hóa, cần cẩu và bơm;
- voyage performance monitoring.
  Giám sát việc thực hiện chức năng chuyến đi.

The above list provides examples of this interface and is not exhaustive. The above systems provide data which may be of interest to cyber criminals to exploit.

Danh sách trên cung cấp các ví dụ về giao diện này và không phải là toàn diện. Các hệ thống trên cung cấp dữ liệu mà các tội phạm mạng có thể quan tâm để khai thác.

Modern technologies can add vulnerabilities to the ships especially if there are insecure designs of networks and uncontrolled access to the internet. Additionally, shoreside and onboard personnel may be unaware how some equipment producers maintain remote access to shipboard equipment and its network system. The risks of misunderstood, unknown, and uncoordinated remote access to an operating ship should be taken into consideration as an important part of the risk assessment.

Công nghệ hiện đại có thể thêm lỗ hổng cho các tàu, đặc biệt là nếu có thiết kế không an toàn của mạng và truy cập không được kiểm soát vào internet. Ngoài ra, nhân viên bên bờ và trên tàu có thể không biết cách thức một số nhà sản xuất thiết bị duy trì việc truy cập từ xa vào thiết bị trên tàu và hệ thống mạng của họ. Những rủi ro của việc truy cập từ xa bị hiểu lầm, không xác định và không phối hợp đến tàu đang hoạt động sẽ được xem xét như một phần quan trọng trong đánh giá rủi ro.

It is recommended that companies should fully understand the ship's OT and IT systems and how these systems connect and integrate with the shore side. This requires an understanding of all computer based onboard systems and how safety, operations, and business can be compromised by a cyber incident.

Khuyến nghị các công ty nên hiểu đầy đủ về hệ thống OT và IT của tàu và cách các hệ thống này kết nối và tích hợp với bờ. Điều này đòi hỏi sự hiểu biết về tất cả các hệ thống trên tàu dựa

trên máy tính và làm thế nào an toàn, hoạt động và kinh doanh có thể bị tổn hại bởi sự cố mạng.

The following should be considered regarding producers and third parties including contractors and service providers:

Các nội dung sau đây cần được xem xét liên quan đến nhà sản xuất và bên thứ ba bao gồm các nhà thầu và nhà cung cấp dịch vụ:

1. The producer's and service provider's cyber security awareness and procedures: Many of these companies lack cyber awareness training and governance in their own organisations and this may represent more sources of vulnerability, which could result in cyber incidents. The companies should have an updated cyber security company policy, which includes training and governance procedures for accessible IT and OT onboard systems.

   Các quy trình và nhận thức về an ninh mạng của nhà sản xuất và nhà cung cấp dịch vụ: Nhiều trong số những công ty này thiếu đào tạo nhận thức về mạng và quản trị trong tổ chức của họ và điều này có thể tạo ra nhiều nguồn lỗ hổng (tính dễ bị tổn thương) hơn, có thể dẫn đến sự cố mạng. Các công ty nên có một chính sách an ninh mạng của công ty được cập nhật, bao gồm các quy trình đào tạo và quản trị cho các hệ thống IT và OT trên tàu có thể tiếp cận được.

2. The maturity of a third-party's cyber security procedures: The shipowner should query the internal governance for cyber network security, and seek to obtain a cyber security assurance when considering future contracts and services. This is particularly important when covering network security if the ship is to be interfaced with the third-party.

   Tính cẩn thận của quy trình an ninh mạng của bên thứ ba: Chủ tàu nên truy vấn quản trị nội bộ về an ninh mạng và tìm cách đạt được sự bảo đảm an ninh mạng khi xem xét các hợp đồng và dịch vụ trong tương lai. Điều này đặc biệt quan trọng khi bảo vệ an ninh mạng nếu tàu được giao tiếp với bên thứ ba.

Common vulnerabilities
Lỗ hổng phổ biến

The following are common cyber vulnerabilities, which may be found onboard existing ships, and on some newbuild ships:

Sau đây là các lỗ hổng mạng phổ biến, có thể tìm thấy trên các tàu hiện có và trên một số tàu mới:

- obsolete and unsupported operating systems;
  Hệ điều hành lỗi thời và không được hỗ trợ;
- outdated or missing antivirus software and protection from malware;
  Phần mềm chống vi rút và bảo vệ khỏi phần mềm độc hại bị lỗi thời hoặc thiếu;
- inadequate security configurations and best practices, including ineffective network management and the use of default administrator accounts and passwords, and ineffective network management which is not based on the principle of least privilege;

Cấu hình bảo mật và các thực hành tốt nhất không đầy đủ, bao gồm quản lý mạng không hiệu quả, sử dụng tài khoản và mật khẩu người quản trị mặc định, quản lý mạng không hiệu quả không dựa trên nguyên tắc đặc quyền tối thiểu;

- shipboard computer networks, which lack boundary protection measures and segmentation of networks;

  Mạng máy tính trên tàu thiếu các biện pháp bảo vệ ranh giới và phân đoạn mạng;

- safety critical equipment or systems always connected with the shore side;
  Thiết bị hoặc hệ thống quan trọng về an toàn luôn được kết nối với bờ;

- inadequate access controls for third parties including contractors and service providers.

  Kiểm soát truy cập không đầy đủ cho bên thứ ba bao gồm nhà thầu và nhà cung cấp dịch vụ.

4. Assess risk exposure
Đánh giá phơi nhiễm rủi ro

Accountability and ownership for cyber security assessment should start at senior management level of a company, instead of being immediately delegated to the ship security officer or the head of the IT department. There are several reasons for this:

Trách nhiệm và quyền sở hữu để đánh giá an ninh mạng nên bắt đầu ở cấp quản lý cấp cao của công ty, thay vì được ủy quyền ngay lập tức cho sỹ quan an ninh tàu hoặc người đứng đầu bộ phận IT. Có một vài nguyên nhân cho vấn đề này:

1. Initiatives to heighten cyber security may at the same time affect standard business procedures and operations, rendering them more time consuming or costly. It is therefore a senior management level strategic responsibility to evaluate and decide on risk versus reward trade-offs.

   Các sáng kiến để nâng cao an ninh mạng có thể đồng thời ảnh hưởng đến các quy trình và hoạt động kinh doanh tiêu chuẩn, khiến tiêu tốn nhiều thời gian hoặc chi phí hơn. Do đó, đó là trách nhiệm chiến lược cấp cao về quản lý để đánh giá và quyết định về sự cân bằng giữa rủi ro và sinh lợi.

2. A number of initiatives which would heighten cyber security are related to business processes and training, and not to IT systems, and therefore need to be anchored organisationally outside the IT department.

   Một số sáng kiến nâng cao an ninh mạng có liên quan đến quá trình kinh doanh và đào tạo, chứ không phải cho hệ thống IT, và do đó cần phải được gắn liền về mặt tổ chức bên ngoài bộ phận IT.

3. Initiatives which heighten cyber security awareness may change how the company interacts with customers, suppliers and authorities, and impose new requirements on the co-operation between the parties. It is a senior management level decision whether and how to drive changes in these relationships.

   Sáng kiến nâng cao nhận thức an ninh mạng có thể thay đổi cách công ty tương tác với khách hàng, nhà cung cấp, cơ quan chức năng, và áp đặt các yêu cầu mới về sự hợp tác giữa các bên. Đây là quyết định của cấp quản lý cấp cao về việc có hay không và làm như thế nào để thúc đẩy những thay đổi trong các mối quan hệ này.

4. Only when the above three aspects have been decided upon will it be possible to clearly outline what the IT requirements of the cyber security strategy will be, and this is the element which can be placed with the IT department.

   Chỉ khi ba khía cạnh trên đã được quyết định thì sẽ có thể phác thảo rõ ràng những yêu cầu IT của chiến lược an ninh mạng là gì, và đây là yếu tố có thể được đặt vào bộ phận IT.

5. Based on the strategic decisions in general, and the risk versus reward trade-offs, relevant contingency plans should be established in relation to handling cyber incidents if they should occur.

   Dựa trên các quyết định chiến lược nói chung, và sự cân bằng giữa rủi ro và sinh lợi, các kế hoạch dự phòng thích hợp phải được thiết lập liên quan đến việc xử lý các sự cố mạng nếu chúng xảy ra.

Senior management should realise their leadership responsibilities by delegating authority and allocating the budget needed to carry out the risk assessment and to develop solutions that are best suit for the company and the operation of their ships.

Quản lý cấp cao cần thực hiện trách nhiệm lãnh đạo của mình bằng cách ủy quyền và phân bổ ngân sách cần thiết để thực hiện đánh giá rủi ro và phát triển các giải pháp phù hợp nhất cho công ty và hoạt động của tàu.

The level of cyber risk will reflect the circumstances of the company, ship (its operation and trade), the IT and OT systems used, and the information and/or data stored. The maritime industry possesses a range of characteristics which affect its vulnerability to cyber incidents:

Mức độ rủi ro mạng sẽ phản ánh hoàn cảnh của công ty, tàu (hoạt động và thương mại), hệ thống IT và OT được sử dụng, và thông tin và/hoặc dữ liệu được lưu trữ. Ngành hàng hải sở hữu một loạt các đặc điểm ảnh hưởng đến tính dễ bị tổn thương của nó trước các sự cố mạng:

- the cyber controls already implemented by the company and onboard its ships;
  Các kiểm soát mạng đã được triển khai bởi công ty và trên tàu của công ty;
- multiple stakeholders are often involved in the operation and chartering of a ship potentially resulting in lack of accountability for the IT infrastructure;

  Nhiều bên liên quan thường tham gia vào hoạt động và thuê một tàu có khả năng dẫn đến thiếu trách nhiệm giải trình cho cơ sở hạ tầng IT;
- the ship being online and how it interfaces with other parts of the global supply chain;

  Tàu đang trực tuyến và cách nó giao tiếp với các bộ phận khác của chuỗi cung ứng toàn cầu;
- ship equipment being remotely monitored eg by the producers;
  Thiết bị tàu được giám sát từ xa, ví dụ như bởi các nhà sản xuất;
- business-critical, data sensitive and commercially sensitive information shared with shorebased service providers;

  Thông tin nhạy cảm về kinh doanh, dữ liệu nhạy cảm và thương mại quan trọng được chia sẻ với các nhà cung cấp dịch vụ trên bờ;
- the availability and use of computer-controlled critical systems for the ship's safety and for environmental protection.

  Tính khả dụng và việc sử dụng các hệ thống quan trọng được máy tính kiểm soát để bảo vệ sự an toàn của tàu và môi trường.

These elements should be considered, and relevant parts incorporated into the company security policies, safety management systems, and ship security plans. Users of these guidelines should refer to specific national legislation and flag state requirements as well as relevant international and industry standards and best practices when developing and implementing cyber risk management procedures.

Các yếu tố này cần được xem xét và các bộ phận liên quan được đưa vào các chính sách an ninh của công ty, các hệ thống quản lý an toàn, và các kế hoạch an ninh tàu. Người sử dụng Hướng dẫn này nên tham khảo các quy định quốc gia, các yêu cầu của quốc gia tàu mang cờ quốc tịch cụ thể cũng như các tiêu chuẩn quốc tế, công nghiệp và thực hành tốt nhất thích hợp khi phát triển và thực hiện các quy trình quản lý rủi ro mạng.

IT and OT systems, software and maintenance can be outsourced to third-party service providers and the company itself may not possess a way of verifying the level of security supplied by these providers. Some companies use different providers responsible for software and cyber security checks.

Các hệ thống, phần mềm và bảo trì IT và OT có thể được thuê ngoài từ các nhà cung cấp dịch vụ bên thứ ba và bản thân công ty có thể không có cách xác minh mức độ bảo mật được cung cấp bởi các nhà cung cấp này. Một số công ty sử dụng các nhà cung cấp khác nhau chịu trách nhiệm về kiểm tra an ninh mạng và phần mềm.

The growing use of big data, smart ships and the 'internet of things' will increase the amount of information available to cyber attackers and the potential attack surface to cyber criminals. This makes the need for robust approaches to cyber security important both now and in the future.

Việc sử dụng ngày càng tăng các dữ liệu lớn, tàu thông minh và 'internet of things' sẽ tăng lượng thông tin có sẵn cho những kẻ tấn công mạng và bề mặt tấn công tiềm tàng vào tội phạm mạng. Điều này làm cho nhu cầu về các phương pháp tiếp cận mạnh mẽ đối với an ninh mạng quan trọng cả hiện tại và trong tương lai.

Third-party access
Việc truy cập của bên thứ ba

Visits to ships by third parties requiring a connection to one or more computers on board can also result in connecting the ship to shore. It is common for technicians, vendors, port officials, marine terminal representatives, agents, pilots, and other technicians to board the ship and plug in devices, such as laptops and tablets. Some technicians may require the use of removable media to update computers, download data and/or perform other tasks. It has also been known for customs officials and port state control officers to board a ship and request the use of a computer to "print official documents" after first inserting an unknown removable media.

Việc thăm tàu của các bên thứ ba yêu cầu kết nối với một hoặc nhiều máy tính trên tàu cũng có thể dẫn đến việc kết nối tàu với bờ. Phổ biến là các kỹ thuật viên, nhà cung cấp, quan chức cảng, đại diện thiết bị đầu cuối hàng hải, đại lý, hoa tiêu và các kỹ thuật viên khác lên tàu và kết nối thiết bị, chẳng hạn như máy tính xách tay và máy tính bảng. Một số kỹ thuật viên có thể yêu cầu sử dụng phương tiện di động (phương tiện tháo lắp được) để cập nhật máy tính, tải xuống dữ liệu và/hoặc thực hiện các tác vụ khác. Đã có các trường hợp các quan chức hải quan và sỹ quan kiểm tra nhà nước cảng để lên tàu và yêu cầu sử dụng một máy tính để "in tài liệu chính thức" sau khi chèn một phương tiện di động không rõ.

Some IT and OT systems are remotely accessible and may operate with a continuous internet connection for remote monitoring, data collection, maintenance functions, safety and security. These systems can be "third-party systems", whereby the contractor monitors and maintains the systems from a remote access. These systems could include both two-way data flow and upload- only. Systems and work stations with remote control, access or configuration functions could, for example, be:

Một số hệ thống IT và OT có thể truy cập từ xa và có thể hoạt động với kết nối internet liên tục để theo dõi từ xa, thu thập dữ liệu, chức năng bảo trì, an toàn và an ninh. Các hệ thống này có thể là "hệ thống của bên thứ ba", theo đó nhà thầu giám sát và duy trì hệ thống từ truy cập từ xa. Các hệ thống này có thể bao gồm cả luồng dữ liệu hai chiều và chỉ tải lên. Ví dụ, các hệ thống và trạm làm việc có chức năng điều khiển từ xa, truy cập hoặc cấu hình có thể là:

- bridge and engine room computers and work stations on the ship's administrative network;

  Các máy tính trên buồng lái, buồng máy và các trạm làm việc trên mạng hành chính của tàu;

- cargo such as containers with reefer temperature control systems or specialised cargo that are tracked remotely;

Hàng hóa như container với hệ thống kiểm soát nhiệt độ lạnh hoặc hàng hóa chuyên dụng được theo dõi từ xa;

- stability decision support systems;
  Các hệ thống hỗ trợ quyết định về ổn định;
- hull stress monitoring systems;
  Hệ thống giám sát ứng suất thân tàu;
- navigational systems including Electronic Navigation Chart (ENC) Voyage Data Recorder (VDR), dynamic positioning (DP);

  Các hệ thống hành hải bao gồm: hải đồ hành hải điện tử (ENC); thiết bị ghi dữ liệu hành trình (VDR), hệ thống định vị động (DP);
- cargo handling, engine, and cargo management systems;
  Các hệ thống làm hàng, máy và quản lý hàng hóa;
- safety and security networks, such as CCTV (closed circuit television);
  Các mạng an toàn và an ninh, chẳng hạn như CCTV (truyền hình mạch kín);
- specialised systems such as drilling operations, blow out preventers, subsea installation systems, Emergency Shut Down (ESD) for gas tankers, submarine cable installation and repair.

  Các hệ thống chuyên dụng như các hoạt động khoan, thiết bị chống phun dầu, hệ thống lắp đặt dưới biển, ngắt khẩn cấp (ESD) cho các tàu chở khí, lắp đặt và sửa chữa cáp ngầm.

The extent and nature of connectivity of equipment should be known by the shipowner or operator and documented as part of the risk assessment.

Mức độ và tính chất kết nối của thiết bị phải được chủ tàu hoặc người khai thác tàu biết và được lập thành hồ sơ như một phần của đánh giá rủi ro.

Impact assessment
Đánh giá tác động

The confidentiality, integrity and availability (CIA) model provides a framework for assessing the impact of:

Mô hình về tính bảo mật, toàn vẹn và khả dụng (CIA) cung cấp khuôn khổ để đánh giá tác động của:

- unauthorised access to and disclosure of information or data about the ship, crew, cargo and passengers;

  Truy cập trái phép và tiết lộ thông tin hoặc dữ liệu về tàu, thuyền viên, hàng hóa và hành khách;
- loss of integrity, which would modify or destroy information and data relating to the safe and efficient operation and administration of the ship;

  Việc mất tính toàn vẹn sẽ làm sửa đổi hoặc phá hủy thông tin và dữ liệu liên quan đến hoạt động an toàn, hiệu quả và quản lý tàu;
- loss of availability due to the destruction of the information and data and/or the disruption to services/ operation of ship systems.

  Mất tính khả dụng do sự phá hủy thông tin và dữ liệu và/hoặc sự gián đoạn dịch vụ/hoạt động của các hệ thống tàu.

The relative importance of confidentiality, integrity and availability changes depending on the use of the information or data. For example, assessing the vulnerability of IT systems related to commercial operations may focus on confidentiality and integrity rather than availability. Conversely, assessing the vulnerability of OT systems onboard ships, particularly safety critical systems, may focus on availability and/or integrity instead of confidentiality.

Tầm quan trọng tương đối của các thay đổi về tính bảo mật, tính toàn vẹn và tính khả dụng tùy thuộc vào việc sử dụng thông tin hoặc dữ liệu. Ví dụ, đánh giá tính dễ bị tổn thương (lỗ hổng) của các hệ thống IT liên quan đến hoạt động thương mại có thể tập trung vào tính bảo mật và tính toàn vẹn hơn là tính khả dụng. Ngược lại, đánh giá tính dễ bị tổn thương của các hệ thống OT trên tàu, đặc biệt là các hệ thống an toàn quan trọng, có thể tập trung vào tính khả dụng và/hoặc tính toàn vẹn thay vì tính bảo mật.

Potential impact ***Tác động tiềm tàng***	**Definition** ***Định nghĩa***	**In practice** ***Trong thực tế***
Low *Thấp*	The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on company and ship, organisational assets, or individuals. *Việc mất tính bảo mật, tính toàn vẹn hoặc tính khả dụng có thể được dự kiến sẽ có tác động tiêu cực hạn chế đối với công ty và tàu, tài sản của tổ chức, hoặc cá nhân.*	A limited adverse effect means that a security breach might: (i) cause a degradation in ship operation to an extent and duration that the organisation is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organisational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals. *Hiệu ứng bất lợi hạn chế có nghĩa là vi phạm an ninh có thể: (i) gây ra sự xuống cấp trong hoạt động của tàu đến một mức độ và thời gian mà tổ chức có thể thực hiện các chức năng chính của nó, nhưng hiệu quả của các chức năng bị giảm đáng kể; (ii) dẫn đến thiệt hại nhỏ đối với tài sản của tổ chức; (iii) dẫn đến tổn thất tài chính nhỏ; hoặc (iv) gây thiệt hại nhỏ cho cá nhân.*
Moderate *Trung bình*	The loss of confidentiality, integrity, or availability could be expected to have a substantial adverse effect on company and ship, company and ship assets, or individuals. *Việc mất tính bảo mật, tính toàn vẹn hoặc tính khả dụng có thể được dự kiến sẽ có tác động bất lợi đáng kể đối với công ty và tàu, tài sản của công*	A substantial adverse effect means that a security breach might: (i) cause a significant degradation in ship operation to an extent and duration that the organisation is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organisational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries. *Tác động bất lợi đáng kể có nghĩa là vi phạm an ninh có thể: (i) gây ra sự suy giảm đáng kể trong hoạt động của tàu đến một mức độ và thời gian mà tổ chức có thể thực hiện các chức năng chính của nó, nhưng hiệu quả của các chức năng bị giảm đáng kể; (ii) dẫn đến thiệt*

	ty và tàu, hoặc cá nhân.	*hại đáng kể cho tài sản của tổ chức; (iii) dẫn đến tổn thất tài chính đáng kể; hoặc (iv) gây thiệt hại đáng kể cho các cá nhân nhưng không gây ra chết người hoặc thương tích đe dọa tính mạng nghiêm trọng.*
High *Cao*	The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on company and ship operations, company and ship assets, or individuals. *Việc mất tính bảo mật, tính toàn vẹn hoặc tính khả dụng có thể được dự kiến sẽ có tác động tiêu cực nghiêm trọng hoặc thảm khốc đến hoạt động của công ty và tàu, tài sản của công ty và tàu, hoặc cá nhân.*	A severe or catastrophic adverse effect means that a security breach might: (i) cause a severe degradation in or loss of ship operation to an extent and duration that the organisation is not able to perform one or more of its primary functions; (ii) result in major damage to organisational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious lifethreatening injuries. *Tác động bất lợi nghiêm trọng hoặc thảm khốc có nghĩa là vi phạm an ninh có thể: (i) gây ra sự xuống cấp nghiêm trọng hoặc mất hoạt động của tàu trong phạm vi và thời gian tổ chức không thể thực hiện một hoặc nhiều chức năng chính của nó; (ii) dẫn đến thiệt hại lớn cho tài sản tổ chức; (iii) dẫn đến tổn thất tài chính lớn; hoặc (iv) dẫn đến tổn hại nghiêm trọng hoặc thảm khốc cho các cá nhân liên quan đến việc mất mạng sống hoặc thương tích nghiêm trọng.*

Table 2. Potential impact levels when using the CIA model
Bảng 2. Mức độ tác động tiềm năng khi sử dụng mô hình CIA

Sensitive information may include ship position, status of and readout from OT systems, cargo details, authorisations, certificates, etc. When it comes to OT systems it is important consider what impact the loss or malfunction of the system will have following a cyber incident.

