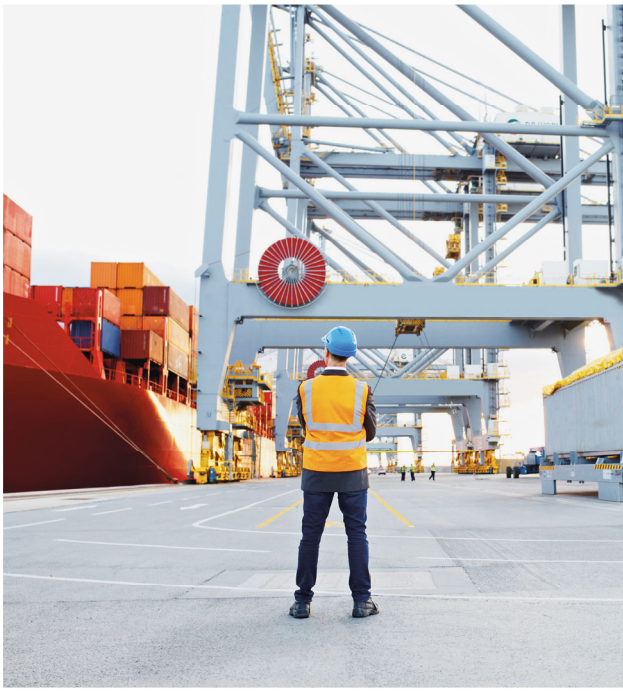
The Institution of Engineering and Technology

Good Practice Guide

Cyber Security for Ports and Port Systems



Department for Transport

[dstl]

Publication information

Authors: Hugh Boyes, Roy Isbell and Alexandra Luck

The IET would like to acknowledge the help and support of the Department for Transport (DfT), the Defence Science and Technology Laboratory (Dstl) and the National Cyber Security Centre (NCSC) in producing this document. The IET would also like to acknowledge the help and support of the ports visited during the preparation of this document.

Published by: Institution of Engineering and Technology, London, United Kingdom

The Institution of Engineering and Technology is registered as a Charity in England & Wales (no. 211014) and Scotland (no. SC038698).

© The Institution of Engineering and Technology

First published in 2016 as:
Code of Practice Cyber Security for Ports and Port Systems
Revised publication in 2020 as:
Good Practice Guide Cyber Security for Ports and Port Systems

This publication is copyright under the Berne Convention and the Universal Copyright Convention. All rights reserved. Apart from any fair dealing for the purposes of research or private study, or criticism or review, as permitted under the Copyright, Designs and Patents Act 1988, this publication may be reproduced, stored or transmitted, in any form or by any means, only with the prior permission in writing of the publishers, or in the case of reprographic reproduction in accordance with the terms of licences issued by the Copyright Licensing Agency. Enquiries concerning reproduction outside those terms should be sent to the publisher at this address:

The Institution of Engineering and Technology
Michael Faraday House
Six Hills Way, Stevenage
Herts, SG1 2AY, United Kingdom
www.theiet.org

While the publisher, authors and contributors believe that the information and guidance given in this work is correct, all parties must rely upon their own skill and judgement when making use of it. Neither the publisher, nor the author, nor any contributors assume any liability to anyone for any loss or damage caused by any error or omission in the work, whether such error or omission is the result of negligence or any other cause. Any and all such liability is disclaimed.

The moral rights of the authors to be identified as authors of this work have been asserted by the authors in accordance with the Copyright, Designs and Patents Act 1988.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application. Compliance with the contents of this document cannot confer immunity from legal obligations.

It is the constant aim of the IET to improve the quality of our products and services. We should be grateful if anyone finding an inaccuracy or ambiguity while using this document would inform the IET Standards development team: ietstandardsenquiries@theiet.org The IET, Six Hills Way, Stevenage SG1 2AY, UK.