Thông tin nhạy cảm có thể bao gồm vị trí tàu, trạng thái và số liệu ra từ hệ thống OT, chi tiết hàng hóa, ủy quyền, chứng chỉ, ... Khi nói đến hệ thống OT, điều quan trọng là xem xét những gì tác động đến sự mất mát hoặc trục trặc của hệ thống sẽ có sau một sự cố không gian mạng..

Example
Ví dụ

A power management system contains a supervisory control and data acquisition (SCADA) system controlling the distribution of onboard electric power. The system contains real-time sensor data which is used onboard for power management. It also generates data about the power consumption, which is used by the shipping company for administrative purposes.

Hệ thống quản lý năng lượng bao gồm hệ thống kiểm soát giám sát và thu thập dữ liệu (SCADA) kiểm soát việc phân phối điện năng trên tàu. Hệ thống này chứa dữ liệu cảm biến thời gian thực được sử dụng trên tàu để quản lý nguồn điện. Nó cũng tạo ra dữ liệu về mức tiêu thụ điện năng, được sử dụng bởi công ty vận tải biển cho mục đích quản trị.

To determine if the information above is critical, the consequences likely to result from a compromise to the confidentiality, integrity or availability should be considered. When doing so the shipping company should determine the criticality of the information stored, processed or transmitted by the SCADA system using the most sensitive information to determine the overall impact of the system.

Để xác định xem thông tin trên có quan trọng hay không, các hậu quả có khả năng dẫn đến mối nguy hiểm tiềm tàng đối với tính bảo mật, tính toàn vẹn hoặc tính khả dụng cần được xem xét. Khi làm như vậy, công ty vận trai biển nên xác định mức độ quan trọng của thông tin được lưu trữ, xử lý hoặc truyền bởi hệ thống SCADA bằng cách sử dụng thông tin nhạy cảm nhất để xác định tác động tổng thể của hệ thống.

As this OT system is using several measuring points and is integrated with other systems, the company decide to consider the effect of an operational malfunction or loss of the SCADA system due to a cyber incident. In this case, the company concludes that this will have a severe effect and thereby a high impact to the operation of the ship.

Vì hệ thống OT này đang sử dụng một số điểm đo và được tích hợp với các hệ thống khác, công ty quyết định xem xét tác động của sự cố hoạt động hoặc mất hệ thống SCADA do sự cố mạng. Trong trường hợp này, công ty kết luận rằng điều này sẽ có ảnh hưởng nghiêm trọng và do đó tác động lớn đến hoạt động của tàu.

Using the CIA model, the shipping company can also conclude that:
Sử dụng mô hình CIA, công ty vận tải biển cũng có thể kết luận:

- losing confidentiality of the sensor data acquired by the SCADA system will have a low impact as the sensors are publicly displayed on board. However, from a safety point of view, it is important that the information transmitted by the sensors can be relied upon therefore there is a high potential impact from a loss of integrity. It will also be a safety issue if the information cannot be read, and there is therefore a high potential impact from a loss of availability.

  Mất tính bí mật của dữ liệu cảm biến thu được bởi hệ thống SCADA sẽ có tác động thấp khi các cảm biến được hiển thị công khai trên tàu. Tuy nhiên, từ quan điểm an toàn, điều quan trọng là thông tin được truyền bởi các cảm biến có thể được dựa vào do đó có tác động tiềm năng cao từ sự mất tính toàn vẹn. Nó cũng sẽ là một vấn đề an toàn nếu thông tin không thể đọc được, và do đó có tác động tiềm năng cao từ sự mất khả dụng.

- for the power consumption information being sent to the shipping company for statistical purposes, it is assessed that there is a low potential impact from a loss of confidentiality. The company does not want the data to be public, however the effect would be limited if it were to happen. There will also be a low potential impact from a loss of integrity as the data is only used for in-house considerations. There is therefore also a low potential impact from a loss of availability.

  Đối với thông tin tiêu thụ năng lượng được gửi đến công ty vận tải biển cho các mục đích thống kê, được đánh giá rằng có tác động tiềm năng thấp do mất tính bảo mật. Công ty không muốn dữ liệu được công khai, tuy nhiên hiệu quả sẽ bị hạn chế nếu nó xảy ra. Cũng sẽ có tác động tiềm năng thấp do mất tính toàn vẹn vì dữ liệu chỉ được sử dụng để cân nhắc nội bộ. Do đó, cũng có tác động tiềm năng thấp do mất tính khả dụng.

The following table shows the result of the assessment:
Bảng sau đây chỉ ra kết quả đánh giá:

SCADA system *Hệ thống SCADA*	Confidentiality *Tính bảo mật*	Integrity *Tính toàn vẹn*	Availability *Tính khả dụng*	Overall impact *Tác động tổng thể*
Sensor data *Dữ liệu cảm biến*	Low *Thấp*	High *Cao*	High *Cao*	High *Cao*
Statistical data *Dữ liệu thống kê*	Low *Thấp*	Low *Thấp*	Low *Thấp*	Low *Thấp*

Table 3. result of CIA assessment of SCADA system
Bảng 3. Kết quả đánh giá CIA của hệ thống SCADA

Bring your own device (BYOD)
Việc mang theo thiết bị của riêng bạn (BYOD)

It is recognised that personnel may be allowed to bring their own devices (BYOD) on board to access the ships' system or network. Although this may be both beneficial and economical for ships, because these devices may be unmanaged, it significantly increases the possibility of vulnerabilities being exposed. Policies and procedures should address their control, use, and how to protect vulnerable data, such as through network segregation.

Thừa nhận là nhân viên có thể được phép mang theo thiết bị của riêng mình (BYOD) lên tàu để truy cập vào hệ thống hoặc mạng của tàu. Mặc dù điều này có thể mang lại cả lợi ích và kinh tế cho tàu, bởi vì các thiết bị này có thể không được quản lý, nó làm tăng đáng kể khả năng xảy ra các lỗ hổng bảo mật. Các chính sách và quy trình nên đề cập đến việc kiểm soát, sử dụng và cách bảo vệ dữ liệu dễ bị tổn thương, chẳng hạn như thông qua việc phân tách mạng.

4.1 Risk assessment made by the company
Đánh giá rủi ro do công ty thực hiện

As mentioned above, the risk assessment process starts by assessing the systems on board, in order to map their robustness to handle the current level of cyber threats. Elements of a ship security assessment (The assessment described is based on regulation 8 of the ISPS Code) can be used when performing the risk assessment, which should physically test and assess the IT and OT systems on board including:

Như đã đề cập ở trên, quá trình đánh giá rủi ro bắt đầu bằng cách đánh giá các hệ thống trên tàu, để thiết lập các biện phap thự tế nhăm xử lý các mức đe dọa mạng hiện tại. Các yếu tố của việc đánh giá an ninh tàu (việc đánh giá được mô tả dựa trên quy định 8 của ISPS Code) có thể được sử dụng khi thực hiện đánh giá rủi ro, cần kiểm tra và đánh giá vật lý các hệ thống IT và OT trên tàu bao gồm:

1. identification of existing technical and procedural controls to protect the onboard IT and OT systems (more information can be found with the Critical Security Controls- http://www.cisecurity.org/critical-controls.cfm);

   Xác định các kiểm soát kỹ thuật và bằng quy trình hiện có để bảo vệ các hệ thống IT và OT trên tàu (có thể tìm thêm thông tin với "Kiểm soát an ninh quan trọng"- www.cisecurity.org/critical-controls.cfm);

2. identification of IT and OT systems that are vulnerable, the specific vulnerabilities identified, including human factors, and the policies and procedures governing the use of these systems (the identification should include searches for known vulnerabilities relevant to the equipment, the current level of patching and firmware updates);

   Xác định các hệ thống IT và OT dễ bị tổn thương, các lỗ hổng cụ thể được xác định, bao gồm các yếu tố con người, và các chính sách và quy trình điều chỉnh việc sử dụng các hệ thống này (việc xác định bao gồm tìm kiếm các lỗ hổng đã biết liên quan đến thiết bị, mức vá hiện tại và cập nhật firmware);

3. identification and evaluation of key ship board operations that are vulnerable to cyber attacks;

   Xác định và đánh giá các hoạt động chủ chốt của tàu dễ bị tấn công mạng;

4. identification of possible cyber incidents and their impact on key ship board operations, and the likelihood of their occurrence to establish and prioritise protection measures.

   Xác định các sự cố mạng có thể xảy ra và tác động của chúng đối với các hoạt động chính của tàu, và khả năng xảy ra sự cố để thiết lập và ưu tiên các biện pháp bảo vệ.

Companies may consult with the producers and service providers of onboard equipment and systems to understand the technical and procedural controls that may already be in place to address cyber security. Furthermore, any identified cyber vulnerability in the factory standard configuration of a critical system or component should be disclosed to facilitate better protection of the equipment in the future.

Các công ty có thể tham vấn với các nhà sản xuất và nhà cung cấp dịch vụ về các thiết bị và hệ thống của tàu để hiểu các kiểm soát kỹ thuật và bằng quy trình có thể đã có để xử lý an ninh mạng. Hơn nữa, bất kỳ lỗ hổng mạng được xác định trong cấu hình tiêu chuẩn nhà máy của một hệ thống hoặc hợp phần quan trọng cần được tiết lộ để tạo điều kiện bảo vệ tốt hơn cho thiết bị trong tương lai.

4.2 Third-party risk assessments
Đánh giá rủi ro của bên thứ ba

Self-assessments can serve as a good start, but may be complemented by third-party risk assessments to drill deeper, and identify the risks and the gaps that may not be found during the self-assessment. Penetration tests of critical IT and OT infrastructure can also be performed to identify whether the actual defence level matches the desired level set forth in the cyber security strategy for the company. Such tests can be performed by external experts simulating attacks using both IT-systems, social engineering and, if desired, even physical penetration of a facility's security perimeter. These tests are referred to as active tests because they involve accessing and inserting software into a system. This may only be appropriate for IT systems. Where risk to OT systems during penetration testing is unacceptable, passive testing approaches should be considered. Passive methods rely on scanning data transmitted by a system to identify vulnerabilities. In general, no attempt is made to actively access or insert software into the system.

Tự đánh giá có thể xem là là một khởi đầu tốt, nhưng có thể được bổ sung bởi các đánh giá rủi ro của bên thứ ba để tìm hiểu sâu hơn, và xác định các rủi ro và khoảng trống có thể không

được tìm thấy trong quá trình tự đánh giá. Các thử nghiệm thâm nhập của cơ sở hạ tầng IT và OT quan trọng cũng có thể được thực hiện để xác định liệu mức phòng thủ thực tế có phù hợp với mức mong muốn được quy định trong chiến lược an ninh mạng cho công ty hay không. Các thử nghiệm như vậy có thể được thực hiện bởi các chuyên gia bên ngoài mô phỏng các cuộc tấn công bằng cách sử dụng cả hai hệ thống IT, kỹ thuật xã hội và nếu muốn, thậm chí sự xâm nhập vật lý vành đai an ninh của cơ sở. Các thử nghiệm này được gọi là thử nghiệm hoạt động vì chúng liên quan đến việc truy cập và chèn phần mềm vào một hệ thống. Điều này chỉ có thể phù hợp với các hệ thống IT. Trường hợp rủi ro đối với các hệ thống OT trong quá trình kiểm tra thâm nhập là không thể chấp nhận, các phương pháp thử nghiệm thụ động cần được xem xét. Phương pháp thụ động dựa vào dữ liệu quét được truyền bởi một hệ thống để xác định các lỗ hổng. Nói chung, không có nỗ lực nào được thực hiện để truy cập một cách chủ động hoặc chèn phần mềm vào hệ thống.

4.3 Risk assessment process
Quá trình đánh giá rủi ro

Phase 1: Pre-assessment activities
Giai đoạn 1: Các hoạt động đánh giá trước

Prior to starting a cyber security assessment on board, the following activities should be performed:

Trước khi bắt đầu đánh giá an ninh mạng trên board, các hoạt động sau đây cần được thực hiện:

- map the ship's key functions and systems and their potential impact levels, for example using the CIA model, taking into consideration the operation of OT systems;

  Vạch ra các chức năng và hệ thống chính của tàu và mức độ tác động tiềm năng của chúng, ví dụ như sử dụng mô hình CIA, có tính đến hoạt động của các hệ thống OT;

- identify main producers of critical shipboard IT and OT equipment;
  Xác định các nhà sản xuất chính của các thiết bị IT và OT quan trọng trên tàu;

- review detailed documentation of critical OT and IT systems including their network architecture, interfaces and interconnections;

  Xem xét tài liệu chi tiết về các hệ thống OT và IT quan trọng bao gồm kiến trúc mạng, giao diện và kết nối của chúng;

- identify cyber security points-of-contact at each of the producers and establish working relationships with them;

  Xác định các điểm liên lạc an ninh mạng tại mỗi nhà sản xuất và thiết lập các mối quan hệ làm việc với họ;

- review detailed documentation on the ship's maintenance and support of its IT and OT systems;

  Xem xét tài liệu chi tiết về việc bảo trì và hỗ trợ của các hệ thống IT và OT của tàu;

- establish contractual requirements and obligations that the shipowner/ship operator may have for maintenance and support of shipboard networks and equipment;

  Thiết lập các yêu cầu và nghĩa vụ theo hợp đồng mà chủ tàu/người khai thác tàu có thể có để bảo trì và hỗ trợ mạng và thiết bị của tàu;

- support, if necessary, the risk assessment with an external expert to develop detailed plans and include producers and service providers.

  Hỗ trợ, nếu cần thiết, việc đánh giá rủi ro với chuyên gia bên ngoài để xây dựng kế hoạch chi tiết, bao gồm các nhà sản xuất và cung cấp dịch vụ.

Phase 2: Ship assessment
Giai đoạn 2: Đánh giá tàu

The goal of the assessment of a ship's network and its systems and devices is to identify any vulnerabilities that could compromise or result in either loss of confidentiality, loss of integrity or result in a loss of operation of the equipment, system, network, or even the ship. These vulnerabilities and weaknesses could fall into one of the following categories:

Mục tiêu của việc đánh giá mạng của tau và các hệ thống,thiết bị của nó là xác định bất kỳ lỗ hổng nào có thể xâm phạm hoặc dẫn đến mất tính bảo mật, mất tính toàn vẹn hoặc dẫn đến mất hoạt động của thiết bị, hệ thống, mạng hoặc thậm chí là tàu. Các lỗ hổng và điểm yếu này có thể rơi vào một trong các loại sau:

1. technical such as software defects or outdated or unpatched systems;
   Kỹ thuật như lỗi phần mềm hoặc hệ thống đã lỗi thời hoặc chưa được vá;
2. design such as access management, unmanaged network interconnections;
   Thiết kế như quản lý truy cập, kết nối mạng không được quản lý;
3. implementation errors for example misconfigured firewalls;
   Lỗi triển khai, ví dụ như tường lửa được định cấu hình sai;
4. procedural or other user errors.
   Lỗi quy trình hoặc người dùng khác.

The activities performed during an assessment would include reviewing the configuration of all computers, servers, routers, and cyber security technologies including firewalls. It should also include reviews of all available cyber security documentation and procedures for connected IT and OT systems and devices.

Các hoạt động được thực hiện trong quá trình đánh giá sẽ bao gồm xem xét cấu hình của tất cả các máy tính, máy chủ, bộ định tuyến và các công nghệ an ninh mạng bao gồm tường lửa. Nó cũng nên bao gồm các đánh giá về tất cả tài liệu và quy trình an ninh mạng có sẵn cho các thiết bị và hệ thống IT và OT được kết nối.

Phase 3: Debrief and vulnerability review/reporting
Giai đoạn 3: Trao đổi và xem xét/báo cáo lỗ hổng

Following the assessment, each identified vulnerability should be evaluated for its potential impact and the probability of its exploitation. Recommended technical and/or procedural corrective actions should be identified for each vulnerability in a final report.

Sau khi đánh giá, mỗi lỗ hổng được xác định cần được đánh giá về tác động tiềm tàng và khả năng khai thác của nó. Các biện pháp khắc phục kỹ thuật và/hoặc bằng quy trình được khuyến nghị nên được xác định cho từng lỗ hổng trong báo cáo cuối cùng.

Ideally, the cyber security assessment report should include:

Lý tưởng nhất, báo cáo đánh giá an ninh mạng nên bao gồm:

- executive summary - a high-level summary of results, recommendations and the overall security profile of the assessed environment, facility or ship;

Tóm tắt điều hành - tóm tắt cấp cao về kết quả, khuyến nghị và hồ sơ an ninh tổng thể của môi trường, cơ sở hoặc tàu được đánh giá;

- technical findings - a detailed, tabular breakdown of discovered vulnerabilities, their probability of exploitation, the resulting impact, and appropriate technical fix and mitigation advice;

  Các phát hiện kỹ thuật - bảng kê chi tiết về các lỗ hổng được phát hiện, xác suất khai thác, tác động thu được và tư vấn sửa chữa kỹ thuật và giảm thiểu thích hợp;

- prioritised list of actions - the priorities allocated should reflect the effectiveness of the measure, the cost, the applicability, etc. It is important that this list does not represent a list of services and products the third-party risk assessor would like to sell, instead of being a complete list of options available;

  Danh sách ưu tiên các hành động - các ưu tiên được phân bổ phải phản ánh hiệu quả của biện pháp, chi phí, khả năng áp dụng, ... Điều quan trọng là danh sách này không đại diện cho danh sách các dịch vụ và sản phẩm mà những người đánh giá rủi ro bên thứ ba muốn bán, thay vì là danh sách đầy đủ các tùy chọn có sẵn;

- supplementary data - a supplement containing the technical details of all key findings and comprehensive analysis of critical flaws. This section should also include sample data recovered during the penetration testing of critical or high-risk vulnerabilities;

  Dữ liệu bổ sung - một bổ sung có chứa các chi tiết kỹ thuật của tất cả các phát hiện quan trọng và phân tích toàn diện các sai sót quan trọng. Phần này cũng nên bao gồm dữ liệu mẫu được thu hồi trong quá trình thử nghiệm thâm nhập các lỗ hổng rủi ro cao hoặc quan trọng;

- appendices - detailed records of all activities conducted by the cyber security assessment team and the tools used during the engagement.

  Các phụ lục - hồ sơ chi tiết của tất cả các hoạt động được thực hiện bởi nhóm đánh giá an ninh mạng và các công cụ được sử dụng trong quá trình tham gia.

Phase 4: Producer debrief
Giai đoạn 4: Trao đổi với nhà sản xuất

Once the shipowner has had an opportunity to review, discuss and assess the findings, a subset of the findings may need to be sent to the producers of the affected systems. Any findings, which are approved by the shipowner for disclosure to the producers, could further be analysed with support from external experts, who should work with the producer's cyber security point of contact to ensure that a full risk and technical understanding of the problem is achieved. This supporting activity is intended to ensure that any remediation plan developed by the producer is comprehensive in nature and the correct solution to eliminate the vulnerabilities identified.

Khi chủ tàu đã có cơ hội xem xét, thảo luận và đánh giá các phát hiện, thì tập hợp các phát hiện có thể cần phải được gửi đến các nhà sản xuất của các hệ thống bị ảnh hưởng. Bất kỳ phát hiện nào, được chủ tàu phê duyệt để thông báo cho các nhà sản xuất, có thể được phân tích thêm với sự hỗ trợ từ các chuyên gia bên ngoài, những người nên làm việc với điểm liên hệ an ninh mạng của nhà sản xuất để đảm bảo sự hiểu biết đầy đủ về kỹ thuật. Hoạt động hỗ trợ này nhằm đảm bảo rằng bất kỳ kế hoạch khắc phục hậu quả nào được phát triển bởi nhà sản xuất là toàn diện về bản chất và là giải pháp chính xác để loại bỏ các lỗ hổng được xác định.

5. Develop protection and detection measures
Phát triển biện pháp phát hiện và bảo vệ

The outcome of the senior management's risk assessment and subsequent company's cyber security strategy should be a reduction in risk, if needed. At a technical level, this would include the necessary actions to be implemented to establish and maintain an agreed level of cyber security.

Kết quả đánh giá rủi ro của quản lý cấp cao và chiến lược an ninh mạng của công ty tiếp theo phải là giảm rủi ro, nếu cần. Ở cấp độ kỹ thuật, điều này sẽ bao gồm các hành động cần thiết được thực hiện để thiết lập và duy trì mức độ an ninh mạng được đồng ý.

Special attention should be given when there has been no control over who has access to the onboard systems. This could, for example, happen during drydocking, layups or when taking over a new or existing ship. In such cases, it is difficult to know if malicious software has been left in the onboard systems. It is recommended that sensitive data is removed from the ship and reinstalled on returning to the ship. Where possible, systems should be scanned for malware before prior to use. OT systems should be tested to check that the functionalities are still intact.

Cần chú ý đặc biệt khi không có sự kiểm soát ai có quyền truy cập vào các hệ thống trên tàu. Điều này có thể, ví dụ, xảy ra trong quá trình tàu trên đà, dừng hoạt động hoặc khi tiếp nhận một tàu mới hoặc tàu hiện có. Trong những trường hợp như vậy, rất khó để biết liệu phần mềm độc hại có bị bỏ lại trong các hệ thống của tàu hay không. Khuyến nghị là dữ liệu nhạy cảm được lấy ra khỏi tàu và cài đặt lại khi đưa trở về tàu. Nếu có thể, các hệ thống sẽ được quét phần mềm độc hại trước khi sử dụng. Các hệ thống OT nên được thử để kiểm tra xem các chức năng vẫn còn nguyên vẹn hay không.

It is critical to identify how to manage cyber security on board and to delegate responsibilities to the master, responsible officers and maybe the company security officer.

Điều quan trọng là để xác định cách thức để quản lý an ninh mạng trên tàu và để giao trách nhiệm cho thuyền trưởng, các sỹ quan có trách nhiệm và có thể là nhân viên an ninh công ty.

Cyber security protection measures may be technical and focused on ensuring that onboard systems are designed and configured to be resilient to cyber attacks. Protection measures may also be procedural and should be covered by company policies, safety management procedures, security procedures and access controls. Both technical and procedural controls should be compatible with the confidentiality, integrity and availability (CIA) model for protecting data and information.

Các biện pháp bảo vệ an ninh mạng có thể là kỹ thuật và tập trung vào việc đảm bảo rằng các hệ thống trên tàu được thiết kế và cấu hình để có khả năng thích ứng trước các cuộc tấn công mạng. Các biện pháp bảo vệ cũng có thể là quy trình và cần được đề cập trong chính sách của công ty, quy trình quản lý an toàn, quy trình an ninh và kiểm soát truy cập. Cả hai kiểm soát kỹ thuật và bằng quy trình phải tương thích với tính bảo mật, tính toàn vẹn và tính khả dụng (CIA) để bảo vệ dữ liệu và thông tin.

It is recognised that technical cyber security controls may be more straightforward to implement on a new ship than on an existing ship. Consideration needs be given to only implement technical controls that are practical and cost effective, particularly on existing ships.

Thừa nhận rằng kiểm soát an ninh mạng bằng kỹ thuật có thể đơn giản hơn để thực hiện trên một tàu mới hơn là trên một tàu hiện có. Cần cân nhắc việc chỉ thực hiện các biện pháp kiểm soát kỹ thuật có tính thực tiễn và hiệu quả về chi phí, đặc biệt là đối với các tàu hiện có.

Implementation of cyber security controls should be prioritised, focusing first on those measures, or combinations of measures, which offer the greatest benefit.

Việc thực hiện các biện pháp kiểm soát an ninh mạng cần được ưu tiên, tập trung đầu tiên vào các biện pháp đó hoặc kết hợp các biện pháp mang lại lợi ích lớn nhất.

5.1 Technical protection measures
Các biện pháp bảo vệ bằng kỹ thuật

The Centre for Internet Security (CIS) provides guidance on measures (CIS, Critical Security Controls for Effective Cyber Security, available at www.cisecurity.org/critical-controls.cfm) that can be used to address cyber security vulnerabilities. The protection measures comprise of a list of Critical Security Controls (CSC) that are prioritised and vetted to ensure that they provide an effective approach for companies to assess and improve their defences. The CSCs include both technical and procedural aspects.

Trung tâm An ninh Internet (CIS) cung cấp hướng dẫn về các biện pháp (CIS, Kiểm soát an ninh quan trọng cho bảo mật mạng hiệu quả - www.cisecurity.org/critical-controls.cfm) có thể được sử dụng để giải quyết các lỗ hổng an ninh mạng. Các biện pháp bảo vệ bao gồm danh sách các Kiểm soát an ninh quan trọng (CSC) được ưu tiên và xem xét chặt chẽ để đảm bảo rằng chúng cung cấp cách tiếp cận hiệu quả cho các công ty để đánh giá và cải thiện hệ thống phòng thủ của họ. Các CSC bao gồm cả các khía cạnh kỹ thuật và quy trình.

The below mentioned examples of CSCs have been selected as particularly relevant to equipment and data onboard ships.

Các ví dụ được đề cập dưới đây của CSC đã được chọn là thích hợp đối với thiết bị và dữ liệu trên tàu.

Limitation to and control of network ports, protocols and services
Giới hạn và kiểm soát các cổng mạng, các giao thức và dịch vụ

Access lists to network systems can be used to implement the company's security policy. This ensures that only appropriate traffic will be allowed via a controlled network or subnet, based on the control policy of that network or subnet.

Có thể sử dụng danh sách truy cập vào các hệ thống mạng để triển khai chính sách an ninh của công ty. Điều này đảm bảo rằng chỉ có lưu lượng truy cập thích hợp sẽ được cho phép thông qua mạng hoặc mạng con được kiểm soát, dựa trên chính sách kiểm soát của mạng hoặc mạng con đó.

It should be a requirement that routers are secured against attacks and unused ports should be closed to prevent unauthorised access to systems or data.

Cần đưa ra yêu cầu là các bộ định tuyến được bảo mật chống lại các cuộc tấn công và các cổng không sử dụng nên được đóng lại để ngăn chặn truy cập trái phép vào các hệ thống hoặc dữ liệu.

Configuration of network devices such as firewalls, routers and switches
Cấu hình các thiết bị mạng như tường lửa, bộ định tuyến và thiết bị chuyển mạch

It should be determined which systems should be attached to controlled or uncontrolled networks (In accordance with EC 61162-460:2015: Maritime navigation and radiocommunication equipment and systems - Digital interfaces - Part 460: Multiple talkers and multiple listeners - Ethernet interconnection - Safety and security). Controlled networks are designed to prevent any security risks from connected devices by use of firewalls, security gateways, routers and switches. Uncontrolled networks may pose risks due to lack of data traffic control and they should be isolated from controlled networks, as direct internet connection makes them highly prone to infiltration by malware. For example:

Cần phải xác định hệ thTống nào được gắn vào mạng được kiểm soát hoặc không kiểm soát được (theo EC 61162-460: 2015: Thiết bị và hệ thống hành hải và thông tin liên lạc vô tuyến điện - Giao diện số - Phần 460: Nhiều người nói và nhiều người nghe - Kết nối ethernet - An toàn và an ninh). Mạng được kiểm soát được thiết kế để ngăn chặn mọi rủi ro an ninh từ các thiết bị được kết nối bằng cách sử dụng tường lửa, cổng an ninh, bộ định tuyến và thiết bị chuyển mạch. Mạng không được kiểm soát có thể gây rủi ro do thiếu kiểm soát lưu lượng dữ liệu và chúng phải được cách ly khỏi các mạng được kiểm soát, vì kết nối internet trực tiếp khiến chúng dễ bị xâm nhập bởi phần mềm độc hại. Ví dụ:

- Networks that are critical to the operation of a ship itself, should be controlled. It is imperative that these systems - have a high level of security.

  Các mạng quan trọng đối với hoạt động của tàu cần được kiểm soát. Điều bắt buộc là các hệ thống này - có mức độ an ninhh cao.

- Networks that provide suppliers with remote access to navigation and other OT system software on onboard equipment, should also be controlled. These networks may be necessary for suppliers to allow upload of system upgrades or perform remote servicing. Shoreside external access points of such connections should be secured to prevent unauthorised access.

  Các mạng cung cấp cho các nhà cung cấp khả năng truy cập từ xa vào phần mềm hành hải và phần mềm hệ thống OT khác trên thiết bị của tàu cũng cần được kiểm soát. Các mạng này có thể cần thiết cho các nhà cung cấp để cho phép tải lên các nâng cấp hệ thống hoặc thực hiện dịch vụ từ xa. Các điểm truy cập bên ngoài trên bờ của các kết nối như vậy phải được bảo mật để ngăn chặn truy cập trái phép.

- Other networks, such as guest access networks, may be uncontrolled, for instance those related to passenger recreational activities or private internet access for crew. Normally, any wireless network should be considered uncontrolled.

  Các mạng khác, chẳng hạn như mạng truy cập của khách, có thể không được kiểm soát, ví dụ như các mạng liên quan đến hoạt động giải trí hành khách hoặc truy cập internet riêng cho thuyền bộ. Thông thường, bất kỳ mạng không dây nào đều được coi là không kiểm soát được.

Onboard networks should be partitioned by firewalls to create safe zones. The fewer communications links and devices in a zone, the more secure the systems and data are in that zone. Confidential and safety critical systems should be in the most protected zone. See annex 2 of these guidelines for more information on shipboard networks and also refer to ISO/IEC 62443.

Các mạng trên tàu phải được phân đoạn bằng tường lửa để tạo vùng an toàn. Các liên kết và thiết bị thông tin liên lạc càng ít hơn trong một khu vực, thì hệ thống và dữ liệu càng an ninh hơn trong khu vực đó. Các hệ thống quan trọng về an toàn cần và bí mật phải ở trong khu vực được bảo vệ tốt nhất. Xem phụ lục 2 của Hướng dẫn này để biết thêm thông tin về mạng trên tàu và tham khảo ISO / IEC 62443.

Physical security
Bảo mật vật lý

Security and safety critical equipment and cable runs should be protected from unauthorised access. Physical security is a central aspect of cyber security (see also the ISPS Code).

Thiết bị quan trọng về an ninh, an toàn và dây cáp cần được bảo vệ khỏi truy cập trái phép. An ninh vật lý là một khía cạnh trung tâm của an ninh mạng (xem thêm Mã ISPS).

Detection, blocking and alerts
Phát hiện, chặn và cảnh báo

Identifying intrusions and infections is a vital part of the controls. A baseline of network operations and expected data flows for users and systems should be established and managed so that cyber incident alert thresholds can be established. Key to this will be the definition of roles and responsibilities for detection to ensure accountability. Additionally, a company may choose to incorporate an Intrusion Detection System (IDS) system or an Intrusion Prevention System (IPS) into the network or as part of the firewall. Some of their main functions include identifying threats/malicious activity and code, and then logging, reporting and attempting to block the activity. Further details concerning IDS and IPS can be found in annex 2 of these guidelines. Ensure that dedicated onboard personnel can understand the alerts and their implications. Incidents detected should be directed to an individual or service provider, who is responsible for acting on this type of alert.

Xác định xâm nhập và bị nhiễm độc là một phần quan trọng trong việc kiểm soát. Đường cơ sở của hoạt động mạng và luồng dữ liệu dự kiến cho người dùng và hệ thống nên được thiết lập, quản lý sao cho ngưỡng cảnh báo sự cố mạng có thể được thiết lập. Giải pháp cho vấn đề này là việc xác định vai trò và trách nhiệm đối với việc phát hiện để đảm bảo trách nhiệm giải trình. Ngoài ra, công ty có thể chọn kết hợp hệ thống Phát hiện xâm nhập (IDS) hoặc Hệ thống ngăn chặn xâm nhập (IPS) vào mạng hoặc là một phần của tường lửa. Một số chức năng chính của chúng bao gồm xác định các mối đe dọa/hoạt động độc hại và mã, sau đó ghi nhật ký, báo cáo và cố gắng chặn hoạt động. Thông tin chi tiết liên quan đến IDS và IPS có thể được tìm thấy trong Phụ lục 2 của Hướng dẫn này. Đảm bảo rằng nhân viên chuyên môn trên tàu có thể hiểu được các cảnh báo và ý nghĩa của chúng. Sự cố được phát hiện phải được chuyển đến một cá nhân hoặc nhà cung cấp dịch vụ, người chịu trách nhiệm về hành động về loại cảnh báo này.

Satellite and radio communication
Thông tin liên lạc vệ tinh và vô tuyến

Cyber security of the radio and satellite connection should be considered in collaboration with the service provider. In this connection, the specification of the satellite link should be considered when establishing the requirements for onboard network protection.

An ninh mạng của kết nối vô tuyến điện và vệ tinh cần được xem xét phối hợp với nhà cung cấp dịch vụ. Trong kết nối này, đặc điểm kỹ thuật của liên kết vệ tinh cần được xem xét khi thiết lập các yêu cầu để bảo vệ mạng trên tàu.

When establishing an uplink connection for ships' navigation and control systems to shore-based service providers, consideration should be given in how to prevent illegitimate connections gaining access to the onboard systems.

Khi thiết lập kết nối truyền tín hiệu cho hệ thống hành hải và kiểm soát của tàu đến các nhà cung cấp dịch vụ trên bờ, cần cân nhắc cách ngăn chặn các kết nối bất hợp pháp tiếp cận với các hệ thống trên tàu.

The access interconnect is the distribution partner's responsibility. The final routing of user traffic from the internet access point to its ultimate destination onboard ("last mile") is the responsibility of the shipowner. User traffic is routed through the communication equipment for onward transmission on board. At the access point for this traffic, it is necessary to provide data security, firewalling and a dedicated "last-mile" connection.

Kết nối truy cập là trách nhiệm của đối tác phân phối. Định tuyến cuối cùng của lưu lượng người dùng từ điểm truy cập internet đến đích cuối cùng của nó trên tàu ("dặm cuối cùng") là trách nhiệm của chủ tàu. Lưu lượng người dùng được định tuyến thông qua thiết bị thông tin liên lạc để truyền đi trên tàu. Tại điểm truy cập cho lưu lượng truy, cần phải cung cấp bảo mật dữ liệu, tường lửa và kết nối "cuối dặm" chuyên dụng.

When using a Virtual Private Network (VPN), the data traffic should be encrypted to an acceptable international standard. Furthermore, a firewall in front of the servers and computers connected to the networks (ashore or on board) should be deployed. The distribution partner should advise on the routing and type of connection most suited for specific traffic. Onshore filtering (inspection/blocking) of traffic is also a matter between a shipowner and the distribution partner. However, it is not sufficient to have either onshore filtering of traffic or firewalls/security inspection/blocking gateways on the ship, because both types are needed and supplement each other to achieve a sufficient level of protection.

Khi sử dụng Mạng riêng ảo (VPN), lưu lượng dữ liệu phải được mã hóa theo tiêu chuẩn quốc tế được chấp nhận. Hơn nữa, tường lửa ở phía trước của các máy chủ và máy tính kết nối với các mạng (trên bờ hoặc trên tàu) nên được triển khai. Đối tác phân phối nên tư vấn về định tuyến và loại kết nối phù hợp nhất cho lưu lượng truy cập cụ thể. Việc lọc trên bờ (kiểm tra/chặn) của lưu lượng truy cập cũng là vấn đề giữa chủ tàu và đối tác phân phối. Tuy nhiên, sẽ là không đủ nếu chỉ thực hiện lọc trên bờ đối với lưu lượng truy cập hoặc áp dụng tường lửa/kiểm tra an ninh/chặn cổng trên tàu, bởi vì cả hai loại là cần thiết và bổ sung cho nhau để đạt được một mức độ bảo vệ đầy đủ.

Producers of satellite communication terminals and other communication equipment may provide management interfaces with security control software that are accessible over the network. This is primarily provided in the form of web-based user interfaces. Protection of such interfaces should be considered when assessing the security of a ship's installation.

Nhà sản xuất thiết bị đầu cuối thông tin liên lạc vệ tinh và thiết bị thông tin liên lạc khác có thể cung cấp giao diện quản lý với phần mềm kiểm soát an ninh có thể truy cập qua mạng. Điều

này chủ yếu được cung cấp dưới dạng giao diện người dùng dựa trên web. Bảo vệ các giao diện như vậy cần được xem xét khi đánh giá tính bảo mật của quá trình cài đặt tàu.

Wireless access control

Kiểm soát truy cập không dây

It should be ensured that wireless access to networks on the ship is limited to appropriate authorised devices and secured using a strong encryption key, which is changed regularly.

Cần đảm bảo rằng truy cập không dây vào mạng trên tàu bị hạn chế với các thiết bị được phép phù hợp và được bảo mật bằng khóa mã hóa mạnh, được thay đổi thường xuyên.

Malware detection

Phát hiện phần mềm độc hại

Scanning software that can automatically detect and address the presence of malware in systems onboard should be regularly updated.

Phần mềm quét có thể tự động phát hiện và giải quyết sự hiện diện của phần mềm độc hại trong các hệ thống trên tàu nên được cập nhật thường xuyên.

As a general guideline, onboard computers should be protected to the same level as office computers ashore. Anti-virus and anti-malware software should be installed, maintained and updated on all personal work-related computers onboard. This will reduce the risk of these computers acting as attack vectors towards servers and other computers on the ship's network. The decision on whether to rely on these defence methods should take into consideration how regularly the scanning software will be able to be updated.

Như một hướng dẫn chung, các máy tính trên tàu phải được bảo vệ ở mức tương tự như các máy tính văn phòng trên bờ. Phần mềm chống vi-rút và phần mềm chống phần mềm độc hại phải được cài đặt, duy trì và cập nhật trên tất cả các máy tính liên quan đến công việc cá nhân trên tàu. Điều này sẽ làm giảm nguy cơ các máy tính này hoạt động như các vectơ tấn công đối với các máy chủ và các máy tính khác trên mạng của tàu. Quyết định về việc có dựa vào các phương pháp phòng thủ này hay không nên đươck xem xét theo tần suất phần mềm quét sẽ có thể được cập nhật.

Secure configuration for hardware and software

Cấu hình an toàn cho phần cứng và phần mềm

Only senior officers should be given administrator profiles so that they can control the set up and disabling of normal user profiles. User profiles should be restricted to only allow the computers, workstations or servers to be used for the purposes for which they are required. User profiles should not allow the user to alter the systems or install and execute new programs.

Chỉ các cán bộ cấp cao mới nên được cung cấp hồ sơ quản trị viên để họ có thể kiểm soát việc thiết lập và vô hiệu hóa hồ sơ người dùng thông thường. Hồ sơ người dùng nên được giới hạn để chỉ cho phép các máy tính, máy trạm hoặc máy chủ được sử dụng cho các mục đích mà chúng được yêu cầu. Hồ sơ người dùng không được cho phép người dùng thay đổi hệ thống hoặc cài đặt và thực thi các chương trình mới.

Email and web browser protection
Bảo vệ email và trình duyệt web

Email communication between ship and shore is a vital part of a ship's operation. Appropriate email and web browser protection serves to:

Giao tiếp qua email giữa tàu và bờ là một phần quan trọng trong hoạt động của tàu. Bảo vệ trình duyệt web và email phù hợp phục vụ:

- protect shoreside and onboard personnel from potential social engineering;
  Bảo vệ người trên bờ trên tàu từ kỹ thuật xã hội tiềm năng;
- prevent email being used as a method of obtaining sensitive information;
  Ngăn chặn email được sử dụng như một phương pháp thu thập thông tin nhạy cảm;
- ensure that the exchange of sensitive information via email or by voice is appropriately protected to ensure confidentiality and integrity of data, for example protecting by encryption;

  Đảm bảo rằng việc trao đổi thông tin nhạy cảm qua email hoặc bằng giọng nói được bảo vệ thích hợp để đảm bảo tính bảo mật và tính toàn vẹn của dữ liệu, ví dụ như bảo vệ bằng mã hóa;
- prevent web browsers and email clients from executing malicious scripts.
  Ngăn các trình duyệt web và khách hàng sử dụng email thực thi các tập lệnh độc hại.

Some best practices for safe email transfer are: email as zip or encrypted file when necessary, disable hyperlinks on email system, and avoid using generic email addresses and ensure the system has configured user accounts.

Một số thực hành tốt nhất để chuyển email an toàn là: email dưới dạng zip hoặc tệp được mã hóa khi cần, vô hiệu hóa siêu liên kết trên hệ thống email và tránh sử dụng địa chỉ email chung và đảm bảo hệ thống đã định cấu hình tài khoản người dùng.

Data recovery capability
Khả năng phục hồi dữ liệu

Data recovery capability is the ability to restore a system and/or data from a secure copy or image thereby allowing the restoration of a clean system. Essential information and software-adequate backup facilities should be available to ensure it can be recovered following a cyber incident.

Khả năng khôi phục dữ liệu là khả năng khôi phục hệ thống và/hoặc dữ liệu từ bản sao hoặc hình ảnh an toàn nhờ đó cho phép khôi phục hệ thống sạch. Thông tin cần thiết và các cơ sở sao lưu đầy đủ phần mềm phải có sẵn để đảm bảo nó có thể được phục hồi sau sự cố mạng.

Retention periods and restore scenarios should be established to prioritise which critical systems need quick restore capabilities to reduce the impact. Systems that have high data availability requirements should be made resilient. OT systems, which are vital to the safe navigation and operation of the ship, should have backup systems to enable the ship to quickly and safely regain navigational and operational capabilities after a cyber incident. More detail on recovery can be found in chapter 7 of these guidelines.

Thời gian lưu giữ và các kịch bản khôi phục nên được thiết lập để ưu tiên các hệ thống quan trọng cần khả năng khôi phục nhanh để giảm tác động. Các hệ thống có yêu cầu tính sẵn sàng cao về dữ liệu phải có khả năng thích ứng. Các hệ thống OT, quan trọng đối với việc hành hải

và hoạt động an toàn của tàu, cần có hệ thống sao lưu để cho phép tàu nhanh chóng và an toàn lấy lại khả năng hành hải và hoạt động sau sự cố mạng. Thông tin chi tiết về phục hồi có thể được tìm thấy trong chương 7 của Hướng dẫn này.

Application software security (patch management)
Bảo mật phần mềm ứng dụng (quản lý bản vá)

Critical safety and security updates should be provided to onboard systems. These updates or patches should be applied correctly and in a timely manner to ensure that any flaws in a system are addressed before they are exploited by a cyber attack.

Các bản cập nhật bảo mật và an toàn quan trọng cần được cung cấp cho các hệ thống trên tàu. Các bản cập nhật hoặc bản vá này phải được áp dụng chính xác và kịp thời để đảm bảo rằng mọi lỗ hổng trong hệ thống được giải quyết trước khi chúng bị khai thác bởi một cuộc tấn công mạng.

5.2 Procedural protection measures
Các biện pháp bảo vệ theo quy trình

Procedural controls are focused on how personnel use the onboard systems. Plans and procedures that contain sensitive information should be kept confidential and handled according to company policies. Examples for procedural actions can be:

Kiểm soát theo quy trình được tập trung vào cách nhân viên sử dụng các hệ thống trên tàu. Các kế hoạch và quy trình có chứa thông tin nhạy cảm phải được giữ bí mật và xử lý theo chính sách của công ty. Ví dụ về các hành động theo quy trình có thể là:

Training and awareness
Đào tạo và nhận thức

Training and awareness is the key supporting element to an effective approach to cyber safety and security as described in these guidelines and summarised in figure 1.

Đào tạo và nhận thức là yếu tố hỗ trợ quan trọng để tiếp cận hiệu quả an toàn và an ninh mạng như được mô tả trong Hướng dẫn này và tóm tắt trong hình 1.