Typeset in the UK by the Institution of Engineering and Technology, Stevenage
Printed in the UK by Elanders, Newcastle Upon Tyne

CONTENTS

List of Figures **5**

Foreword **7**

1 Introduction **9**

1.1 Who should use this Good Practice Guide? 10

1.2 Maritime Security Regulations in the UK 10

1.3 Terms and definitions 10

2 Cyber security **11**

2.1 What is cyber security? 11

2.2 What are the motivations behind a cyber-attack? 12

2.3 Environmental threats to port infrastructure 13

3 Cyber security in ports **15**

3.1 Why is cyber security important to ports? 15

3.2 Cyber security standards, guidance and good practice 15

4 Developing a Cyber Security Assessment (CSA) **17**

5 Developing a Cyber Security Plan (CSP) **19**

5.1 Review of the CSP 20

5.2 Monitoring and auditing of the CSP 20

6 Managing cyber security **21**

6.1 Role of the CySO 21

6.2 Port Security Committee (PSC) 22

6.3 Security Operations Centre (SOC) 22

6.4 Provision of information to third parties 23

6.5 Handling security breaches and incidents 23

7 Terms and definitions **25**

7.1 Terms 25

7.2 Acronyms 27

Appendix A Understanding cyber security **29**

A.1 Cyber security attributes 29

A.2 Threat actor groups 30

A.3 Port assets and cyber security 32

Appendix B Process for developing a Cyber Security Assessment (CSA) **37**

B.1 Identification and evaluation of important cyber assets and infrastructure 37

B.2 Identification of the port business processes 38

B.3 Identification and assessment of risks arising from potential threats and vulnerabilities 39

B.4 Identification, assessment, selection and prioritisation of countermeasures 40

© The Institution of Engineering and Technology

CONTENTS

B.5 Review acceptability of residual risk 40
B.6 Review of the Cyber Security Assessment (CSA) 40
B.7 Model port cyber security assessment 41

Appendix C Contents of a Cyber Security Plan (CSP) 47

Appendix D Identifying and implementing mitigation measures 55
D.1 People 55
D.2 Physical 56
D.3 Technological 57
D.4 Resilience 59

Appendix E Model terms of reference for a Port Security Committee (PSC) or Port Security Authority (PSA) 61

Appendix F Handling release of information to third parties 63

Appendix G Handling security breaches and incidents 65

Appendix H Bibliography 67
H.1 General IT and cyber security standards 67
H.2 Security and safety of Industrial Control Systems (ICA & SCADA) 68
H.3 Business-related security guidance 69
H.4 Other standards and guidance 69

© The Institution of Engineering and Technology

LIST OF FIGURES

Figure 2.1	Cyber security attributes
Figure 2.2	Cyber security threat actors
Figure 3.1	Port assets affected by cyber security
Figure 4.1	Overview of CSA process
Figure 5.1	Relationship of CSP to other documents
Figure 6.1	Key functions of a SOC
Figure B.1	Example of components supporting access control process, courtesy of BSI

© The Institution of Engineering and Technology

© The Institution of Engineering and Technology

FOREWORD

Cyber-attacks on port systems are no longer considered hypothetical or simply the stuff of fictional narrative.

In June 2017 the Maersk shipping company was hit by a cyber-attack from the purely destructive NotPetya virus. The virus entered Maersk's systems through a widely used piece of tax accounting software in Ukraine. Maersk was not the intended target for the attack, but the consequences for the company were very real. The virus spread through the company globally and made all their applications and data unavailable for several days. Real world operations – including its Rotterdam terminal – were seriously affected, with losses in the region of $200-300million.

NotPetya could attack the Maersk global network because it was loaded onto one unpatched computer operating in a single local office – connected to the global network. The incident shows the vulnerability of everyone to cyber-attacks: you do not even have to be the intended victim. Maersk could recover relatively quickly because it recognised that resilience and recovery processes are as important as trying to prevent an attack. Being able to recover all your systems and data from secure backups within hours of an attack will protect your business from potentially serious financial and reputational damage.