The internal cyber threat is considerable and should not be underestimated. Personnel have a key role in protecting IT and OT systems but can also be careless, for example by using removable media to transfer data between systems without taking precautions against the transfer of malware. Training and awareness should be tailored to the appropriate levels for:

Các mối đe dọa mạng nội bộ là đáng kể và không nên đánh giá thấp. Nhân viên có vai trò quan trọng trong việc bảo vệ hệ thống IT và OT nhưng cũng có thể bất cẩn, ví dụ bằng cách sử dụng phương tiện di động (tháo lắp được) để truyền dữ liệu giữa các hệ thống mà không thực hiện các biện pháp phòng ngừa việc chuyển phần mềm độc hại. Đào tạo và nâng cao nhận thức cần được điều chỉnh phù hợp với các cấp độ thích hợp để:

- onboard personnel including the master, officers and crew;
  Người trên tàu bao gồm thuyền trưởng, sĩ quan và thuyền viên;
- shoreside personnel, who support the management and operation of the ship.
  Nhân viên trên bờ hỗ trợ việc quản lý và vận hành tàu.

These guidelines assume that other major stakeholders in the supply chain, such as charterers, classification societies and service providers, will carry out their own best-practice cyber security protection and training. It is advised that owners and operators ascertain the

status of cyber security preparedness of their third-party providers as part of their sourcing procedures for such services.

Hướng dẫn này giả định rằng các bên liên quan khác trong chuỗi cung ứng, như người thuê tàu, tổ chức phân cấp tàu và nhà cung cấp dịch vụ, sẽ thực hiện bảo vệ và đào tạo an ninh mạng theo thực hành tốt nhất của bản thân họ. Khuyến cáo các chủ tàu và người kha thác tàu nắm chắc tình trạng chuẩn bị an ninh mạng của các nhà cung cấp bên thứ ba của họ như là một phần của quy trình tìm nguồn cung ứng cho các dịch vụ đó.

An awareness programme should be in place for all onboard personnel, covering at least the following:

Chương trình về nhận thức nên được áp dụng cho tất cả những trên tàu, bao gồm ít nhất những nội dung sau đây:

- risks related to emails and how to behave in a safe manner (examples are phishing attacks where the user clicks on a link to a malicious site);

  Các rủi ro liên quan đến email và cách ứng xử một cách an toàn (ví dụ là các cuộc tấn công lừa đảo mà người dùng nhấp vào liên kết đến trang web độc hại);

- risks related to internet usage, including social media, chat forums and cloud-based file storage where data movement is less controlled and monitored;

  Các rủi ro liên quan đến việc sử dụng internet, bao gồm các phương tiện truyền thông xã hội, diễn đàn trò chuyện và lưu trữ tệp dựa trên đám mây, khi mà việc di chuyển dữ liệu ít được kiểm soát và giám sát hơn;

- risks related to the use of own devices (these devices may be missing security patches and controls, such as anti-virus, and may transfer the risk to the environment to which they are connected);

  Các rủi ro liên quan đến việc sử dụng các thiết bị của riêng mình (các thiết bị này có thể thiếu các bản vá và kiểm soát bảo mật, chẳng hạn như chống vi-rút và có thể chuyển rủi ro đến môi trường mà chúng được kết nối);

- risks related to installing and maintaining software on company hardware using infected hardware (removable media) or software (infected package);

  Các rủi ro liên quan đến việc cài đặt và bảo trì phần mềm trên phần cứng của công ty sử dụng phần cứng bị nhiễm (phương tiện di động) hoặc phần mềm (gói bị nhiễm);

- risks related to poor software and data security practices where no anti-virus checks or authenticity verifications are performed;

  Các rủi ro liên quan đến thực hành bảo mật dữ liệu và phần mềm yếu kém, nơi không có kiểm tra xác thực hoặc kiểm chứng tính xác thực;

- safeguarding user information, passwords and digital certificates;
  Bảo vệ thông tin người dùng, mật khẩu và chứng chỉ số;

- cyber risks in relation to the physical presence of non-company personnel, eg, where thirdparty technicians are left to work on equipment without supervision;

  Các rủi ro mạng liên quan đến sự hiện diện vật lý của các nhân viên không phải là người của công ty, ví dụ, nơi các kỹ thuật viên bên thứ ba phải làm việc trên thiết bị mà không có sự giám sát;

- detecting suspicious activity or devices and how to report if a possible cyber incident is in progress (examples of this are strange connections that are not normally seen or someone plugging in an unknown device on the ship network);

  Phát hiện hoạt động hoặc thiết bị đáng ngờ và cách báo cáo nếu sự cố mạng có thể xảy ra (ví dụ về các kết nối lạ thường không được nhìn thấy hoặc ai đó cắm thiết bị không xác định trên mạng của tàu);

- awareness of the consequences or impact of cyber incidents to the safety and operations of the ship;
  Nhận thức về hậu quả hoặc tác động của sự cố mạng đến sự an toàn và hoạt động của tàu;.
- understanding how to implement preventative maintenance routines such as anti-virus and anti-malware, patching, backups, and incident-response planning and testing;

  Hiểu cách thực hiện các thói quen bảo trì phòng ngừa như chống virus và chống phần mềm độc hại, vá, sao lưu và lập kế hoạch và thử nghiệm đáp trả sự cố;

- procedures for protection against risks from service providers' removable media before connecting to the ship's systems.

  Các quy trình bảo vệ chống lại rủi ro từ phương tiện di động của nhà cung cấp dịch vụ trước khi kết nối với hệ thống của tàu.

In addition, personnel need to be made aware that the presence of anti-malware software does not remove the requirement for robust security procedures, for example controlling the use of all removable media.

Ngoài ra, nhân viên cần nhận thức rằng sự hiện diện của phần mềm chống phần mềm độc hại không loại bỏ yêu cầu về các quy trình bảo mật mạnh, ví dụ như kiểm soát việc sử dụng tất cả các phương tiện di động.

Further, applicable personnel should know the signs when a computer has been compromised. This may include the following:

Hơn nữa, nhân viên có thể áp dụng nên biết các dấu hiệu khi máy tính bị xâm phạm. Điều này có thể bao gồm những vấn đề sau đây:

- an unresponsive or slow to respond system;
  Hệ thống phản hồi không phản hồi hoặc chậm;
- unexpected password changes or authorised users being locked out of a system;

  Thay đổi mật khẩu không mong muốn hoặc người dùng được ủy quyền bị khóa khỏi hệ thống;

- unexpected errors in programs, including failure to run correctly or programs running unexpectedly;

  Lỗi không mong muốn trong các chương trình, bao gồm cả việc không chạy đúng hoặc các chương trình chạy bất ngờ;

- unexpected or sudden changes in available disk space or memory;
  Thay đổi bất ngờ hoặc đột ngột trong không gian đĩa hoặc bộ nhớ còn trống;
- emails being returned unexpectedly;
  Email bị trả lại bất ngờ;

- unexpected network connectivity difficulties;
  Khó khăn bất ngờ trong kết nối mạng;
- frequent system crashes;
  Sự cố hệ thống thường xuyên;
- abnormal hard drive or processor activity;
  Hoạt động của bộ xử lý hoặc ổ cứng bất thường;
- unexpected changes to browser, software or user settings, including permissions.

  Những thay đổi bất ngờ đối với cài đặt trình duyệt, phần mềm hoặc người dùng, bao gồm cả sự cho phép.

And, nominated personnel should be able to understand reports from IDS systems, if used. This list is not comprehensive and is intended to raise awareness of potential signs, which should be treated as possible cyber incidents.

Và, nhân viên được chỉ định sẽ có thể hiểu các báo cáo từ các hệ thống IDS, nếu được sử dụng. Danh sách này không phải là toàn diện và được thiết kế để nâng cao nhận thức về các dấu hiệu tiềm năng, nên được coi là sự cố mạng có thể xảy ra.

Access for visitors
Quyền truy cập cho người đến thăm

Du khách như các cơ quan chức năng, kỹ thuật viên, đại lý, quan chức cảng và đại diện chủ sở hữu nên bị hạn chế đối với việc truy cập máy tính trong khi lên máy bay. Truy cập trái phép vào các máy tính mạng OT nhạy cảm nên bị cấm thông qua các rào cản vật lý được đánh dấu rõ ràng. Nếu truy cập vào mạng của khách truy cập là bắt buộc và được cho phép, thì nó sẽ bị hạn chế về đặc quyền của người dùng. Việc truy cập vào một số mạng nhất định vì lý do bảo trì cần được phê duyệt và phối hợp theo các thủ tục thích hợp như được nêu rõ bởi nhà điều hành công ty / tàu. Nếu khách truy cập yêu cầu truy cập máy tính và máy in, một máy tính độc lập, được kết nối không khí từ tất cả các mạng được kiểm soát, nên được sử dụng. Để tránh truy cập trái phép, các trình chặn phương tiện di động nên được sử dụng trên tất cả các máy tính có thể truy cập vật lý và các cổng mạng khác.

Visitors such as authorities, technicians, agents, port officials, and owner representatives should be restricted with regard to computer access whilst on board. Unauthorised access to sensitive OT network computers should be prohibited through clearly marked physical barriers. If access to a network by a visitor is required and allowed, then it should be restricted in terms of user privileges. Access to certain networks for maintenance reasons should be approved and coordinated following appropriate procedures as outlined by the company/ship operator. If a visitor requires computer and printer access, an independent computer, which is air-gapped from all controlled networks, should be used. To avoid unauthorised access, removable media blockers should be used on all other physically accessible computers and network ports.

Người đến thăm như các cơ quan chức năng, kỹ thuật viên, đại lý, quan chức cảng và đại diện chủ tàu nên bị hạn chế đối với việc truy cập máy tính trong khi ở trên tau. Truy cập trái phép vào các máy tính mạng OT nhạy cảm nên bị cấm thông qua các rào cản vật lý được đánh dấu rõ ràng. Nếu việc truy cập vào mạng của người đến thăm là bắt buộc và được cho phép, thì nó sẽ bị hạn chế về đặc quyền của người dùng. Việc truy cập vào một số mạng nhất định vì lý do bảo trì cần được phê duyệt và phối hợp theo các quy trình thích hợp quy định bởi công ty/người khai thác tàu. Nếu người đến thăm yêu cầu việc truy cập máy tính và máy in, thì nên sử dụng máy tính không được kết nối với các mạng được kiểm soát. Để tránh truy cập trái

phép, các trình chặn phương tiện di động nên được sử dụng trên tất cả các máy tính có thể truy cập vật lý và các cổng mạng khác.

Upgrades and software maintenance
Nâng cấp và bảo trì phần mềm

Hardware or software that is no longer supported by its producer or software developer will not receive updates to address potential vulnerabilities. For this reason, the use of hardware and software, which is no longer supported, should be carefully evaluated by the company as part of the cyber risk assessment.

Phần cứng hoặc phần mềm không còn được nhà sản xuất hoặc nhà phát triển phần mềm hỗ trợ sẽ không nhận được bản cập nhật để giải quyết các lỗ hổng tiềm ẩn. Vì lý do này, việc sử dụng phần cứng và phần mềm không còn được hỗ trợ, nên được công ty đánh giá cẩn thận như một phần của đánh giá rủi ro mạng.

Relevant hardware and software installations on board should be updated to maintain a sufficient security level. Procedures for timely updating of software may need to be put in place taking into account the ship type, speed of internet connectivity, sea time, etc. Software includes computer operating systems, which should also be kept up to date.

Cài đặt phần cứng và phần mềm có liên quan trên tàu phải được cập nhật để duy trì mức độ bảo mật đầy đủ. Quy trình cập nhật kịp thời phần mềm có thể cần được tính đến loại tàu, tốc độ kết nối internet, thời gian đi biển, ... Phần mềm bao gồm hệ điều hành máy tính cũng cần được cập nhật.

Additionally, a number of routers, switches and firewalls, and various OT devices will be running their own firmware, which may require regular updates and so should be addressed in the procedural requirements.

Ngoài ra, một số thiết bị định tuyến, thiết bị chuyển mạch, tường lửa và các thiết bị OT khác nhau sẽ chạy chương trình cơ sở của riêng chúng, có thể yêu cầu cập nhật thường xuyên và do đó cần được giải quyết trong các yêu cầu về quy trình.

Effective maintenance of software depends on the identification, planning and execution of measures necessary to support maintenance activities throughout the full software lifecycle. An industry standard (See: Industry standard on software maintenance of shipboard equipment by BIMCO and CIRM (Comité International Radio-Maritime)) to ensure safe and secure software maintenance has been developed. It specifies requirements for all stakeholders involved in software maintenance of shipboard equipment and associated integrated systems. The standard covers on board, on shore and remote software maintenance.

Việc bảo trì phần mềm hiệu quả phụ thuộc vào việc xác định, lập kế hoạch và thực hiện các biện pháp cần thiết để hỗ trợ các hoạt động bảo trì trong toàn bộ vòng đời phần mềm. Tiêu chuẩn công nghiệp (xem: Tiêu chuẩn công nghiệp về bảo trì phần mềm thiết bị trên tàu của BIMCO và CIRM (Comité International Radio-Maritime)) để đảm bảo việc bảo trì phần mềm an toàn và bảo mật đã được phát triển. Nó quy định các yêu cầu cho tất cả các bên liên quan tham gia vào việc bảo trì phần mềm thiết bị trên tàu và các hệ thống tích hợp liên quan. Các tiêu chuẩn bao gồm trên tàu, trên bờ và bảo trì phần mềm từ xa.

Anti-virus and anti-malware tool updates
Cập nhật công cụ chống vi-rút và chống phần mềm độc hại

In order for scanning software tools to detect and deal with malware, they need to be updated. Procedural requirements should be established to ensure updates are distributed to ships on a timely basis and that all relevant computers on board are updated.

Để quét các công cụ phần mềm nhằm phát hiện và xử lý phần mềm độc hại, chúng cần được cập nhật. Yêu cầu về quy trình phải được thiết lập để đảm bảo cập nhật được phân phối cho tàu kịp thời và tất cả các máy tính có liên quan trên tàu đều được cập nhật.

Remote access
Tiếp cận từ xa

Policy and procedures should be established for control over remote access to onboard IT and OT systems. Clear guidelines should establish who has permission to access, when they can access, and what they can access. Any procedures for remote access should include close co-ordination with the ship's master and other key senior ship personnel.

Chính sách và quy trình cần được thiết lập để kiểm soát truy cập từ xa vào các hệ thống IT và OT trên tàu. Các hướng dẫn rõ ràng cần quy định ai có quyền truy cập, khi nào họ có thể truy cập và những gì họ có thể truy cập. Bất kỳ quy trình nào để truy cập từ xa đều phải có sự phối hợp chặt chẽ với thuyền trưởng và các nhân viên cao cấp quan trọng khác trên tàu.

All remote access occurrences should be recorded for review in case of a disruption to an IT or OT system. Systems, which require remote access, should be clearly defined, monitored and reviewed periodically.

Tất cả các lần truy cập từ xa phải được ghi lại để xem xét trong trường hợp có sự gián đoạn đối với hệ thống IT hoặc OT. Các hệ thống yêu cầu truy cập từ xa cần được xác định rõ ràng, theo dõi và xem xét định kỳ.

Use of administrator privileges
Sử dụng đặc quyền của quản trị viên

Access to information should only be allowed to relevant authorised personnel.
Truy cập thông tin chỉ được phép cho nhân viên được ủy quyền có liên quan.

Administrator privileges allow full access to system configuration settings and all data. Users logging into systems with administrator privileges may enable existing vulnerabilities to be more easily exploited. Administrator privileges should only be given to appropriately trained personnel who have a need, as part of their role in the company or on board, to log into systems using these privileges. In any case, use of administrator privileges should always be limited to functions requiring such access.

Đặc quyền của quản trị viên cho phép truy cập đầy đủ vào cài đặt cấu hình hệ thống và tất cả dữ liệu. Người dùng đăng nhập vào các hệ thống có quyền quản trị có thể cho phép các lỗ hổng hiện có dễ khai thác hơn. Đặc quyền của quản trị viên chỉ nên được trao cho những nhân viên được đào tạo thích hợp, những người có nhu cầu, như một phần vai trò của họ trong công ty hoặc trên tàu, để đăng nhập vào các hệ thống bằng cách sử dụng các đặc quyền này. Trong mọi trường hợp, việc sử dụng đặc quyền của quản trị viên sẽ luôn bị giới hạn ở các chức năng yêu cầu quyền truy cập đó.

User privileges should be removed when the people concerned are no longer on board. User accounts should not be passed on from one user to the next using generic user names. Similar rules should be applied to any onshore personnel with remote access to systems on ships when they change role and no longer need access.

Đặc quyền của người dùng sẽ bị xóa khi những người liên quan không còn ở trên tàu nữa. Tài khoản người dùng không được chuyển từ người dùng này sang người dùng khác bằng tên người dùng chung. Quy tắc tương tự nên được áp dụng cho bất kỳ nhân viên trên bờ nào có quyền truy cập từ xa vào hệ thống trên tàu khi họ thay đổi vai trò và không cần truy cập nữa.

In a business environment, such as shipping, access to onboard systems is granted to various stakeholders. Suppliers and contractors are a risk because they often have both intimate knowledge of a ship's operations and often full access to systems.

Trong môi trường kinh doanh, chẳng hạn như vận tải biển, quyền truy cập vào các hệ thống trên tàu được cấp cho các bên liên quan khác nhau. Các nhà cung cấp và nhà thầu là một rủi ro vì họ thường có cả kiến thức sâu sắc về hoạt động của tàu và thường truy cập đầy đủ vào các hệ thống.

To protect access to confidential data and safety critical systems, a robust password policy should be developed (more information can be found in NIST publication SP 800-63-3 Digital Identity Guidelines). Passwords should be strong and changed periodically. The company policy should address the fact that over-complicated passwords, which must be changed too frequently, are at risk of being written on a piece of paper and kept near the computer.

Để bảo vệ quyền truy cập vào dữ liệu bí mật và các hệ thống an toàn quan trọng, nên xây dựng một chính sách mật khẩu mạnh mẽ (có thể tìm thêm thông tin trong ấn phẩm SP 800-63-3 Hướng dẫn nhận dạng số của NIST). Mật khẩu phải mạnh và thay đổi định kỳ. Chính sách của công ty nên giải quyết thực tế là mật khẩu quá phức tạp, phải được thay đổi quá thường xuyên, có nguy cơ bị viết trên một mảnh giấy và được giữ gần máy tính.

Physical and removable media controls
Kiểm soát truyền thông vật lý di động

Transferring data from uncontrolled systems to controlled systems represents a major risk of introducing malware. Removable media can be used to bypass layers of defences and can be used to attack systems that are otherwise not connected to the internet. A clear policy for the use of such media devices is essential; it must ensure that media devices are not normally used to transfer information between un-controlled and controlled systems.

Việc chuyển dữ liệu từ các hệ thống không kiểm soát được sang các hệ thống được kiểm soát là rủi ro chính của việc giới thiệu phần mềm độc hại. Truyền thông di động có thể được sử dụng để bỏ qua các lớp phòng thủ và có thể được sử dụng để tấn công các hệ thống không được kết nối với internet. Một chính sách rõ ràng cho việc sử dụng các thiết bị truyền thông như vậy là rất cần thiết; nó phải đảm bảo rằng các thiết bị truyền thông thường không được sử dụng để truyền thông tin giữa các hệ thống không được kiểm soát và kiểm soát.

There are, however, situations where it is unavoidable to use these media devices, for example during software maintenance. In such cases, there should be a procedure in place to require checking of removable media for malware and/or validating legitimate software by digital signatures and watermarks.

Tuy nhiên, có những trường hợp không thể tránh khỏi khi sử dụng các thiết bị truyền thông này, ví dụ như trong quá trình bảo trì phần mềm. Trong những trường hợp như vậy, cần phải có một quy trình để yêu cầu kiểm tra phương tiện di động liên quan đến phần mềm độc hại và/hoặc xác nhận hợp lệ phần mềm hợp pháp bằng chữ ký số và hình mờ.

Policies and procedures relating to the use of removable media should include a requirement to scan any removable media device in a computer that is not connected to the ship's controlled networks. If it is not possible to scan the removable media on board, eg the laptop of a maintenance technician, then the scan could be done prior to boarding with the result

and timing duly documented. Companies should consider notifying ports and terminals about the requirement to scan removable media prior to permitting the uploading of files onto a ship's system. This scanning should be carried out when transferring the following file types:

Các chính sách và quy trình liên quan đến việc sử dụng truyền thông di động phải bao gồm yêu cầu quét bất kỳ thiết bị truyền thông di động nào trong máy tính không được kết nối với mạng được kiểm soát của tàu. Nếu không thể quét truyền hông di động trên tàu, ví dụ như máy tính xách tay của kỹ thuật viên bảo trì, thì việc quét có thể được thực hiện trước khi lên tàu với kết quả và thời gian được lập thành hồ sơ đầy đủ. Các công ty nên cân nhắc việc thông báo các cổng và thiết bị đầu cuối về yêu cầu quét truyền thông di động trước khi cho phép tải tệp lên hệ thống của tàu. Quá trình quét này phải được thực hiện khi chuyển các loại tệp sau:

- cargo files and loading plans eg container ship BAPLIE files;

  Cập tập tin về hàng hóa và sơ đồ xếp hàng, ví dụ như tập tin BAPLIE của tàu container (sơ đồ xếp container của tàu trong đó đã có số container và vị trí chính xác của container trên tàu);
- national, customs, and port authority forms;
  Các biểu mẫu của quốc gia, hải quan và cơ quan có thẩm quyền tại cảng;
- bunkering and lubrication oil forms;
  Các biểu mẫu về dầu nhiên liệu và dầu bôi trơn;
- ship's stores and provisions lists;
  Danh mục đồ dự trữ và nhu yếu phẩm của tàu;
- engineering maintenance files.
  Các tệp bảo trì kỹ thuật.

This list represents examples and should not be seen as exhaustive.
Danh sách này đưa ra các ví dụ và không nên được xem là đầy đủ.

Equipment disposal, including data destruction
Loại bỏ thiết bị, bao gồm cả phá hủy dữ liệu

Obsolete equipment can contain data which is commercially sensitive or confidential. The company should have a procedure in place to ensure that the data held in obsolete equipment is properly destroyed prior to disposing of the equipment, ensuring that vital information cannot be retrieved.

Thiết bị lỗi thời có thể chứa dữ liệu nhạy cảm về mặt thương mại hoặc bí mật. Công ty cần có quy trình để đảm bảo rằng dữ liệu được lưu trữ trong thiết bị lỗi thời bị phá hủy hoàn toàn trước khi loại bỏ thiết bị, đảm bảo không thể khôi phục được thông tin quan trọng.

Obtaining support from ashore and contingency plans
Nhận hỗ trợ từ các kế hoạch dự phòng trên bờ

Ships should have access to technical support in the event of a cyber attack. Details of this support and associated procedures should be available on board. Please refer to Chapter 6 of these guidelines for more information about contingency planning.

Tàu phải có quyền truy cập vào hỗ trợ kỹ thuật trong trường hợp có tấn công mạng. Thông tin chi tiết về hỗ trợ này và các quy trình liên quan cần có sẵn trên tàu. Tham khảo Chương 6 của Hướng dẫn này để biết thêm thông tin về lập kế hoạch dự phòng.

6. Establish contingency plans
Thiết lập kế hoạch dự phòng

When developing contingency plans for implementation onboard ships, it is important to understand the significance of any cyber incident, particularly for IT and OT systems and prioritise response actions accordingly.

Khi xây dựng kế hoạch dự phòng để thực hiện trên tàu, điều quan trọng là phải hiểu tầm quan trọng của bất kỳ sự cố mạng nào, đặc biệt đối với các hệ thống IT và OT và ưu tiên các hành động phản ứng phù hợp.

Any cyber incident should be assessed in accordance with the CIA model (see chapter 4) to estimate the impact on operations, assets etc. In most cases, a loss of IT systems on board, including a data breach of confidential information, will be a business continuity issue and should not have any impact on the safe operation of the ship. In the event of a cyber incident affecting IT systems only, the priority may be the immediate implementation of an investigation and recovery plan.

Bất kỳ sự cố mạng nào cũng phải được đánh giá theo mô hình CIA (xem chương 4) để ước tính tác động đến hoạt động, tài sản, ... Trong hầu hết các trường hợp, mất hệ thống IT trên tàu, bao gồm việc vi phạm dữ liệu thông tin bí mật, sẽ là vấn đề liên tục trong kinh doanh và không nên có bất kỳ tác động nào đến hoạt động an toàn của tàu. Trong trường hợp sự cố mạng chỉ ảnh hưởng đến hệ thống IT, thì ưu tiên có thể là việc triển khai ngay lập tức kế hoạch điều tra và khôi phục.

The loss of OT systems may have a significant and immediate impact on the safe operation of the ship. Should a cyber incident result in the loss or malfunctioning of OT systems, it will be essential that effective actions are taken to ensure the immediate safety of the crew, ship and protection of the marine environment. In general, appropriate contingency plans for cyber incidents, including the loss of critical systems and the need to use alternative modes of operation, should be addressed by appropriate operational and emergency procedures included in the safety management system. Some of the existing procedures in the ship's safety management system have already covered such cyber incidents.

Việc mất các hệ thống OT có thể có tác động đáng kể và ngay lập tức đến hoạt động an toàn của tàu. Nếu một sự cố mạng dẫn đến sự mất mát hoặc trục trặc của hệ thống OT, điều quan trọng là phải thực hiện các hành động hiệu quả để đảm bảo an toàn ngay lập tức cho thuyền bộ, tàu và bảo vệ môi trường biển. Nói chung, các kế hoạch dự phòng thích hợp cho các sự cố mạng, bao gồm cả việc mất các hệ thống quan trọng và nhu cầu sử dụng các phương thức hoạt động thay thế, cần được đề cập bằng các quy trình vận hành và khẩn cấp phù hợp trong hệ thống quản lý an toàn. Một số quy trình hiện có trong hệ thống quản lý an toàn của tàu đã bao gồm các sự cố mạng như vậy.

The safety management system will already include procedures for reporting accidents or hazardous situations and define levels of communication and authority for decision making. Where appropriate, such procedures should be amended to reflect communication and authority in the event of a cyber incident.

Hệ thống quản lý an toàn sẽ bao gồm các quy trình báo cáo sự cố hoặc các tình huống nguy hiểm và xác định mức độ thông tin liên lạc và thẩm quyền để ra quyết định. Khi thích hợp, các quy trình như vậy sẽ được sửa đổi để phản ánh thông tin liên lạc và thẩm quyền trong trường hợp xảy ra sự cố mạng.

The following is a non-exhaustive list of the actions in response to the type of cyber incidents, which should be addressed in contingency plans on board:

Sau đây là danh sách không đầy đủ các hành động để đáp ứng với loại sự cố mạng cần được đề cập trong các kế hoạch dự phòng trên tàu:

- loss of availability of electronic navigational equipment or loss of integrity of navigation related data;

  Mất khả năng sử dụng thiết bị hành hải điện tử hoặc mất tính toàn vẹn của dữ liệu liên quan đến hành hải;

- loss of availability or integrity of external data sources, including but not limited to GNSS;

  Mất tính khả dụng hoặc tính toàn vẹn của các nguồn dữ liệu bên ngoài, bao gồm nhưng không giới hạn đối với GNSS;

- loss of essential connectivity with the shore, including but not limited to the availability of Global Maritime Distress and Safety System (GMDSS) communications;

  Mất kết nối thiết yếu với bờ, bao gồm nhưng không giới hạn đối với sự sẵn có của thông tin liên lạc sử dụng hệ thống an toàn và thông tin hàng hải toàn cầu (GMDSS);

- loss of availability of industrial control systems, including propulsion, auxiliary systems and other critical systems, as well as loss of integrity of data management and control;

  Mất các hệ thống kiểm soát công nghiệp, bao gồm động cơ đẩy, hệ thống phụ trợ và các hệ thống quan trọng khác, cũng như mất tính toàn vẹn của quản lý và kiểm soát dữ liệu;

- the event of a ransomware or denial or service incident.
  Các sự kiện của phần mềm gián điệp hoặc từ chối hoặc sự cố dịch vụ.

It is important that onboard personnel understand that the loss of OT systems due to a cyber incident must be treated like any other equipment failure. Furthermore, it is important to ensure that a loss of equipment or reliable information due to a cyber incident does not make existing emergency plans and procedures redundant. It is crucial that contingency plans, and related information, are available in a non-electronic form as some types of cyber incidents can include the deletion of data and shutdown of communication links.

Điều quan trọng là người trên tàu hiểu rằng việc mất các hệ thống OT do sự cố mạng phải được xử lý giống như bất kỳ lỗi thiết bị nào khác. Hơn nữa, điều quan trọng là phải đảm bảo rằng việc mất thiết bị hoặc thông tin tin cậy do sự cố mạng không làm cho các kế hoạch và quy trình dự phngf hiện có trở nên dư thừa. Điều quan trọng là kế hoạch dự phòng và thông tin liên quan có sẵn ở dạng không phải điện tử vì một số loại sự cố mạng có thể bao gồm việc xóa dữ liệu và tắt liên kết thông tin liên lạc.

There may be occasions when responding to a cyber incident may be beyond the competencies on board or at head office due to the complexity or severity of such incidents. In these cases, external expert assistance may be required (for example post event forensic analysis and clean-up).

Có thể có những dịp khi đáp trả sự cố mạng có thể vượt quá khả năng trên tàu hoặc tại trụ sở chính do tính chất phức tạp hoặc mức độ nghiêm trọng của các sự cố đó. Trong những trường hợp này, sự hỗ trợ của chuyên gia bên ngoài có thể được yêu cầu (ví dụ như phân tích điều tra và làm sạch sau sự kiện).

7. Respond to and recover from cyber security incidents
Đáp trả và khôi phục từ sự cố an ninh mạng

It is important to understand that cyber incidents may not disappear by themselves. If for example the ECDIS has been infected with malware, starting up the back-up ECDIS may cause another cyber incident. It is, therefore, recommended to plan how to carry out the cleaning and restoring of infected systems.

Điều quan trọng là phải hiểu rằng sự cố trên mạng có thể không tự biến mất. Ví dụ, nếu ECDIS đã bị nhiễm phần mềm độc hại, khởi động ECDIS dự phòng có thể gây ra một sự cố mạng khác. Do đó, nên lập kế hoạch làm thế nào để thực hiện việc làm sạch và khôi phục lại các hệ thống bị lây nhiễm.

Knowledge about previous identified cyber incidents should be used to improve the response plans of all ships in the company's fleet and an information strategy for such incidents may be considered.

Kiến thức về các sự cố mạng đã được nhận biết trước đó nên được sử dụng để cải thiện các kế hoạch ứng phó của tất cả các tàu trong đội tàu của công ty và một chiến lược thông tin cho các sự cố như vậy có thể được xem xét.

7.1 Effective response
Đáp trả hiệu quả

A team, which may include a combination of onboard and shore-based personnel and/or external experts, should be established to take the appropriate action to restore the IT and/or OT systems so that the ship can resume normal operations. The team should be capable of performing all aspects of the response.

Một nhóm, có thể bao gồm sự kết hợp giữa nhân viên trên tàu và trên bờ và/hoặc các chuyên gia bên ngoài, nên được thiết lập để có hành động thích hợp để khôi phục hệ thống IT và/hoặc OT để tàu có thể tiếp tục hoạt động bình thường. Nhóm phải có khả năng thực hiện tất cả các khía cạnh của phản hồi.

An effective response should at least consist of the following steps:

Một phản hồi hiệu quả ít nhất phải bao gồm các bước sau:

1. **Initial assessment:** To ensure an appropriate response, it is essential that the response team find out:

   Đánh giá ban đầu: *Để đảm bảo sự phản hồi thích hợp, nhóm phản hồi cần tìm ra:*

   - how the incident occurred;
     Sự việc xảy ra như thế nào;
   - which IT and/or OT systems were affected and how;
     Hệ thống IT và/hoặc OT nào bị ảnh hưởng và cách thức ảnh hưởng;
   - the extent to which the commercial and/or operational data is affected;
     Phạm vi mà dữ liệu thương mại và/hoặc hoạt động bị ảnh hưởng;
   - to what extent any threat to IT and OT remains.
     Ở mức độ nào mà bất kỳ mối đe dọa nào đối với IT và OT vẫn còn tồn tại.

2. **Recover systems and data:** Following an initial assessment of the cyber incident, IT and OT systems and data should be cleaned, recovered and restored, so far as is possible, to an operational condition by removing threats from the system and restoring software. The content of a recovery plan is covered in section 7.2.

   Khôi phục hệ thống và dữ liệu: *Sau đánh giá ban đầu về sự cố mạng, các hệ thống và dữ liệu IT và OT phải được làm sạch, khôi phục và phục hồi, đến mức độ có thể, về điều kiện hoạt động bằng cách loại bỏ các mối đe dọa khỏi hệ thống và phần mềm khôi phục. Nội dung của kế hoạch phục hồi được trình bày trong phần 7.2.*

3. **Investigate the incident:** To understand the causes and consequences of a cyber incident, an investigation should be undertaken by the company, with support from an external expert, if appropriate. The information from an investigation will play a significant role in preventing a potential recurrence. Investigations into cyber incidents are covered in section 7.3.

   Điều tra vụ việc: *Để hiểu nguyên nhân và hậu quả của một sự cố mạng, công ty cần tiến hành điều tra với sự hỗ trợ của một chuyên gia bên ngoài, nếu thích hợp. Thông tin từ cuộc điều tra sẽ đóng một vai trò quan trọng trong việc ngăn chặn sự tái diễn tiềm tàng. Các điều tra về sự cố mạng được đề cập trong phần 7.3.*

4. **Prevent a re-occurrence:** Considering the outcome of the investigation mentioned above, actions to address any inadequacies in technical and/or procedural protection measures should be considered, in accordance with the company procedures for implementation of corrective action.

   Ngăn chặn sự tái diễn: *Xem xét kết quả điều tra đã đề cập ở trên, các hành động đề cập đến bất kỳ bất cập nào về các biện pháp bảo vệ kỹ thuật và/hoặc theo quy trình cần được xem xét, phù hợp với các quy trình của công ty để thực hiện hành động khắc phục.*

When a cyber incident is complex, for example if IT and/or OT systems cannot be returned to normal operation, it may be necessary to initiate the recovery plan alongside onboard contingency plans. When this is the case, the response team should be able to provide advice to the ship on:

Khi một sự cố mạng phức tạp, ví dụ nếu hệ thống IT và/oặc OT không thể quay trở lại hoạt động bình thường, có thể cần thiết để bắt đầu kế hoạch khôi phục cùng với các kế hoạch dự phòng trên tàu. Trong trường hợp này, nhóm phản ứng có thể cung cấp lời khuyên cho tàu về:

- whether IT or OT systems should be shut down or kept running to protect data;
  Liệu các hệ thống IT hoặc OT có nên tắt hay tiếp tục chạy để bảo vệ dữ liệu;
- whether certain ship communication links with the shore should be shut down;

  Liệu một số liên kết thông tin liên lạc nào đó của tàu với bờ có nên bị đóng hay không;
- the appropriate use of any advanced tools provided in pre-installed security software;

  Việc sử dụng thích hợp bất kỳ công cụ tiên tiến nào được cung cấp trong phần mềm bảo mật được cài đặt sẵn;

- the extent to which the incident has compromised IT or OT systems beyond the capabilities of existing recovery plans.

  Mức độ mà sự cố đã làm tổn hại đến các hệ thống IT hoặc OT vượt quá khả năng của các kế hoạch phục hồi hiện có.

7.2 Recovery plan
Kế hoạch phục hồi

Recovery plans should be available in hard copy on board and ashore. The purpose of the plan is to support the recovery of systems and data necessary to restore IT and OT to an operational state. To ensure the safety of onboard personnel, the operation and navigation of the ship should be prioritised in the plan. The recovery plan should be understood by personnel responsible for cyber security. The detail and complexity of a recovery plan will depend on the type of ship and the IT, OT and other systems installed on board.

Kế hoạch phục hồi nên có sẵn trong bản cứng trên tàu và lên bờ. Mục đích của kế hoạch là hỗ trợ phục hồi các hệ thống và dữ liệu cần thiết để khôi phục IT và OT về trạng thái hoạt động. Để đảm bảo sự an toàn của người trên tàu, việc vận hành và hành hải của tàu phải được ưu tiên trong kế hoạch. Kế hoạch khôi phục nên được hiểu bởi nhân viên chịu trách nhiệm về an ninh mạng. Chi tiết và độ phức tạp của một kế hoạch phục hồi sẽ phụ thuộc vào loại tàu và IT, OT và các hệ thống khác được lắp đặt trên tàu.

As explained in section 5.1, a data recovery capability is a valuable technical protection measure. Data recovery capabilities are normally in the form of software backup for IT data. The availability of a software backup, either on board or ashore, should enable recovery of IT to an operational condition following a cyber incident.

Như đã giải thích trong phần 5.1, khả năng khôi phục dữ liệu là một biện pháp bảo vệ kỹ thuật có giá trị. Khả năng khôi phục dữ liệu thường ở dạng sao lưu phần mềm cho dữ liệu IT. Sự sẵn có của bản sao lưu phần mềm, hoặc trên tàu hoặc lên bờ, cho phép khôi phục IT về điều kiện hoạt động sau một sự cố mạng.

Recovery of OT may be more complex especially if there are no backup systems available and recovery may involve assistance from ashore. Details of where this assistance is available and by whom, should be part of the recovery plan, for example by proceeding to a port to obtain assistance from a service engineer.

Phục hồi OT có thể phức tạp hơn đặc biệt là nếu không có sẵn hệ thống sao lưu và phục hồi có thể liên quan đến sự hỗ trợ từ bờ. Thông tin chi tiết về nơi có hỗ trợ này và do ai thực hiện, nên là một phần của kế hoạch khôi phục, ví dụ bằng cách tiếp tục đến một cảng để nhận được sự hỗ trợ từ kỹ sư dịch vụ.

If qualified personnel are available on board, more extensive diagnostic and recovery actions may be performed. Otherwise, the recovery plan will be limited to obtaining quick access to technical support.

Nếu nhân viên đủ năng lực có sẵn trên tàu, các hành động chẩn đoán và phục hồi rộng hơn có thể được thực hiện. Nếu không, kế hoạch khôi phục sẽ bị giới hạn để có được sự truy cập nhanh đến các hỗ trợ kỹ thuật.

7.3 Investigating cyber incidents
Điều tra sự cố mạng

Investigating a cyber incident can provide valuable information about the way in which a vulnerability was exploited. Companies should, wherever possible, investigate cyber incidents affecting IT and OT on board in accordance with company procedures. A detailed investigation may require external expert support.

Điều tra sự cố mạng có thể cung cấp thông tin có giá trị về cách thức mà lỗ hổng đã được khai thác. Các công ty nên, bất cứ khi nào có thể, điều tra sự cố mạng ảnh hưởng đến IT và OT trên tàu theo quy trình của công ty. Điều tra chi tiết có thể yêu cầu hỗ trợ chuyên gia bên ngoài.

The information from an investigation can be used to improve the technical and procedural protection measures on board and ashore. It will also provide the wider maritime industry with a better understanding of maritime cyber risks. Any investigation should result in:

Thông tin từ cuộc điều tra có thể được sử dụng để cải thiện các biện pháp bảo vệ kỹ thuật và bằng quy trình trên tàu và trên bờ. Nó cũng sẽ cung cấp cho ngành công nghiệp hàng hải rộng lớn hơn với sự hiểu biết tốt hơn về các rủi ro mạng hàng hải. Bất kỳ điều tra nào cũng sẽ dẫn đến:

- a better understanding of the potential cyber risks facing the maritime industry both on board and ashore;

  Hiểu rõ hơn về các rủi ro mạng tiềm tàng đối với ngành hàng hải cả trên tàu và trên bờ;

- identification of lessons learned, including improvements in training to increase awareness;

  Xác định các bài học kinh nghiệm, bao gồm các cải tiến trong đào tạo để nâng cao nhận thức;

- updates to technical and procedural protection measures to prevent a recurrence.
  Cập nhật các biện pháp bảo vệ kỹ thuật và bằng quy trình để ngăn chặn sự tái diễn.

7.4 Losses arising from a cyber incident
Các tổn thất phát sinh từ sự cố mạng

For insurers, the term “cyber” includes many different aspects and it is important to distinguish between them and their effects on insurance cover. Also, it is important to note that according to the general understanding of insurers, there is no systemic risk to ships arising from a cyber incident and the impact of an incident is expected to be most likely confined to a single ship.

Đối với các nhà bảo hiểm, thuật ngữ “cyber” bao gồm nhiều khía cạnh khác nhau và điều quan trọng là phải phân biệt giữa chúng và ảnh hưởng của chúng đối với bảo hiểm. Ngoài ra, điều quan trọng cần lưu ý là theo sự hiểu biết chung của các nhà bảo hiểm, không có rủi ro hệ thống đối với các tàu phát sinh từ một sự cố mạng và tác động của một sự cố được cho là có khả năng bị giới hạn trong một con tàu duy nhất.

Companies will be aware that specific non-marine insurance cover may be available to cover data loss and the resulting fines and penalties resulting from equipment failure.

Các công ty sẽ nhận thức được rằng bảo hiểm phi hàng hải cụ thể có thể có sẵn để bù đắp cho việc mất dữ liệu, các khoản phạt liên quan và tiền phạt do hỏng thiết bị.

Companies should be able to demonstrate that they are acting with reasonable care in their approach to managing cyber risk and protecting the ship from any damage that may arise from a cyber incident.

Các công ty sẽ có thể chứng minh rằng họ đang hành động với sự chăm sóc hợp lý trong cách tiếp cận của họ để quản lý rủi ro mạng và bảo vệ con tàu khỏi bất kỳ thiệt hại nào có thể phát sinh do sự cố mạng.

Cover for property damage
Chi trả thiệt hại về tài sản

Generally, in many markets offering marine property insurance, the policy may cover loss or damage to the ship and its equipment caused by a shipping incident such as grounding, collision, fire or flood, even when the underlying cause of the incident is a cyber incident. It may be noted that currently in some markets exclusion clauses for cyber attacks exist. If the marine policy contains an exclusion clause for cyberattacks, the loss or damage will not be covered.

Nói chung, ở nhiều thị trường bảo hiểm tài sản hàng hải, chính sách có thể bao gồm tổn thất hoặc thiệt hại cho tàu và thiết bị do sự cố vận tải biển như mắc cạn, va chạm, hỏa hoạn hoặc ngập nước, ngay cả khi nguyên nhân cơ bản của vụ việc là sự cố mạng . Cần lưu ý rằng hiện tại trong một số thị trường loại trừ các điều khoản cho các cuộc tấn công mạng tồn tại. Nếu chính sách hàng hải có chứa một điều khoản loại trừ cho các cuộc tấn công mạng, sự mất mát hoặc thiệt hại sẽ không được chi trả.

Companies are recommended to check with their insurers / brokers in advance whether their policy covers claims caused by cyber incidents and/or by cyber attacks.

Khuyến nghị các công ty nên kiểm tra với công ty bảo hiểm/môi giới của họ trước liệu chính sách của họ có bao gồm các khiếu nại do sự cố mạng và/hoặc do các cuộc tấn công mạng hay không.

Guidelines for the market have been published, in which marine insurers are recommended to ask questions about company cyber security awareness and non-technical procedures. Companies should, therefore, expect a request for non-technical information regarding their approach to cyber security from insurers.

Hướng dẫn cho thị trường đã được công bố, trong đó các công ty bảo hiểm hàng hải được khuyến nghị đặt câu hỏi về nhận thức an ninh mạng của công ty và các quy trình phi kỹ thuật. Do đó, các công ty sẽ mong đợi một yêu cầu về thông tin phi kỹ thuật liên quan đến cách tiếp cận an ninh mạng của họ từ các công ty bảo hiểm.

The limited data on the frequency, severity of loss or probability of physical damage resulting from a cyber incident, represents a challenge and means that standard pricing is not available.

Các dữ liệu hạn chế về tần suất, mức độ nghiêm trọng của mất mát hoặc xác suất thiệt hại vật chất do sự cố mạng gây ra là một thách thức và có nghĩa là giá chuẩn không có sẵn.

Cover for liability
Chi trả cho trách nhiệm

It is recommended to contact the P&I Club for detailed information about cover provided to shipowners and charterers in respect of liability to third parties (and related expenses) arising from the operation of ships.