In other cyber security incidents, port assets have been infected with malware and there has been unintentional jamming or interference with wireless networks. Here are some things to consider:

Do you own, operate or occupy a port or port facility that has electronic or computer-based systems?

If the port systems were to fail, malfunction or were misused, would this result in economic, operational, physical or reputational loss or damage, or disrupt operations?

Do you own an information asset that includes information about your strategy or commercial operations, either the construction or the operation of your port or port facility, including any port systems?

If this information asset were compromised, could this result in economic, operational, physical or reputational loss or damage?

If your answer to any of the above questions is 'yes', then this Good Practice Guide (originally published in 2016 as *Code of Practice Cyber Security for Ports and Port Systems)* is essential reading. It will help you determine who in your organisation needs to take action.

Cyber security is not just about preventing hackers gaining access to systems and information. It also addresses the maintenance, integrity, confidentiality and availability of information and systems, ensuring business continuity and the continuing utility of cyber assets. We need to consider how to protect systems from physical attack, force majeure events, etc. when designing port systems or when supporting operational processes. Personnel security aspects are also important, as the insider threat from staff or contractors who decide to behave in a careless or malicious way cannot be ignored.

© The Institution of Engineering and Technology

Failure to address security risks could lead to serious injury or fatality, disruption or damage to port systems, loss of use of buildings, impact upon business operations, reputational damage, loss of revenue, financial penalties or litigation. Port owners, operators and port facility occupiers need to understand cyber security and promote awareness of this subject to their stakeholders. This should include provision of appropriate briefings to the design, construction and operations teams, and their supporting supply chains.

Port facilities are becoming increasingly complex and dependent on the extensive use of information and communications technologies (ICT) at all stages of their lifecycles – for example, in the growth of automated berthing operations. Some of this technology is embedded in the fixed and mobile assets used to operate the port; other elements may be remotely located, such as the systems used to schedule vessel and cargo movements. This Good Practice Guide explains why it is essential that cyber security be considered as part of a holistic approach throughout an asset's lifecycle, as well as setting out the potential financial, reputational and safety consequences that may arise if threats are ignored.

It is intended that this Good Practice Guide be used as an integral part of an organisation's overall risk management system and subsequent business planning, to ensure that the cyber security of port systems is managed cost-effectively, as part of mainstream business.

© The Institution of Engineering and Technology

SECTION 1

Introduction

This Good Practice Guide is a revision of an earlier code of practice on cyber security, published by the Department for Transport (DfT) in 2016. The guidance was developed following visits to several UK ports by the authors and personnel from the Defence Science and Technology Laboratory (Dstl). Since this Guide was originally published in 2016, the Network and Information Systems Directive (the NIS Directive) has been implemented in the transport sector, following the coming into force of the UK implementing legislation (the NIS Regulations) on 10th May 2018.

Some UK ports and port facilities are designated part of the Critical National Infrastructure and these will receive further advice on the implementation of mandatory requirements of the NIS Directive from the DfT and the National Cyber Security Centre (NCSC).

Whilst not a mandatory requirement for other ports, the aim should be to integrate cyber security into the overall security planning for a port or port-based facility. This revised guidance also includes an update about the scope of the NIS Directive (see Clause 3.2).

This Guide considers the cyber security requirement at both ports and port facilities, advocating a coherent, port-wide based approach. It is intended to complement the port security standards and their respective requirements by providing additional guidance on the cyber-related aspects of the security measures set out. It therefore makes extensive reference to, and assumes knowledge of, the definitions and concepts contained within those requirements.

This Good Practice Guide uses principles, rather than national legislation or specific standards, to help promote good practice. The specific cyber security measures implemented should depend upon the profile of the port and its facilities, its use and the nature of the cargos handled.