Khuyến nghị nên liên hệ với Bảo hiểm P&I để biết thông tin chi tiết về bảo hiểm được cung cấp cho chủ tàu và người thuê tàu về trách nhiệm đối với bên thứ ba (và các chi phí liên quan) phát sinh từ hoạt động của tàu.

An incident caused, for example by malfunction of a ship's navigation or mechanical systems because of a criminal act or accidental cyber attack, does not in itself give rise to any exclusion of normal P&I cover.

Một sự cố gây ra, ví dụ do sự cố của hệ thống hành hải của tàu hoặc hệ thống cơ khí do hành vi phạm tội hoặc tấn công mạng tình cờ, không gây ra bất kỳ sự loại trừ chi trả P&I thông thường nào.

It should be noted that many losses, which could arise from a cyber incident are not in the nature of third-party liabilities arising from the operation of the ship. For example, financial loss caused by ransomware, or costs of rebuilding scrambled data would not be identified in the coverage.

Cần lưu ý rằng nhiều tổn thất, có thể phát sinh từ một sự cố không mạng phải là bản chất của trách nhiệm của bên thứ ba phát sinh từ hoạt động của tàu. Ví dụ, tổn thất tài chính do phần mềm gián điệm gây ra, hoặc chi phí xây dựng lại dữ liệu bị xáo trộn sẽ không được xác định trong phạm vi bảo hiểm.

Normal cover, in respect of liabilities, is subject to a war risk exclusion and cyber incidents in the context of a war or terror risk, will not normally be covered.

Chi trả thông thường, đối với các trách nhiệm, phải chịu sự loại trừ rủi ro chiến tranh và các sự cố mạng trong bối cảnh chiến tranh hoặc rủi ro khủng bố, thông thường sẽ không được chi trả.

Annex 1. Target systems, equipment and technologies
Phụ lục 1. Hệ thống, thiết bị và công nghệ mục tiêu

This annex provides a summary of potentially vulnerable systems and data onboard ships to assist companies with assessing their cyber risk exposure. Vulnerable systems, equipment and technologies may include:

Phụ lục này cung cấp bản tóm tắt các hệ thống và dữ liệu có khả năng dễ bị tổn thương trên tàu để hỗ trợ các công ty đánh giá rủi ro xâm nhập mạng của họ. Các hệ thống, thiết bị và công nghệ dễ bị tổn thương có thể bao gồm:

Communication systems
Hệ thống thông tin liên lạc

- integrated communication systems;
  Các hệ thống thông tin liên lạc tích hợp;
- satellite communication equipment;
  Thiết bị thông tin liên lạc vệ tinh;
- Voice Over Internet Protocols (VOIP) equipment;
  Thiết bị Truyền giọng nói trên giao thức **IP** *(VOIP)*
- wireless networks (WLANs);
  Mạng không dây (WLAN);
- public address and general alarm systems.
  Thiết bị truyền thanh công cộng và hệ thống báo động chung.

Bridge systems
Hệ thống buồng lái

- integrated navigation system;
  Hệ thống hành hải tích hợp;
- positioning systems (GPS, etc.)
  Các hệ thống định vị (GPS, ...);
- Electronic Chart Display Information System (ECDIS);
  Hệ thống hiển thị hải đồ và thông tin điện tử (ECDIS);
- Dynamic Positioning (DP) systems;
  Hệ thống định vị động (DP);
- systems that interface with electronic navigation systems and propulsion/manoeuvring systems;

  Các hệ thống giao diện với hệ thống hành hải điện tử và hệ thống đẩy tàu/hệ thống lái tàu;
- Automatic Identification System (AIS);
  Hệ thống nhận dạng tự động (AIS);
- Global Maritime Distress and Safety System (GMDSS);
  Hệ thống thông tin an toàn và cứu nạn hàng hải toàn cầu (GMDSS);
- radar equipment;
  Thiết bị ra đa;

- Voyage Data Recorders (VDR);
  Thiết bị ghi dữ liệu hành trình (VDR);
- other monitoring and data collection systems.
  Các hệ thống giám sát và thu thập thông tin khác.

Propulsion and machinery management and power control systems
Hệ thống đẩy, quản lý máy móc và kiểm soát năng lượng

- engine governor;
  Bộ điều tốc động cơ;
- power management;
  Quản lý năng lượng;
- integrated control system;
  Hệ thống kiểm soát tích hợp;
- alarm system;
  Hệ thống báo động;
- emergency response system.
  Hệ thống ứng phó khẩn cấp.

Access control systems
Các hệ thống kiểm soát việc tiếp cận

- surveillance systems such as CCTV network;
  Hệ thống giám sát như mạng truyền hình mạch kín (CCTV);
- Bridge Navigational Watch Alarm System (BNWAS);
  Hệ thống báo động trực ca hành hải buồng lái (BNWAS);
- Shipboard Security Alarm Systems (SSAS);
  Hệ thống báo động an ninh tàu (SSAS);
- electronic "personnel-on-board" systems.
  Hệ thống "người trên tàu" điện tử.

Cargo management systems
Các hệ thống quản lý hàng

- Cargo Control Room (CCR) and its equipment;
  Buồng điều khiển hàng và thiết bị của buồng này;
- level indication system;
  Hệ thống chỉ báo mức chất lỏng;
- valve remote control system;
  Hệ thống điều khiển van từ xa;
- ballast water systems;
  Hệ thống nước dằn;
- water ingress alarm system.
  Hệ thống báo động nước xâm nhập.

Passenger servicing and management systems
Hệ thống quản lý và dịch vụ hành khách

- Property Management System (PMS);
  Hệ thống quản lý tài sản (PMS);
- electronic health records;
  Bản ghi sức khỏe điện tử;
- financial related systems;
  Hệ thống liên quan đến tài chính;
- ship passenger/seafarer boarding access systems;
  Hệ thống tiếp cận tàu của hành khách/thuyền bộ;
- infrastructure support systems like domain naming system (DNS) and user authentication/authorisation systems.

  Hệ thống hỗ trợ cơ sở hạ tầng như hệ thống đặt tên miền (DNS) và hệ thống xác thực/ủy quyền người dùng

Passenger-facing networks
Hệ thống dùng cho hành khách

- passenger Wi-Fi or LAN internet access;
  Truy cập internet Wi-Fi hoặc LAN của hành khách;
- guest entertainment systems;
  Hệ thống giải trí dành cho khách;
- passenger Wi-Fi or Local Area Network (LAN) internet access, for example where onboard personnel can connect their own devices;

  Truy cập internet Wi-Fi hoặc mạng cục bộ (LAN) cho hành khách, ví dụ như nhân viên trên tàu có thể kết nối thiết bị của riêng họ;
- guest entertainment systems.
  Hệ thống giải trí dành cho hành khách.

Core infrastructure systems
Hệ thống cơ sở hạ tầng cốt lõi

- security gateways;
  Cổng an ninh;
- routers;
  Bộ định tuyến;
- switches;
  Thiết bị chuyển mạch;
- firewalls;
  Tường lửa;
- Virtual Private Network(s) (VPN);
  Mạng riêng ảo (VPN);
- Virtual LAN(s) (VLAN);
  Mạng LAN ảo (VLAN);

- intrusion prevention systems;
  Hệ thống ngăn ngừa xâm nhập;
- security event logging systems.
  Hệ thống ghi sự kiện bảo mật.

Administrative and crew welfare systems
Hệ thống phúc lợi thuyền viên và hành chính

- administrative systems;
  Hệ thống hành chính;
- crew Wi-Fi or LAN internet access, for example where onboard personnel can connect their own devices.

  Truy cập Internet Wi-Fi hoặc mạng LAN của thuyền bộ, ví dụ nhân viên trên tàu có thể kết nối thiết bị của riêng họ.

Annex 2. Onboard networks
Phụ lục 2. Mạng trên tàu

A secure network depends on the IT/OT set up onboard the ship, and the effectiveness of the company policy based on the outcome of the risk assessment. Control of entry points and physical network control on an existing ship may be limited because cyber security had not been considered during the ship's construction. It is recommended that network layout and network control should be planned for all new buildings.

Một mạng lưới an toàn phụ thuộc vào IT/OT được thiết lập trên tàu và hiệu quả của chính sách công ty dựa trên kết quả đánh giá rủi ro. Kiểm soát các điểm vào và kiểm soát mạng vật lý trên tàu hiện có có thể bị giới hạn vì an ninh mạng không được xem xét trong quá trình đóng tàu. Khuyến nghị nên lập kế hoạch bố trí mạng và kiểm soát mạng cho tất cả các tàu đóng mới.

Direct communication between an uncontrolled and a controlled network should be prevented. Furthermore, several protection measures should be added:

Giao tiếp trực tiếp giữa một mạng không được kiểm soát và được kiểm soát nên được ngăn chặn. Hơn nữa, cần thêm một số biện pháp bảo vệ:

- implement network separation and/or traffic management;
  Thực hiện tách mạng và/hoặc quản lý lưu lượng;
- manage encryption protocols to ensure correct level of privacy and commercial communication;

  Quản lý các giao thức mã hóa để đảm bảo mức độ riêng tư và thông tin liên lạc thương mại chính xác;
- manage use of certificates to verify origin of digitally signed documents, software or services.

  Quản lý việc sử dụng chứng chỉ để xác minh nguồn gốc của các tài liệu, phần mềm hoặc dịch vụ được ký điện tử.

In general, only equipment or systems that need to communicate with each other over the network should be able to do so. The overriding principle should be that the networking of equipment or systems is determined by operational need.

Nói chung, chỉ những thiết bị hoặc hệ thống cần trao đổi thông tin với nhau qua mạng mới có thể làm như vậy. Nguyên tắc quan trọng (vượt quyền) phải là mạng của thiết bị hoặc hệ thống được xác định theo nhu cầu hoạt động.

Physical layout
Bố trí vật lý

The physical layout of the network should be carefully considered. It is important to consider the physical location of essential network devices, including servers, switches, firewalls and cabling. This will help restrict access and maintain the physical security of the network installation and control of entry points to the network.

Bố trí vật lý của mạng nên được xem xét cẩn thận. Điều quan trọng là phải xem xét vị trí vật lý của các thiết bị mạng cần thiết, bao gồm máy chủ, thiết bị chuyển mạch, tường lửa và cáp. Điều này sẽ giúp hạn chế quyền truy cập và duy trì tính bảo mật vật lý của việc cài đặt mạng và kiểm soát các điểm vào mạng.

Network management

Quản lý mạng

Any network design will need to include an infrastructure for administering and managing the network. This may include installing network management software on dedicated workstations and servers providing file sharing, email and other services to the network.

Bất kỳ thiết kế mạng nào cũng sẽ cần bao gồm cơ sở hạ tầng để quản trị và quản lý mạng. Điều này có thể bao gồm việc cài đặt phần mềm quản lý mạng trên các máy trạm và máy chủ chuyên dụng cung cấp chia sẻ tệp, email và các dịch vụ khác cho mạng.

Network segmentation

Phân đoạn mạng

Onboard networks should normally accommodate the following:

Các mạng trên tàu thông thường nên có:

1. necessary communication between OT equipment;
   Thông tin liên lạc cần thiết giữa các thiết bị OT;
2. configuration and monitoring of OT equipment;
   Cấu hình và giám sát các thiết bị OT;
3. onboard administrative and business tasks including email and sharing business related files or folders;
   Các nhiệm vụ quản trị và kinh doanh trên tàu bao gồm email và chia sẻ các tệp hoặc thư mục liên quan đến kinh doanh;
4. recreational internet access for crew and/or passengers.
   Truy cập internet giải trí cho thuyền bộ và/hoặc hành khách.

Effective network segmentation is a key aspect of "defence in depth". OT, IT and public networks should be separated or segmented by appropriate protection measures. The protection measures used may include, but are not limited to an appropriate combination of the following:

Phân đoạn mạng hiệu quả là một khía cạnh quan trọng của "bảo vệ theo chiều sâu". OT, IT và mạng công cộng nên được tách ra hoặc phân đoạn bằng các biện pháp bảo vệ thích hợp. Các biện pháp bảo vệ được sử dụng có thể bao gồm, nhưng không giới hạn đối với sự kết hợp thích hợpcủa các biện sau đây:

- a perimeter firewall between the onboard network and the internet;
  Tường lửa vành đai giữa mạng trên tàu và internet;
- network switches between each network segment;
  Chuyển mạch mạng giữa mỗi phân đoạn mạng;
- internal firewalls between each network segment;
  Tường lửa nội bộ giữa mỗi phân đoạn mạng;
- Virtual Local Area Networks (VLAN) to host separate segments.
  Mạng cục bộ ảo (VLAN) để lưu trữ các phân đoạn riêng biệt.

In addition, each segment should have its own range of Internet Protocol (IP) addresses. Network segmentation does not remove the need for systems within each segment to be configured with appropriate network access controls and software firewalls and malware detection.

Ngoài ra, mỗi phân đoạn phải có dải địa chỉ Giao thức Internet (IP) riêng. Phân đoạn mạng không loại bỏ sự cần thiết cho các hệ thống trong mỗi phân đoạn được cấu hình với các kiểm soát truy cập mạng thích hợp và tường lửa phần mềm và sự phát hiện phần mềm độc hại.

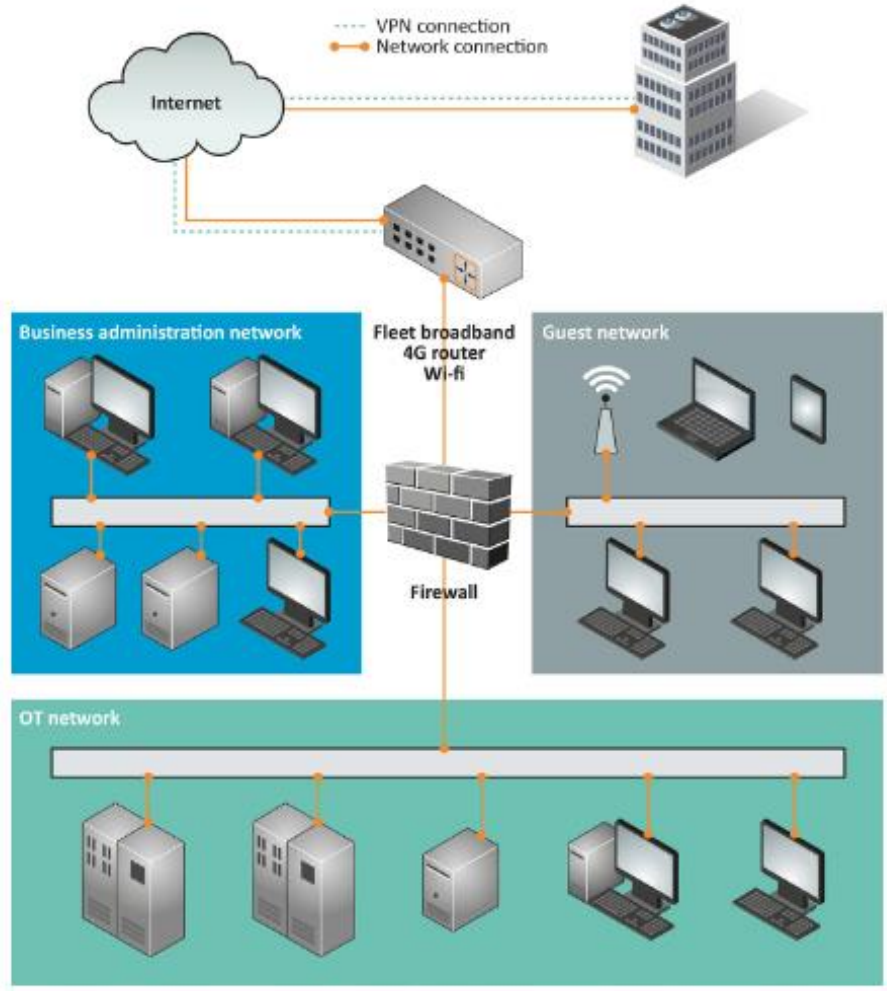

Figure 2. Example of an onboard network
Hình 2. Ví dụ về mạng trên tàu

In the example shown, the network has been segmented using a perimeter firewall, which supports three VLANs.

Trong ví dụ nêu trên, mạng đã được phân đoạn bằng tường lửa chu vi, hỗ trợ ba VLAN.

1. The OT Network containing equipment and systems, that performs safety critical functions;

   Mạng OT có chứa thiết bị và hệ thống, thực hiện các chức năng quan trọng về an toàn;

2. The IT network containing equipment and systems, that performs administrative or business functions;

   Mạng IT có trang thiết bị và hệ thống thực hiện chức năng quản trị hoặc kinh doanh;

3. A crew and guest network, providing uncontrolled internet access.
   Mạng cho thuyền bộ và khách cung cấp truy cập internet không kiểm soát được.

Considerations should be made on how to maximise the security of the switches themselves. To achieve the highest level of security, each network should use a different hardware switch.

This will minimise the chance of an attacker jumping between networks due to misconfiguration or by acquiring access to the configuration of a switch.

Cần cân nhắc về cách tối đa hóa mức độ an ninh của bản thân các thiết bị chuyển mạch. Để đạt được mức bảo mật cao nhất, mỗi mạng phải sử dụng một thiết bị chuyển mạch phần cứng khác nhau. Điều này sẽ giảm thiểu khả năng kẻ tấn công nhảy giữa các mạng do cấu hình sai hoặc bằng cách truy cập vào cấu hình của thiết bị chuyển mạch.

A correctly configured and appropriate firewall is an essential element of the proper segmentation of a network installation. The onboard installation should be protected by at least a perimeter firewall to control traffic between the internet and the onboard network. To prevent any unintended communication taking place, the firewall should be configured by default to deny all communication. Based on this configuration, rules should be implemented. The rules should be designed to allow passage of data traffic that is essential for the intended operation of that network.

Tường lửa được cấu hình đúng và thích hợp là một yếu tố thiết yếu của phân đoạn thích hợp của cài đặt mạng. Việc cài đặt trên tàu nên được bảo vệ bởi bởi ít nhất một tường lửa chu vi để kiểm soát lưu lượng giữa internet và mạng trên tàu. Để ngăn chặn bất kỳ giao tiếp không mong muốn nào xảy ra, tường lửa sẽ được cấu hình theo mặc định để từ chối tất cả các giao tiếp. Dựa trên cấu hình này, các quy tắc nên được thực hiện. Các quy tắc nên được thiết kế để cho phép thông qua lưu lượng dữ liệu cần thiết cho hoạt động dự định của mạng đó.

For example, if a specific endpoint receives updates from the internet, the rule should allow the specific endpoint to connect specifically to the server handling the specific update service. Enabling general internet access to a specified endpoint for updates is bad practice.

Ví dụ, nếu một thiết bị đầu cuối cụ thể nhận các bản cập nhật từ internet, quy tắc phải cho phép điểm cuối cụ thể kết nối cụ thể với máy chủ xử lý dịch vụ cập nhật cụ thể. Việc kích hoạt truy cập internet chung đến một điểm cuối được chỉ định để cập nhật là thực hành không tốt.

Uncontrolled networks like a crew or passenger network should not be allowed any communication with the controlled networks. The uncontrolled network should be considered as unsafe as the internet since the devices connecting to it are unmanaged, their security status (antivirus, updates, etc.) is unknown and their users could be acting maliciously, intentionally or unintentionally.

Các mạng không được kiểm soát như mạng dùng cho thuyền bộ hoặc hành khách không được phép liên lạc với các mạng được kiểm soát. Mạng không được kiểm soát nên được coi là không an toàn như internet vì các thiết bị kết nối với nó không được quản lý, trạng thái bảo mật (chống vi-rút, cập nhật, ...) không xác định và người dùng của họ có thể hoạt động độc hại, cố ý hoặc vô ý

Monitoring data activity

Theo dõi hoạt động dữ liệu

It is essential to monitor and manage systems to be aware of the networks' status and to detect any unauthorised data traffic. Logging should be implemented in the firewall and ideally in all network-attached devices so that in case of a breach, the responsible person can trace back the source and methodology of the attack. This will help to secure the network from any similar attacks in the future.

Điều quan trọng là phải theo dõi và quản lý hệ thống để biết trạng thái của mạng và phát hiện bất kỳ lưu lượng dữ liệu trái phép nào. Việc ghi nhật ký phải được thực hiện trong tường lửa và lý tưởng là trong tất cả các thiết bị liên kết mạng để trong trường hợp vi phạm, người chịu

trách nhiệm có thể truy nguyên nguồn và phương pháp tấn công. Điều này sẽ giúp bảo vệ mạng khỏi bất kỳ cuộc tấn công tương tự nào trong tương lai.

A network Intrusion Detection System (IDS) or Intrusion Protection System (IPS) can alert the system administrator in real-time of any attacks to the network systems. The IDS and IPS inspect data traffic, entry points or both to identify known threats or to reject traffic, which does not comply with the security policy. An IPS should comply with the latest industry best practices and guidelines.

Hệ thống phát hiện xâm nhập mạng (IDS) hoặc Hệ thống bảo vệ xâm nhập (IPS) có thể cảnh báo cho người quản trị hệ thống trong thời gian thực về bất kỳ cuộc tấn công nào vào hệ thống mạng. IDS và IPS kiểm tra lưu lượng dữ liệu, điểm vào hoặc cả hai để xác định các mối đe dọa đã biết hoặc từ chối lưu lượng truy cập không tuân thủ chính sách bảo mật. Một IPS phải tuân thủ các hướng dẫn và thực hành tốt công nghiệp mới nhất.

It is recommended to place a sensor on the internet-facing segment, because the public servers are a visible target to attackers. Another sensor should be placed behind the firewall, to monitor traffic between the internet and the internal network. An lDS/IPS sensor could also be placed by a remote-access segment, for instance a Virtual Private Network (VPN).

Khuyến nghị nên đặt cảm biến trên phân khúc hướng về internet (internet-facing) vì máy chủ công cộng là mục tiêu hiển thị đối với kẻ tấn công. Một cảm biến khác nên được đặt phía sau tường lửa, để giám sát lưu lượng giữa internet và mạng nội bộ. Một cảm biến lDS / IPS cũng có thể được đặt bởi một phân đoạn truy cập từ xa, ví dụ một mạng riêng ảo (VPN).

Secure running environment

Môi trường chạy an toàn.

Normally referred to as a sandbox, a secure running environment provides additional protection against cyber threats by isolating executable software from the underlying operating system. This prevents unauthorised access to the operating systems, on which the software is running. The sandbox enables software to be run under a specific set of rules and this adds control over processes and computer resources. Therefore, the sandbox prevents malicious, malfunctioning or untrusted software from affecting the rest of the system.

Thông thường được gọi là (hộ cát) sandbox, một môi trường chạy an toàn cung cấp sự bảo vệ bổ sung chống lại các mối đe dọa trên mạng bằng cách cô lập phần mềm thực thi từ hệ điều hành cơ bản. Điều này ngăn chặn truy cập trái phép vào hệ điều hành, trên đó phần mềm đang chạy. Hộp cát cho phép phần mềm được chạy theo một bộ quy tắc cụ thể và điều này bổ sung thêm quyền kiểm soát các quy trình và tài nguyên máy tính. Do đó, hộp cát ngăn chặn phần mềm độc hại, hỏng hóc hoặc không đáng tin cậy ảnh hưởng đến phần còn lại của hệ thống.

Annex 3. Glossary
Phụ lục 3. Bảng thuật ngữ

Access control is selective limiting of the ability and means to communicate with or otherwise interact with a system, to use system resources to handle information, to gain knowledge of the information the system contains or to control system components and functions.	***Kiểm soát truy cập*** *là hạn chế chọn lọc khả năng và phương tiện để giao tiếp với hoặc tương tác với hệ thống, sử dụng tài nguyên hệ thống để xử lý thông tin, thu thập kiến thức về thông tin hệ thống chứa hoặc kiểm soát các thành phần và chức năng của hệ thống.*
Back door is a secret method of bypassing normal authentication and verification when accessing a system. A back door is sometimes created by hidden parts of the system itself or established by separate software.	***Cửa sau*** *là phương pháp bí mật bỏ qua xác thực và xác minh thông thường khi truy cập hệ thống. Cửa sau đôi khi được tạo ra bởi các phần ẩn của hệ thống hoặc được thiết lập bằng phần mềm riêng biệt*
Bring your own device (BYOD) allows employees to bring personally owned devices (laptops, tablets, and smart phones) to the ship and to use those devices to access privileged information and applications for business use.	***Mang thiết bị của riêng bạn (BYOD)*** *cho phép nhân viên mang các thiết bị cá nhân (máy tính xách tay, máy tính bảng và điện thoại thông minh) tới tàu và sử dụng các thiết bị đó để truy cập thông tin và ứng dụng đặc quyền sử dụng cho kinh doanh.*
Cyber attack is any type of offensive manoeuvre that targets IT and OT systems, computer networks, and/or personal computer devices attempting to compromise, destroy or access company and ship systems and data.	***Tấn công mạng*** *là bất kỳ kiểu tấn công nào nhắm mục tiêu đến các hệ thống IT và OT, mạng máy tính và/hoặc thiết bị máy tính cá nhân cố gắng làm hại, phá hủy hoặc truy cập vào hệ thống và dữ liệu của công ty và tàu.*
Cyber incident is an occurrence, which actually or potentially results in adverse consequences to an onboard system, network and computer or the information that they process, store or transmit, and which may require a response action to mitigate the consequences.	***Sự cố mạng*** *là sự cố xảy ra hoặc có khả năng gây hậu quả bất lợi cho hệ thống, mạng và máy tính trên tàu hoặc thông tin mà chúng xử lý, lưu trữ hoặc truyền, và có thể yêu cầu hành động phản hồi để làm giảm thiểu hậu quả.*
Cyber risk management means the process of identifying, analysing, assessing, and communicating a cyber- related risk and accepting, avoiding, transferring, or mitigating it to an acceptable level; taking into consideration the costs and benefits of actions taken by stakeholders.	***Quản lý rủi ro mạng*** *có nghĩa là quá trình xác định, phân tích, đánh giá và thông ti về rủi ro liên quan đến mạng và chấp nhận, tránh, chuyển giao hoặc làm giảm thiểu đến mức độ chấp nhận được; lưu ý đến chi phí và lợi ích của các hành động mà các bên liên quan thực hiện.*
Cyber system is any combination of facilities, equipment, personnel, procedures and communications integrated to provide cyber services; examples include business systems, control systems and access control systems.	***Hệ thống mạng*** *sự kết hợp bất kỳ của các phương tiện, thiết bị, nhân sự, quy trình và truyền thông tích hợp để cung cấp các dịch vụ mạng; ví dụ bao gồm hệ thống kinh doanh, hệ thống kiểm soát và hệ thống kiểm soát truy cập*

Defence in breadth is a planned, systematic set of activities that seek to identify, manage, and reduce exploitable vulnerabilities in IT and OT systems, networks and equipment at every stage of the system, network, or sub-component life cycle. Onboard ships this approach will generally focus on network design, system integration, operations and maintenance.	***Bảo vệ theo chiều rộng*** *là một tập hợp các hoạt động có hệ thống nhằm tìm kiếm, xác định và giảm thiểu các lỗ hổng có thể khai thác trong các hệ thống, mạng và thiết bị IT và OT ở mọi giai đoạn của vòng đời hệ thống, mạng hoặc tiểu hợp phần. Trên tàu phương pháp này nói chung sẽ tập trung vào thiết kế mạng, tích hợp hệ thống, vận hành và bảo trì.*
Defence in depth is an approach which uses layers of independent technical and procedural protection measures to protect IT and OT on board.	***Bảo vệ theo chiều sâu*** *là cách tiếp cận sử dụng các lớp biện pháp bảo vệ kỹ thuật và bằng quy trình độc lập để bảo vệ IT và OT trên tàu.*
Executable software includes instructions for a computer to perform specified tasks according to encoded instructions.	***Phần mềm thực thi*** *bao gồm các hướng dẫn cho máy tính để thực hiện các tác vụ được chỉ định theo hướng dẫn được mã hóa.*
Firewall is a logical or physical break designed to prevent unauthorised access to IT infrastructure and information.	***Firewall*** *là một sự phá vỡ logic hoặc vật lý được thiết kế để ngăn chặn truy cập trái phép vào cơ sở hạ tầng và thông tin IT.*
Firmware is software imbedded in electronic devices that provides control, monitoring and data manipulation of engineered products and systems. They are normally self-contained and not accessible to user manipulation.	***Firmware*** *là phần mềm nhúng trong các thiết bị điện tử cung cấp điều khiển, giám sát và thao túng dữ liệu của các sản phẩm và hệ thống được thiết kế. Chúng thông thường tự khép kín và không thể tiếp cận thao túng người dùng.*
Flaw is unintended functionality in software.	***Lỗ hổng*** *là chức năng không mong muốn trong phần mềm.*
Intrusion Detection System (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station.	***Hệ thống phát hiện xâm phạm (IDS)*** *là một thiết bị hoặc ứng dụng phần mềm giám sát các hoạt động mạng hoặc hệ thống cho các hoạt động độc hại hoặc vi phạm chính sách và tạo báo cáo tới một trạm quản lý.*
Intrusion Prevention System (IPS), also known as Intrusion Detection and Prevention System (IDPS), are network security appliances that monitor network and/or system activities for malicious activity.	***Hệ thống phòng chống xâm nhập (IPS)****, còn được gọi là Hệ thống phát hiện và ngăn chặn xâm nhập (IDPS), là các thiết bị an ninh mạng giám sát các hoạt động mạng và/hoặc hệ thống đối với hoạt động độc hại.*
Local Area Network (LAN) is a computer network that interconnects computers within a limited area such as a home, ship or office building, using network media.	***Mạng cục bộ (LAN)*** *là mạng máy tính kết nối các máy tính trong một khu vực giới hạn như nhà, tàu hoặc tòa nhà văn phòng, sử dụng phương tiện mạng.*
Malware is a generic term for a variety of malicious software which can infect computer systems and impact on their performance.	***Phần mềm độc hại*** *là thuật ngữ chung cho nhiều phần mềm độc hại có thể lây nhiễm các hệ thống máy tính và tác động đến việc thực hiện chức năng của chúng.*

Operational technology (OT) includes devices, sensors, software and associated networking that monitor and control onboard systems.	***Công nghệ hoạt động (OT)*** *bao gồm các thiết bị, cảm biến, phần mềm và mạng liên quan theo dõi và kiểm soát các hệ thống trên tàu.*
Patches are software designed to update software or supporting data to improve the software or address security vulnerabilities and other bugs in operating systems or applications.	***Bản vá*** *là phần mềm được thiết kế để cập nhật phần mềm hoặc hỗ trợ dữ liệu để cải thiện phần mềm hoặc giải quyết lỗ hổng bảo mật và các lỗi khác trong hệ điều hành hoặc ứng dụng.*
Phishing refers to the process of deceiving recipients into sharing sensitive information with a third-party.	***Lừa đảo*** *đề cập đến quá trình lừa dối người nhận chia sẻ thông tin nhạy cảm với bên thứ ba.*
Principle of least privilege refers to the restriction of user account privileges only to those with privileges that are essential to perform its intended function.	***Nguyên tắc đặc quyền tối thiểu*** *đề cập đến việc hạn chế các đặc quyền tài khoản người dùng chỉ dành cho những người có đặc quyền cần thiết để thực hiện chức năng dự định của nó.*
Producer is the entity that manufactures the shipboard equipment and associated software.	***Nhà sản xuất*** *là thực thể sản xuất thiết bị của tàu và phần mềm liên quan.*
Recovery refers to the activities after an incident to restore essential services and operations in the short and medium term and fully restore all capabilities in the longer term.	***Phục hồi*** *đề cập đến các hoạt động sau một sự cố để khôi phục các dịch vụ và hoạt động thiết yếu trong ngắn hạn và trung hạn và khôi phục hoàn toàn tất cả các khả năng trong thời gian dài hơn.*
Removable media is a collective term for all methods of storing and transferring data between computers. This includes laptops, USB memory sticks, CDs, DVDs and diskettes.	***Phương tiệndi đông (phương tiện tháo lắp được)*** *là một thuật ngữ chung cho tất cả các phương thức lưu trữ và truyền dữ liệu giữa các máy tính. Điều này bao gồm máy tính xách tay, thẻ nhớ USB, đĩa CD, DVD và đĩa mềm.*
Risk assessment is the process which collects information and assigns values to risks for informing priorities, developing or comparing courses of action, and informing decision making.	***Đánh giá rủi ro*** *là quá trình thu thập thông tin và gán các giá trị cho các rủi ro để thông báo các ưu tiên, phát triển hoặc so sánh các loạt hành động và thông báo ra quyết định.*
Risk management is the process of identifying, analysing, assessing and communicating risk and accepting, avoiding, transferring or controlling it to an acceptable level considering associated costs and benefits of any actions taken.	***Quản lý rủi ro*** *là quá trình xác định, phân tích, đánh giá và thông tin rủi ro và chấp nhận, tránh, chuyển giao hoặc kiểm soát nó ở mức chấp nhận được, lưu ý đến chi phí liên quan và lợi ích của bất kỳ hành động nào được thực hiện.*
Sandbox is an isolated environment, in which a program may be executed without affecting the underlying system (computer or operating system) and any other applications. A sandbox is often used when executing untrusted software.	***Sandbox (hộp cát)*** *là một môi trường bị cô lập, trong đó một chương trình có thể được thực hiện mà không ảnh hưởng đến hệ thống bên dưới (máy tính hoặc hệ điều hành) và bất kỳ ứng dụng nào khác. Một sandbox thường được sử dụng khi thực thi phần mềm không tin cậy.*

Service provider is a company or person who provides and performs software maintenance.	***Nhà cung cấp dịch vụ*** *là công ty hoặc người cung cấp và thực hiện bảo trì phần mềm.*
Social engineering is a method used to gain access to systems by tricking a human into revealing confidential information.	***Kỹ thuật xã hội*** *là phương pháp được sử dụng để truy cập vào các hệ thống bằng cách lừa một người tiết lộ thông tin bí mật.*
Software whitelisting means specifying the software which may be present and active on an IT or OT system.	***Lập danh sách trắng phần mềm*** *có nghĩa là xác định phần mềm có thể có mặt và hoạt động trên hệ thống IT hoặc OT.*
Virtual Local Area Network (VLAN) is the logical grouping of network nodes. A virtual LAN allows geographically dispersed network nodes to communicate as if they were physically on the same network.	***Mạng cục bộ ảo (VLAN)*** *là nhóm các nút mạng hợp lý. Một mạng LAN ảo cho phép các nút mạng phân tán địa lý để giao tiếp như thể chúng nằm trên cùng một mạng.*
Virtual Private Network (VPN) enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network, thereby benefiting from the functionality, security and management policies of the private network.	***Mạng riêng ảo (VPN)*** *cho phép người dùng gửi và nhận dữ liệu trên các mạng chia sẻ hoặc công cộng như thể các thiết bị máy tính của họ được kết nối trực tiếp với mạng riêng, qua đó hưởng lợi từ các chính sách chức năng, bảo mật và quản lý của mạng riêng.*
Virus is a hidden, self-replicating section of computer software that maliciously infects and manipulates the operation of a computer program or system.	***Virus*** *là phần ẩn, tự sao chép của phần mềm máy tính độc hại lây nhiễm và thao túng hoạt động của chương trình hoặc hệ thống máy tính.*
Wi-Fi is all short-range communications that use some type of electromagnetic spectrum to send and/or receive information without wires.	***Wi-Fi*** *là tất cả các liên lạc tầm ngắn sử dụng một số loại phổ điện từ để gửi và/hoặc nhận thông tin mà không cần dây.*

Annex 4. Organisations and companies behind the guidelines
Phụ lục 4. Các tổ chức và công ty tham gia xây dựng Hướng dẫn này

The following organisations and companies have participated in the development of these guidelines:

Các tổ chức và công ty sau đây đã tham gia xây dựng hướng dẫn này

BIMCO

Chamber of Shipping of America (CSA)

Cobham SATCOM COLUMBIA Shipmanagement Ltd

Cruise Lines International Association (CLIA)

CyberKeel

Inmarsat

International Association of Dry Cargo Shipowners (INTERCARGO)

International Association of Independent Tanker Owners (INTERTANKO)

International Chamber of Shipping (ICS)

International Union of Maritime Insurance (IUMI)

Maersk Line

Naftomar Shipping and Trading

NCC Group

Oil Companies International Marine Forum (OCIMF)

SOFTimpact Ltd

Templar Executives

United States Maritime Resource Center (USMRC)

Wilhelmsen Group

Zodiac Maritime Ltd

INTERNATIONAL MARITIME ORGANIZATION
TỔ CHỨC HÀNG HẢI QUỐC TẾ

MSC-FAL.1/Circ.3
5 July 2017

GUIDELINES ON MARITIME CYBER RISK MANAGEMENT
HƯỚNG DẪN VỀ QUẢN LÝ RỦI RO MẠNG HÀNG HẢI

1 The Facilitation Committee, at its forty-first session (4 to 7 April 2017), and the Maritime Safety Committee, at its ninety-eighth session (7 to 16 June 2017), having considered the urgent need to raise awareness on cyber risk threats and vulnerabilities, approved the Guidelines on maritime cyber risk management, as set out in the annex.

1 Ủy ban Tạo điều kiện, tại phiên họp thứ bốn mươi lăm (ngày 04 - 07/4/2017) và Ủy ban An toàn hàng hải, tại phiên họp thứ chín mươi tám (từ ngày 07 - 16/6/2017), đã xem xét nhu cầu cấp thiết để nâng cao nhận thức về các mối đe dọa và lỗ hổng đối với an ninh mạng, đã phê chuẩn Hướng dẫn về quản lý rủi ro mạng hàng hải, như được nêu trong phụ lục.

2 The Guidelines provide high-level recommendations on maritime cyber risk management to safeguard shipping from current and emerging cyber threats and vulnerabilities. The Guidelines also include functional elements that support effective cyber risk management.

2 Hướng dẫn cung cấp các khuyến nghị cấp cao về quản lý rủi ro mạng hàng hải để bảo vệ vận tải biển khỏi các rủi ro và lỗ hổng hiện tại đang nổi lên. Hướng dẫn này cũng bao gồm các yếu tố chức năng hỗ trợ quản lý rủi ro mạng hiệu quả.

3 Member Governments are invited to bring the contents of this circular to the attention of all stakeholders concerned.

3 Đề nghị các Chính phủ thành viên phổ biến nội dung của thông tư này đến tất cả các bên liên quan.

4 This circular supersedes the interim guidelines contained in MSC.1/Circ.1526.

4 Thông tư này thay thế Hướng dẫn tạm thời nêu tại Thông tư MSC.1/Circ.1526.

ANNEX
PHỤ LỤC

GUIDELINES ON MARITIME CYBER RISK MANAGEMENT
HƯỚNG DẪN VỀ QUẢN LÝ RỦI RO MẠNG HÀNG HẢI

1 INTRODUCTION
GIỚI THIỆU

1.1 These Guidelines provide high-level recommendations for maritime cyber risk management. For the purpose of these Guidelines, maritime cyber risk refers to a measure of the extent to which a technology asset is threatened by a potential circumstance or event, which may result in shipping-related operational, safety or security failures as a consequence of information or systems being corrupted, lost or compromised.

1.1 Hướng dẫn này cung cấp các khuyến nghị cấp cao về quản lý rủi ro mạng hàng hải. Theo mục đích của Hướng dẫn này, rủi ro mạng hàng hải đề cập đến việc xác định mức độ tài sản công nghệ bị đe doạ bởi một tình huống hoặc sự kiện tiềm ẩn, có thể dẫn đến các lỗi vận hành, an toàn hoặc bảo mật liên quan đến vận tải biển do hậu quả của thông tin hoặc hệ thống bị hỏng, mất hoặc bị xâm phạm.

1.2 Stakeholders should take the necessary steps to safeguard shipping from current and emerging threats and vulnerabilities related to digitization, integration and automation of processes and systems in shipping.

1.2 Các bên liên quan nên thực hiện các bước cần thiết để bảo vệ vận tải biển khỏi các mối đe dọa hiện tại đang nổi lên và các lỗ hổng liên quan đến số hóa, tích hợp và tự động hóa các quy trình và hệ thống trong vận tải biển.

1.3 For details and guidance related to the development and implementation of specific risk management processes, users of these Guidelines should refer to specific Member Governments' and Flag Administrations' requirements, as well as relevant international and industry standards and best practices.

1.3 Để biết chi tiết và chỉ dẫn liên quan đến việc phát triển và thực hiện các quá trình quản lý rủi ro cụ thể, người sử dụng Hướng dẫn này nên tham khảo các yêu cầu của Chính phủ thành viên và Chính quyền hàng hải cụ thể, cũng như các tiêu chuẩn và thực hành tốt nhất của quốc tế và công nghiệp có liên quan.

1.4 Risk management is fundamental to safe and secure shipping operations. Risk management has traditionally been focused on operations in the physical domain, but greater reliance on digitization, integration, automation and network-based systems has created an increasing need for cyber risk management in the shipping industry.

1.4 Quản lý rủi ro là nền tảng cho các hoạt động vận tải biển an toàn và an ninh. Quản lý rủi ro theo truyền thống tập trung vào các hoạt động trong lĩnh vực vật lý, nhưng sự phụ thuộc lớn hơn vào số hóa, tích hợp, tự động hóa và các hệ thống dựa trên mạng đã tạo ra nhu cầu ngày càng tăng về quản lý rủi ro mạng trong ngành vận tải biển.

1.5 Predicated on the goal of supporting safe and secure shipping, which is operationally to cyber risks, these Guidelines provide recommendations that can be incorporated into existing risk management processes. In this regard, the Guidelines are complementary to the safety and security management practices established by this Organization.

1.5 Xác định mục tiêu là hỗ trợ ngành vận tải biển an toàn và an ninh, có khả năng thích ứng về hoạt động trước các rủi ro mạng, Hướng dẫn này đưa ra các khuyến nghị có thể được đưa vào các quá

trình quản lý rủi ro hiện có. Về vấn đề này, Hướng dẫn bổ sung cho các thực hành quản lý an toàn và an ninh do Tổ chức thiết lập.

2 GENERAL

TỔNG QUÁT

2.1 Background

Bối cảnh

2.1.1 Cybertechnologies have become essential to the operation and management of numerous systems critical to the safety and security of shipping and protection of the marine environment. In some cases, these systems are to comply with international standards and Flag Administration requirements. However, the vulnerabilities created by accessing, interconnecting or networking these systems can lead to cyber risks which should be addressed. Vulnerable systems could include, but are not limited to:

2.1.1 Công nghệ mạng đã trở thành cần thiết cho hoạt động và quản lý của nhiều hệ thống quan trọng đối với sự an toàn và an ninh của vận tải biển và bảo vệ môi trường biển. Trong một số trường hợp, các hệ thống này phải tuân thủ các tiêu chuẩn quốc tế và các yêu cầu về Chính quyền tàu mang cờ. Tuy nhiên, các lỗ hổng được tạo ra bằng cách truy cập, kết nối hoặc nối mạng các hệ thống này có thể dẫn đến các rủi ro mạng cần được giải quyết. Các hệ thống dễ bị tổn thương có thể bao gồm, nhưng không giới hạn đối với:

.1 Bridge systems;

Hệ thống buồng lái;

.2 Cargo handling and management systems;

Hệ thống quản lý và thao tác hàng hóa;

.3 Propulsion and machinery management and power control systems;

Quản lý thiết bị đẩy tàu, máy móc và hệ thống kiểm soát năng lượng;

.4 Access control systems;

Hệ thống kiểm soát việc tiếp cận tàu;

.5 Passenger servicing and management systems;

Hệ thống quản lý và phục vụ hành khách;

.6 Passenger facing public networks;

Mạng công cộng dành cho hành khách;

.7 Administrative and crew welfare systems; and

Hệ thống phúc lợi cho thuyền viên và hành chính; và

.8 Communication systems.

Hệ thống thông tin liên lạc.

2.1.2 The distinction between information technology and operational technology systems should be considered. Information technology systems may be thought of as focusing on the use of data as information. Operational technology systems may be thought of as focusing on the use of data to control or monitor physical processes. Furthermore, the protection of information and data exchange within these systems should also be considered.