The rapid evolution in the use of, and reliance upon, information and communication technologies (ICT), as well as the advances in automation and the potential for integration of multiple electronic systems supporting management functions and business applications, increases the importance of addressing inherent vulnerabilities. It is vital that port operators understand and implement appropriate and proportionate measures to address the resilience and cyber security issues that arise. Only by doing so can they fully meet their responsibilities for the secure operation of their facilities.

While this Good Practice Guide is concerned solely with the cyber security of ports and port systems, it recognises that, with a large proportion of security breaches caused by people and poor processes, it is essential that personnel, process and physical aspects directly related to these technological systems are also considered and appropriate measures put in place. Recommendations relating to these aspects are therefore detailed throughout this Good Practice Guide, where relevant.

Except for any ship-to-shore interface, it is not the purpose of this Good Practice Guide to consider the cyber security of the ships to which the International Ship and Port Facility Security (ISPS) Code applies.

© The Institution of Engineering and Technology

1.1 Who should use this Good Practice Guide?

This Good Practice Guide is intended for use by those with responsibility for protecting the port/port facility, ships (when docked or berthed), persons, cargo, cargo transport units and ships' stores within the port from the risks of a security incident. It will also be of interest and relevance to those individuals involved in:

(a) the financial and operational management of the port or port facility;
(b) contractual arrangements with third parties;
(c) determining policies relating to acceptable staff behaviour;
(d) the specification, design, construction and maintenance of ports;
(e) the specification, design, development, integration, commissioning, operation and maintenance of port systems, including associated software and technologies; and
(f) management of specific security tasks, including incident response and the handling of security breaches.

1.2 Maritime Security Regulations in the UK

In December 2002 the International Maritime Organisation (IMO) adopted a new international instrument called the International Ship and Port Facility Security (ISPS) Code, which was incorporated by the European Commission (EC) into EC Regulation 725/2004 and brought into UK law under The Ship and Port Facility (Security) Regulations 2004. In July 2017 the IMO approved Guidelines on maritime cyber risk management (MSC-FAL.1/Circ.3) to provide high-level recommendations on maritime cyber risk management, to safeguard shipping from current and emerging cyber threats and vulnerabilities.

For convenience, the ISPS Code, EC Regulation and the EC Directive, along with maritime security regulatory material published by the UK Department for Transport (DfT), are collectively referred to in this Good Practice Guide as the 'port security standards'.

1.3 Terms and definitions

Definitions used in this Good Practice Guide are, to the extent that is practicable, in keeping with those contained in the International Convention for the Safety of Life at Sea (SOLAS), 1974, as amended. For ease of reference, certain terms used in this Good Practice Guide are defined in Section 7.

© The Institution of Engineering and Technology

SECTION 2

Cyber security

2.1 What is cyber security?

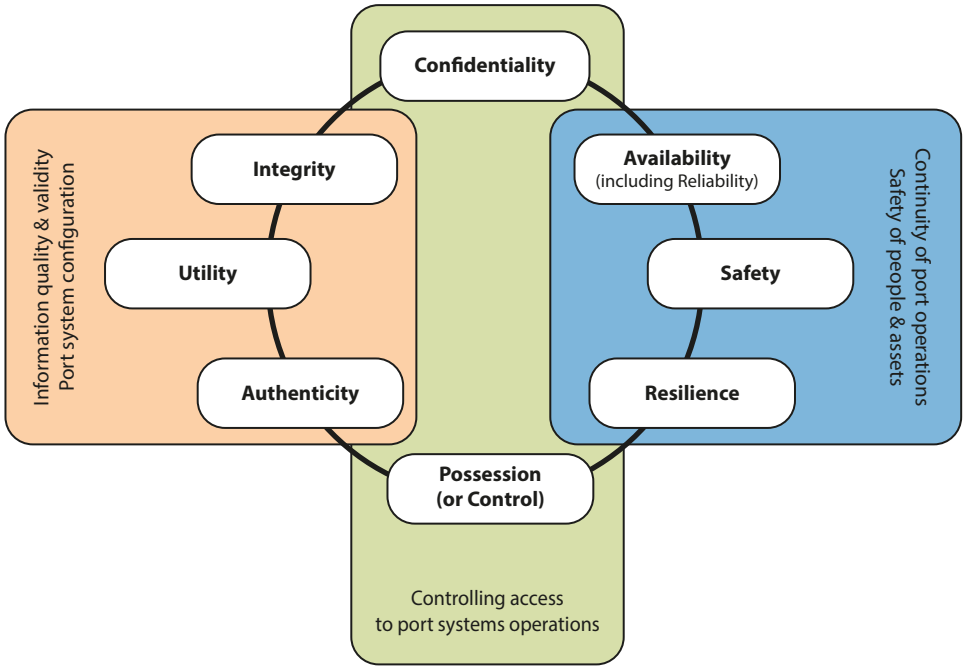
Cyber security can be defined as "the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organisation and user's assets."[1]

Within this definition, 'cyber environment' comprises the standalone computers and interconnected networks of both information and operational technology that use electronic, computer-based and wireless systems, including information, services, social and business functions that exist only in cyberspace.

The 'organisation and user's assets' includes connected and standalone computing devices, personnel, infrastructure, applications, services, telecommunication systems, and the totality of transmitted, processed or stored data in the cyber environment.

Cyber security strives to attain and maintain eight general security objectives, shown in Figure 2.1[2] and described in Appendix A.

▼ **Figure 2.1** Cyber security attributes



1 International Telecommunications Union (2008). Overview of cyber security. ITU-T X.1250, Geneva, Switzerland.

2 Adapted from Figure 2 of Boyes, H (2015) 'Cybersecurity and Cyber-Resilient Supply Chains'. Technology Innovation Management Review, 5 (4): 28-34

© The Institution of Engineering and Technology

The varied nature of cyber security threats means that there is no single approach that can address all the risks. The rate of change of technology and the steady flow of serious vulnerabilities in operating systems, software libraries and applications mean that any strategy needs to be kept under regular review.

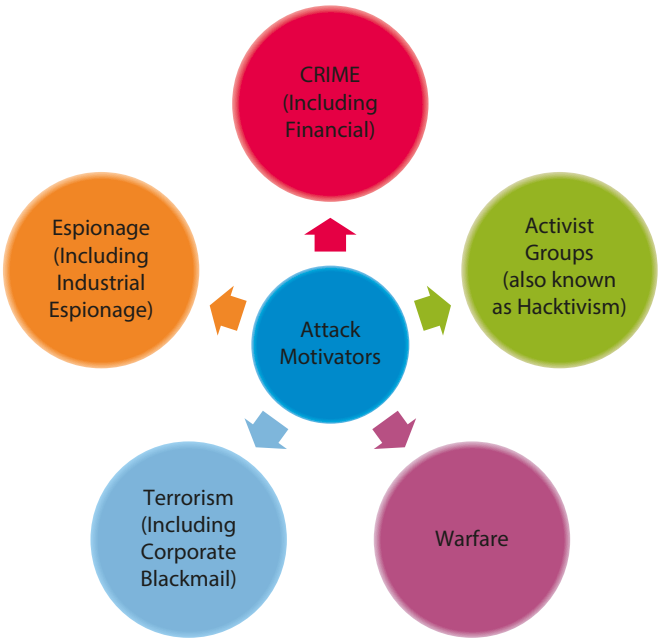
Business change also has a significant impact on cyber security, for example, with the introduction of bring-your-own-device (BYOD) and the trend to deliver some assets as services, such as the provision of back-up or standby power supplies under the management and control of a third party.