2.1.2 Cần xem xét sự khác biệt giữa công nghệ thông tin và các hệ thống công nghệ hoạt động. Hệ thống công nghệ thông tin có thể được coi là tập trung vào việc sử dụng dữ liệu như thông tin. Các hệ thống công nghệ hoạt động có thể được coi là tập trung vào việc sử dụng dữ liệu để kiểm soát hoặc

theo dõi các quá trình vật lý. Hơn nữa, việc bảo vệ thông tin và trao đổi dữ liệu trong các hệ thống này cũng cần được xem xét.

2.1.3 While these technologies and systems provide significant efficiency gains for the maritime industry, they also present risks to critical systems and processes linked to the operation of systems integral to shipping. These risks may result from vulnerabilities arising from inadequate operation, integration, maintenance and design of cyber-related systems, and from intentional and unintentional cyberthreats.

2.1.3 Trong khi các công nghệ và hệ thống này mang lại hiệu quả đáng kể cho ngành hàng hải, chúng cũng gây rủi ro cho các hệ thống và quá trình quan trọng liên quan đến hoạt động của các hệ thống tích hợp trong vận tải biển. Những rủi ro này có thể là kết quả của các lỗ hổng phát sinh từ sự hoạt động, tích hợp, bảo trì và thiết kế các hệ thống liên quan đến mạng không đầy đủ, và từ các mối đe dọa chủ ý và không chủ ý.

2.1.4 Threats are presented by malicious actions (e.g. hacking or introduction of malware) or the unintended consequences of benign actions (e.g. software maintenance or user permissions). In general, these actions expose vulnerabilities (e.g. outdated software or ineffective firewalls) or exploit a vulnerability in operational or information technology. Effective cyber risk management should consider both kinds of threat.

2.1.4 Các mối đe dọa được biểu thị bởi các hành động nguy hiểm (ví dụ: sự xâm nhập hoặc giới thiệu phần mềm độc hại) hoặc hậu quả ngoài ý muốn của các hành động vô hại (ví dụ: bảo trì phần mềm hoặc quyền của người dùng). Nói chung, những hành động này phơi bày các lỗ hổng (ví dụ: phần mềm đã lỗi thời hoặc tường lửa không hiệu quả) hoặc khai thác lỗ hổng trong công nghệ hoạt động hoặc thông tin. Quản lý rủi ro mạng hiệu quả nên xem xét cả hai loại mối đe dọa.

2.1.5 Vulnerabilities can result from inadequacies in design, integration and/or maintenance of systems, as well as lapses in cyberdiscipline. In general, where vulnerabilities in operational and/or information technology are exposed or exploited, either directly (e.g. weak passwords leading to unauthorized access) or indirectly (e.g. the absence of network segregation), there can be implications for security and the confidentiality, integrity and availability of information. Additionally, when operational and/or information technology vulnerabilities are exposed or exploited, there can be implications for safety, particularly where critical systems (e.g. bridge navigation or main propulsion systems) are compromised.

2.1.5 Các lỗ hổng có thể là kết quả của những bất cập trong thiết kế, tích hợp và/hoặc bảo trì hệ thống, cũng như sai sót trong nguyên tắc mạng. Nói chung, nơi lỗ hổng trong hoạt động và/hoặc công nghệ thông tin bị phơi nhiễm hoặc khai thác, hoặc trực tiếp (ví dụ như mật khẩu yếu dẫn đến truy cập trái phép) hoặc gián tiếp (ví dụ như thiếu sự tách biệt mạng), có thể có liên quan đến an ninh và tính bảo mật, tính nguyên vẹn và tính khả dụng của thông tin. Ngoài ra, khi lỗ hổng công nghệ và/hoặc lỗ hổng công nghệ thông tin bị phơi nhiễm hoặc khai thác, có thể có liên quan đến an toàn, đặc biệt là khi các hệ thống quan trọng (ví dụ như hành hải buồng lái hoặc hệ thống đẩy chính) bị xâm nhập.

2.1.6 Effective cyber risk management should also consider safety and security impacts resulting from the exposure or exploitation of vulnerabilities in information technology systems. This could result from inappropriate connection to operational technology systems or from procedural lapses by operational personnel or third parties, which may compromise these systems (e.g. inappropriate use of removable media such as a memory stick).

2.1.6 Quản lý rủi ro mạng hiệu quả cũng nên xem xét các tác động an toàn và an ninh do phơi nhiễm hoặc khai thác các lỗ hổng trong các hệ thống công nghệ thông tin. Điều này có thể là do kết nối không phù hợp với các hệ thống công nghệ hoạt động hoặc từ các sai sót quy trình do nhân viên vận hành hoặc bên thứ ba, có thể làm tổn hại đến các hệ thống này (ví dụ: sử dụng không thích hợp phương tiện di động như thẻ nhớ).

2.1.7 Further information regarding vulnerabilities and threats can be found in the additional guidance and standards referenced in section 4.

2.1.7 Thông tin thêm về các lỗ hổng và mối đe dọa có thể được tìm thấy trong hướng dẫn và tiêu chuẩn bổ sung được tham chiếu trong phần 4.

2.1.8 These rapidly changing technologies and threats make it difficult to address these risks only through technical standards. As such, these Guidelines recommend a risk management approach to cyber risks that is resilient and evolves as a natural extension of existing safety and security management practices.

2.1.8 Những công nghệ và mối đe dọa thay đổi nhanh chóng này gây khó khăn cho việc giải quyết những rủi ro liên quan chỉ thông qua các tiêu chuẩn kỹ thuật. Như vậy, Hướng dẫn này khuyến nghị cách tiếp cận quản lý rủi ro đối với các rủi ro mạng có khả năng thích ứng và phát triển, như là một phần mở rộng tự nhiên của các thực tiễn quản lý an toàn và an ninh hiện có.

2.1.9 In considering potential sources of threats and vulnerabilities and associated risk mitigation strategies, a number of potential control options for cyber risk management should also be taken into consideration, including amongst others, management, operational or procedural, and technical controls.

2.1.9 Khi xem xét các nguồn tiềm năng của các mối đe dọa và lỗ hổng và chiến lược giảm thiểu rủi ro liên quan, một số tùy chọn kiểm soát tiềm năng cho quản lý rủi ro mạng cũng cần được xem xét, bao gồm, ngoài các biện pháp khác, quản lý, vận hành hoặc kiểm soát vận hành hoặc bằng quy trình và kiểm soát kỹ thuật.

2.2 Application

Ứng dụng

2.2.1 These Guidelines are primarily intended for all organizations in the shipping industry, and are designed to encourage safety and security management practices in the cyber domain.

2.2.1 Hướng dẫn này chủ yếu dành cho tất cả các tổ chức trong ngành vận tải biển và được thiết kế để khuyến khích các hoạt động quản lý an toàn và an ninh trong lĩnh vực mạng.

2.2.2 Recognizing that no two organizations in the shipping industry are the same, these Guidelines are expressed in broad terms in order to have a widespread application. Ships with limited cyber-related systems may find a simple application of these Guidelines to be sufficient; however, ships with complex cyber-related systems may require a greater level of care and should seek additional resources through reputable industry and Government partners.

2.2.2 Thừa nhận là không có hai tổ chức nào trong ngành vận tải biển giống nhau, Hướng dẫn này được thể hiện bằng các thuật ngữ rộng để có ứng dụng rộng rãi. Các tàu có hệ thống liên quan đến mạng hạn chế có thể thấy ứng dụng đơn giản của Hướng dẫn này là đủ; tuy nhiên, các tàu có hệ thống liên quan đến mạng phức tạp có thể yêu cầu mức độ chăm sóc cao hơn và nên tìm kiếm nguồn bổ sung thông qua các đối tác chính phủ và ngành công nghiệp có uy tín.

2.2.3 These Guidelines are recommendatory.

2.2.3 Hướng dẫn này là khuyến nghị.

3 ELEMENTS OF CYBER RISK MANAGEMENT

NGUYÊN TẮC QUẢN LÝ RỦI RO MẠNG

3.1 For the purpose of these Guidelines, cyber risk management means the process of identifying, analysing, assessing, and communicating a cyber-related risk and accepting, avoiding, transferring, or mitigating it to an acceptable level, considering costs and benefits of actions taken to stakeholders.

3.1 Theo mục đích của Hướng dẫn này, quản lý rủi ro mạng có nghĩa là quá trình xác định, phân tích, đánh giá và thông tin rủi ro liên quan đến mạng và chấp nhận, tránh, chuyển giao hoặc làm giảm thiểu đến mức độ chấp nhận được, xem xét chi phí và lợi ích của các hành động cho các bên liên quan.

3.2 The goal of maritime cyber risk management is to support safe and secure shipping, which is operationally resilient to cyber risks.

3.2 Mục tiêu của quản lý rủi ro mạng hàng hải là hỗ trợ vận tải biển an toàn và an ninh, có khả năng thích ứng về hoạt động trước các rủi ro mạng.

3.3 Effective cyber risk management should start at the senior management level. Senior management should embed a culture of cyber risk awareness into all levels of an organization and ensure a holistic and flexible cyber risk management regime that is in continuous operation and constantly evaluated through effective feedback mechanisms.

3.3 Quản lý rủi ro mạng hiệu quả nên bắt đầu ở cấp quản lý cấp cao. Quản lý cấp cao nên áp dụng văn hóa nhận thức về rủi ro mạng vào tất cả các cấp của tổ chức, đảm bảo chế độ quản lý rủi ro mạng linh hoạt, toàn diện đang hoạt động liên tục và được đánh giá liên tục thông qua các cơ chế phản hồi hiệu quả.

3.4 One accepted approach to achieve the above is to comprehensively assess and compare an organization's current, and desired, cyber risk management postures. Such a comparison may reveal gaps that can be addressed to achieve risk management objectives through a prioritized cyber risk management plan. This risk-based approach will enable an organization to best apply its resources in the most effective manner.

3.4 Một cách tiếp cận được chấp nhận để đạt được điều nói trên là đánh giá và so sánh toàn diện tình hình quản lý rủi ro mạng hiện tại và mong muốn của tổ chức. Sự so sánh như vậy có thể bộc lộ khoảng trống có thể được giải quyết để đạt được các mục tiêu quản lý rủi ro thông qua kế hoạch quản lý rủi ro mạng được ưu tiên. Cách tiếp cận dựa trên rủi ro này sẽ cho phép tổ chức áp dụng tốt nhất các nguồn lực của mình một cách hiệu quả nhất.

3.5 These Guidelines present the functional elements that support effective cyber risk management. These functional elements are not sequential - all should be concurrent and continuous in practice and should be incorporated appropriately in a risk management framework:

3.5 Hướng dẫn này trình bày các yếu tố chức năng hỗ trợ quản lý rủi ro mạng hiệu quả. Các yếu tố chức năng này không tuần tự - tất cả nên đồng thời và liên tục trong thực tế và cần được kết hợp một cách thích hợp trong một khung quản lý rủi ro:

.1 Identify: Define personnel roles and responsibilities for cyber risk management and identify the systems, assets, data and capabilities that, when disrupted, pose risks to ship operations.

Xác định: Xác định vai trò và trách nhiệm của nhân viên đối với việc quản lý rủi ro mạng và xác định các hệ thống, tài sản, dữ liệu và khả năng khi bị gián đoạn gây rủi ro cho hoạt động của tàu.

.2 Protect: Implement risk control processes and measures, and contingency planning to protect against a cyber-event and ensure continuity of shipping operations.

Bảo vệ: Thực hiện các quy trình và biện pháp kiểm soát rủi ro và lập kế hoạch dự phòng để bảo vệ chống lại sự kiện mạng và đảm bảo tính liên tục của các hoạt động vận tải biển.

.3 Detect: Develop and implement activities necessary to detect a cyber-event in a timely manner.

Phát hiện: Phát triển và thực hiện các hoạt động cần thiết để phát hiện sự kiện trên mạng một cách kịp thời.

.4 Respond: Develop and implement activities and plans to provide resilience and to restore systems necessary for shipping operations or services impaired due to a cyber-event.

Đáp trả: Phát triển và thực hiện các hoạt động và kế hoạch để cung cấp khả năng phục hồi và khôi phục các hệ thống cần thiết cho hoạt động vận tải biển hoặc dịch vụ bị suy yếu do sự kiện mạng.

.5 Recover: Identify measures to back-up and restore cyber systems necessary for shipping operations impacted by a cyber-event.

Khôi phục: Xác định các biện pháp sao lưu và khôi phục các hệ thống mạng cần thiết cho các hoạt động vận tải biển bị ảnh hưởng bởi sự kiện mạng.

3.6 These functional elements encompass the activities and desired outcomes of effective cyber risk management across critical systems affecting maritime operations and information exchange, and constitute an ongoing process with effective feedback mechanisms.

3.6 Các yếu tố chức năng này bao gồm các hoạt động và kết quả mong muốn của quản lý rủi ro mạng hiệu quả trên các hệ thống quan trọng ảnh hưởng đến hoạt động hàng hải và trao đổi thông tin, và tạo thành một quá trình liên tục với các cơ chế phản hồi hiệu quả.

3.7 Effective cyber risk management should ensure an appropriate level of awareness of cyber risks at all levels of an organization. The level of awareness and preparedness should be appropriate to roles and responsibilities in the cyber risk management system.

3.7 Quản lý rủi ro mạng hiệu quả phải đảm bảo mức độ nhận thức phù hợp về rủi ro mạng ở tất cả các cấp của tổ chức. Mức độ nhận thức và sự chuẩn bị cần phù hợp với vai trò và trách nhiệm trong hệ thống quản lý rủi ro mạng.

4 BEST PRACTICES FOR IMPLEMENTATION OF CYBER RISK MANAGEMENT

4.1 The approach to cyber risk management described herein provides a foundation for better understanding and managing cyber risks, thus enabling a risk management approach to address cyber threats and vulnerabilities. For detailed guidance on cyber risk management, users of these Guidelines should also refer to Member Governments' and Flag Administrations' requirements, as well as relevant international and industry standards and best practices.

4.1 Cách tiếp cận quản lý rủi ro mạng được mô tả ở đây cung cấp nền tảng để hiểu và quản lý rủi ro mạng tốt hơn, tạo điều kiện tiếp cận quản lý rủi ro để giải quyết các mối đe doạ và lỗ hổng mạng. Để có các chỉ dẫn chi tiết về quản lý rủi ro mạng, người dùng Hướng dẫn này cũng nên tham khảo các yêu cầu của Chính phủ thành viên và Chính quyền quốc gia tàu mang cờ, cũng như các tiêu chuẩn quốc tế và công nghiệp có liên quan, và thực hành tốt nhất.

4.2 Additional guidance and standards may include, but are not limited to:[1]

4.2 Các chỉ dẫn và tiêu chuẩn bổ sung có thể bao gồm, nhưng không giới hạn:[1]

.1 The Guidelines on Cyber Security Onboard Ships produced and supported by BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, OCIMF and IUMI.

Hướng dẫn về an ninh mạng trên tàu được xây dựng và hỗ trợ bởi BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, OCIMF và IUMI.

---

[1] The additional guidance and standards are listed as a non-exhaustive reference to further detailed information for users of these Guidelines. The referenced guidance and standards have not been issued by the Organization and their use remains at the discretion of individual users of these Guidelines.

Chỉ dẫn và tiêu chuẩn bổ sung được liệt kê dưới dạng tham chiếu không đầy đủ để cung cấp thêm thông tin chi tiết cho người dùng các Hướng này. Chỉ dẫn và tiêu chuẩn được tham chiếu chưa được Tổ chức ban hành và việc sử dụng chúng vẫn theo quyết định của cá nhân người dùng trong Hướng này.

.2 ISO/IEC 27001 standard on Information technology – Security techniques – Information security management systems – Requirements. Published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

.2 Tiêu chuẩn ISO/ IEC 27001 về Công nghệ thông tin - Kỹ thuật bảo mật - Hệ thống quản lý bảo mật thông tin - Yêu cầu. Được công bố chung bởi Tổ chức Tiêu chuẩn hóa quốc tế (ISO) và Ủy ban Kỹ thuật Điện quốc tế (IEC).

.3 United States National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity (the NIST Framework).

.3 Khuôn khổ của Viện Tiêu chuẩn và Công nghệ quốc gia Hoa Kỳ về cải thiện cơ sở hạ tầng quan trọng an ninh mạng (Khuôn khổ NIST).

4.3 Reference should be made to the most current version of any guidance or standards utilized.

4.3 Tham khảo nên theo phiên bản mới nhất của bất kỳ chỉ dẫn hoặc tiêu chuẩn nào được sử dụng.

INTERNATIONAL MARITIME ORGANIZATION
TỔ CHỨC HÀNG HẢI QUỐC TẾ

RESOLUTION MSC.428(98)
NGHỊ QUYẾT MSC.428(98)

(adopted on 16 June 2017)
(Thông qua ngày 16/6/2017)

MARITIME CYBER RISK MANAGEMENT IN SAFETY MANAGEMENT SYSTEMS
QUẢN LÝ RỦI RO MẠNG HÀNG HẢI TRONG HỆ THỐNG QUẢN LÝ AN TOÀN

THE MARITIME SAFETY COMMITTEE,
ỦY BAN AN TOÀN HÀNG HẢI,

RECOGNIZING the urgent need to raise awareness on cyber risk threats and vulnerabilities to support safe and secure shipping, which is operationally resilient to cyber risks,

GHI NHẬN nhu cầu cấp thiết để nâng cao nhận thức về các mối đe dọa và lỗ hổng rủi ro mạng để hỗ trợ vận tải biển an toàn và an ninh, có khả năng thích ứng về hoạt động với rủi ro mạng,

RECOGNIZING ALSO that Administrations, classification societies, shipowners and ship operators, ship agents, equipment manufacturers, service providers, ports and port facilities, and all other maritime industry stakeholders should expedite work towards safeguarding shipping from current and emerging cyber threats and vulnerabilities,

THỪA NHẬN RẰNG rằng Chính quyền, tổ chức đăng kiểm, chủ tàu và người khai thác tàu, đại lý tàu, nhà sản xuất thiết bị, nhà cung cấp dịch vụ, cảng và bến cảng, và tất cả các bên liên quan khác trong ngành hàng hải cần tiến hành công việc để bảo vệ vận tải biển từ các mối đe dọa và lỗ hổng mạng hiện tại đang nổi lên,

BEARING IN MIND MSC-FAL.1/Circ.3 on *Guidelines on maritime cyber risk management* approved by the Facilitation Committee, at its forty-first session (4 to 7 April 2017), and by the Maritime Safety Committee, at its ninety-eighth session (7 to 16 June 2017), which provides high-level recommendations for maritime cyber risk management that can be incorporated into existing risk management processes and are complementary to the safety and security management practices established by this Organization,

LƯU Ý THÔNG TƯ MSC-FAL.1/Circ.3 về Hướng dẫn quản lý rủi ro mạng hàng hải được Ủy ban Tạo điều kiện phê duyệt tại phiên họp bốn mươi mốt (từ ngày 4 đến ngày 07/4/2017) và được Ủy ban An toàn hàng hải phê duyệt tại phiên họp chín mươi tám (từ ngày 7 đến ngày 16/06/2017), cung cấp các khuyến nghị cấp cao về quản lý rủi ro mạng hàng hải có thể được đưa vào các quá trình quản lý rủi ro hiện có và bổ sung cho các thực hành quản lý an toàn và an ninh do Tổ chức này thiết lập,

RECALLING resolution A.741(18) by which the Assembly adopted the International Management Code for the Safe Operation of Ships and for Pollution Prevention (International Safety Management (ISM) Code) and recognized, inter alia, the need for appropriate organization of management to enable it to respond to the need of those on board ships to achieve and maintain high standards of safety and environmental protection,

NHẮC LẠI nghị quyết A.741(18) mà Hội đồng đã thông qua Bộ luật quản lý quốc tế về hoạt động an toàn của tàu và phòng ngừa ô nhiễm (Bộ luật quản lý an toàn quốc tế (ISM)) và thừa nhận, ngoài các nội dung khác, sự cần thiết đối với việc tổ chức quản lý phù hợp để cho phép đáp ứng nhu cầu của những người trên tàu nhằm đạt được và duy trì các tiêu chuẩn cao về an toàn và bảo vệ môi trường,

NOTING the objectives of the ISM Code which include, inter alia, the provision of safe practices in ship operation and a safe working environment, the assessment of all identified risks to ships, personnel and the environment, the establishment of appropriate safeguards, and the continuous improvement of safety management skills of personnel ashore and aboard ships,

LƯU Ý các mục tiêu của Bộ luật ISM bao gồm, ngoài các nội dung khác, các quy định về thực hành an toàn trong hoạt động tàu và môi trường làm việc an toàn, việc đánh giá tất cả các rủi ro được xác định đối với tàu, con người và môi trường, việc thiết lập các biện pháp bảo vệ phù hợp và cải thiện liên tục kỹ năng quản lý an toàn của người trên bờ và trên tàu,

1 AFFIRMS that an approved safety management system should take into account cyber risk management in accordance with the objectives and functional requirements of the ISM Code;

1 KHẲNG ĐỊNH một hệ thống quản lý an toàn được phê duyệt cần lưu ý đến việc quản lý rủi ro mạng phù hợp với các mục tiêu và yêu cầu chức năng của Bộ luật ISM;

2 ENCOURAGES 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 1 January 2021;

2. KHUYẾN KHÍCH các Chính quyền hàng hải đảm bảo rằng các rủi ro mạng được đề cập một cách thích hợp trong các hệ thống quản lý an toàn không muộn hơn đợt thẩm tra hàng năm đầu tiên của Giấy chứng nhận phù hợp (DOC) của công ty sau ngày 01/01/2021;

3 ACKNOWLEDGES the necessary precautions that could be needed to preserve the confidentiality of certain aspects of cyber risk management;

3 THỪA NHẬN các biện pháp phòng ngừa cần thiết có thể cần để bảo vệ tính bảo mật của một số khía cạnh nhất định trong quản lý rủi ro mạng;

4 REQUESTS Member States to bring this resolution to the attention of all stakeholders.

4 YÊU CẦU Các Quốc gia thành viên phổ biến nghị quyết này đến tất cả các bên liên quan.

***