2.2 What are the motivations behind a cyber-attack?

The motivations of cyber threat actors to participate in a cyber-attack on a port system (as illustrated in Figure 2.2) can be varied, including state-sponsored espionage, the pursuit of greater kudos amongst hackers, or simply perverse curiosity. Motives include:

(a) espionage: seeking unauthorised access to sensitive information (intellectual property, commercial information, corporate strategies, personal data, pattern of life) and disruption for state or commercial purposes.
(b) activism (also known as 'hacktivism'): seeking publicity or creating pressure on behalf of a specific objective or cause, for example, to prevent the handling of specific cargos or to disrupt construction of a new port facility. The target may be the port itself, the operator of a port facility or a third party, such as the supplier or recipient of the cargo.
(c) criminal: largely driven by financial gain, this can include criminal damage, theft of cargo, smuggling of goods and people, and attempts to evade taxes and excise duties.
(d) terrorism: use of the port to instil fear and cause physical and economic disruption.
(e) warfare: conflict between nation states, where the aim is disruption of transport systems/infrastructure to deny operational use or disable specific port facilities, such as bulk terminals.

▼ **Figure 2.2** Cyber security threat actors



© The Institution of Engineering and Technology

The threat actors may be classified into seven categories, which are detailed further in Appendix A:

(a) individuals;
(b) activist groups;
(c) competitors;
(d) cyber criminals;
(e) terrorists;
(f) proxy terror threat actors; and
(g) nation states.

Any of these threat actors are equally relevant to elements of the port systems located beyond its perimeter, to port information/data stored on external servers, to services delivered by third parties and to the port's supply chain.

When considering the potential threats from the hostile groups listed above, it is important to recognise that there may be some convergence between the aims and objectives of individual groups. For example, some of the malware developed by cyber-criminal gangs includes sophisticated command and control functionality, allowing secure exfiltration of information and updating of modular components to deliver new or varied exploits over time. A machine or device that was compromised initially for financial crime could be used in future to access sensitive data or to provide a backdoor to allow attacks on port facilities or systems.

2.3 Environmental threats to port infrastructure

In addition to the human threat actors, there are environmental threats to port systems arising from natural causes, including solar events, weather, animals and insects. Their effects can result in damage, failure or significant impairment to utilities and port systems. In the case of the latter, port data may be lost or corrupted.

An example of the impact of natural causes on port operations was the tidal surge of 5th December 2013 that affected the port at Immingham, resulting in millions of tonnes of seawater surging over the lock gates into the port. Immingham, the UK's busiest cargo port, was under water for weeks. The port had a network of over 40 electricity substations, of which nearly half had a degree of water damage and ten were seriously impaired. These substations supplied electricity to port systems; due to the damage to the port's power supply infrastructure, the port could not be operated. The impounding pumps, used to maintain the water level in the docks, were located underground and were completely inundated. The motors and equipment had to be stripped down to be repaired or replaced.

Although port operations were severely disrupted, business continuity plans allowed some port operations to be restored within a few days, with the port operating on a tidal basis, with many operations diverted to Grimsby.

© The Institution of Engineering and Technology

© The Institution of Engineering and Technology

SECTION 3

Cyber security in ports

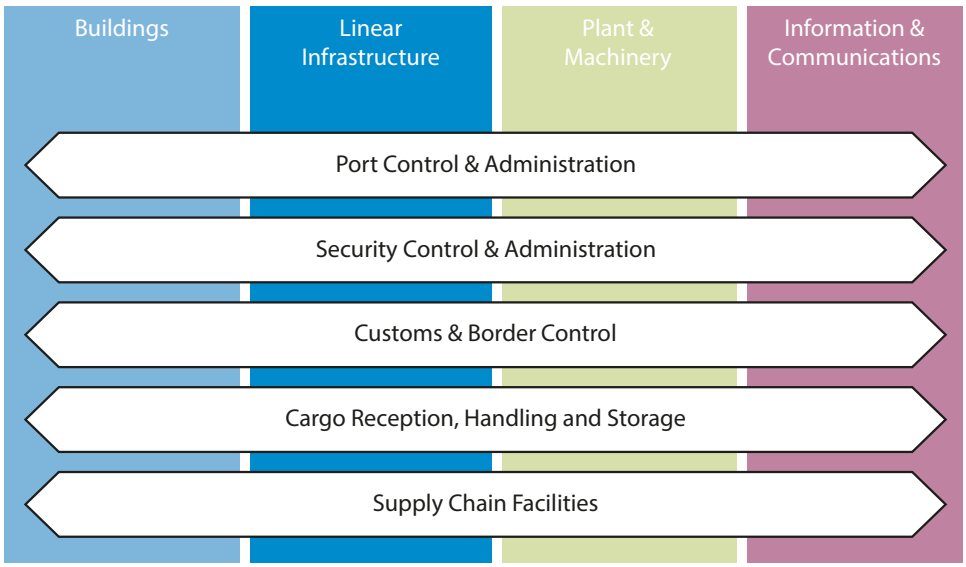
3.1 Why is cyber security important to ports?

A port is a complex cyber environment that encompasses both land and waterside activities and systems. As illustrated in Figure 3.1, and examined in more detail in Appendix A, a port typically comprises four main asset types (buildings, linear infrastructure, plant and machinery, and information and communications systems) that are used to provide a range of operational services and where technology plays an increasingly important role.

The loss, or compromise, of one or more of these assets has the potential to impact upon:

(a) the speed and efficiency at which the port can operate;
(b) the ability of the port to be able to safely carry out particular operations; and
(c) the health and safety of staff and other people affected by the work activities being undertaken and to whom a duty of care is owed.

▼ **Figure 3.1** Port assets affected by cyber security



3.2 Cyber security standards, guidance and good practice

Since this Guide was originally published in 2016, the Network and Information Systems Directive (the NIS Directive) has been implemented in the transport sector, following the coming into force of the UK implementing legislation (the NIS Regulations) on 10th May 2018.

© The Institution of Engineering and Technology

The Directive is designed to boost the overall level of security for network and information systems that support the delivery of essential services. It applies to those sectors that are vital for our economy and society, including the transport sector. It will continue to apply irrespective of the UK's relationship with the EU.

There is no specific conflict between this Good Practice Guide and the NIS principles. If ports, or related port-based organisations, have been following this Good Practice Guide (previously published as a *Code of Practice: Cyber Security for Ports and Port Systems* in 2016), then they will be making progress towards complying with the NIS principles. However, it is important to note that although there is overlap in several areas, following this revised Good Practice Guide, or the ISPS Code, will not automatically make a port compliant with the NIS Regulations. This Guide should only be considered as additional supporting guidance and is not legally binding. The NIS principles go further than the scope of this Guide and there is additional technical guidance that has been developed by the National Cyber Security Centre (NCSC) relating to compliance with the NIS Directive.

© The Institution of Engineering and Technology

SECTION 4

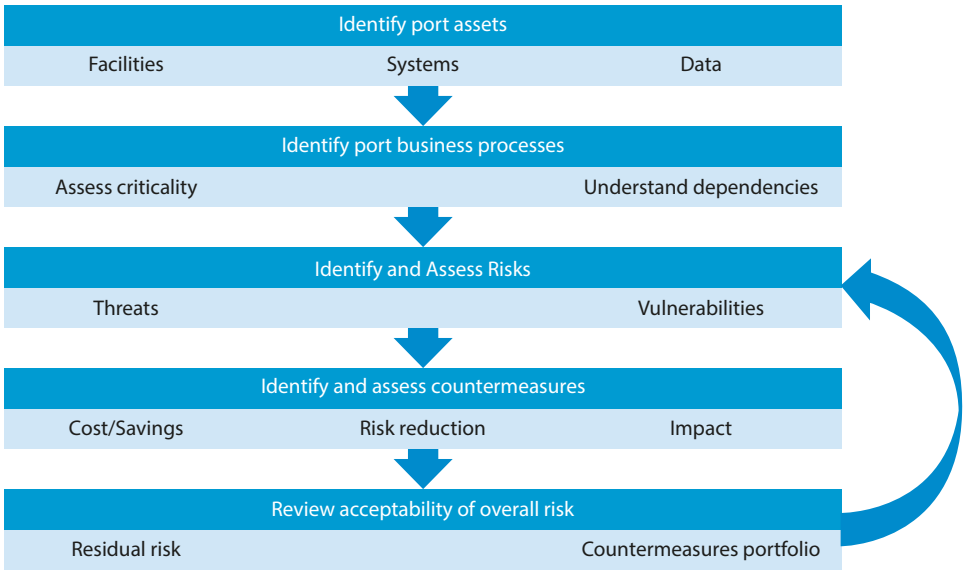
Developing a Cyber Security Assessment (CSA)

In compliance with the port security standards, security assessments are conducted for ports and port facilities. The purpose of these assessments is to identify vulnerabilities in physical structures, personnel protection systems and business processes that may lead to a security incident. It is intended that wherever appropriate, the Cyber Security Assessment (CSA) should build upon the existing security assessments.

As set out in the port security standards and illustrated in Figure 4.1, these assessments should include the:

(a) identification and evaluation of assets and infrastructure (for example, facilities, systems and data) that are considered important to protect, and the external infrastructure systems upon which they depend;
(b) identification of the port business processes using the assets and infrastructure, to assess criticality of assets and understand any internal and external dependencies;
(c) identification and assessment of risks arising from possible threats to the assets and infrastructure, and of vulnerabilities and the likelihood of their occurrence, to establish the need for and to prioritise security measures;
(d) identification, assessment, selection and prioritisation of controls, mitigations and procedural changes, based on their costs, the level of effectiveness in reducing the risk and any impact upon the port's operations; and
(e) identification of the acceptability of the overall residual risk, including human factors, and weaknesses in the infrastructure, policies and procedures, based on the portfolio of controls and mitigations that have been selected.

▼ **Figure 4.1** Overview of CSA process



While the above assessments do not cover the full range of potential cyber security threats, the port or port facility should produce a CSA that includes each of the aspects listed.

For further details of a process to create a CSA, see Appendix B.

© The Institution of Engineering and Technology

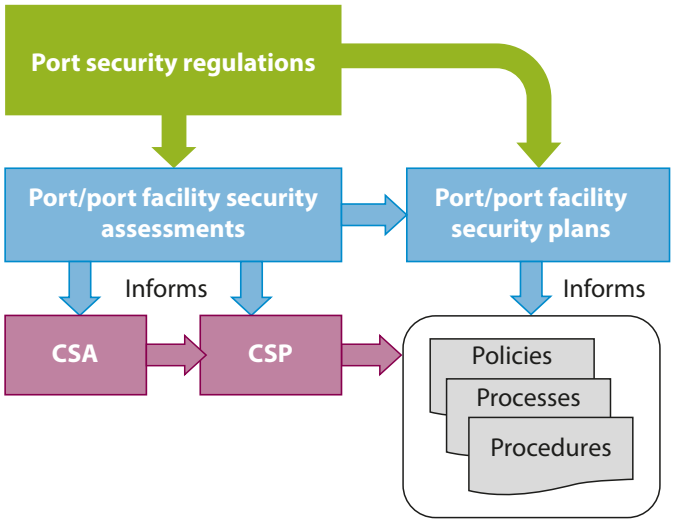
© The Institution of Engineering and Technology

Developing a Cyber Security Plan (CSP)

The security assessments form the basis of the security plans for the port and port facilities. These plans should address the issues identified in the relevant assessment through the establishment of appropriate security measures designed to minimise the likelihood of a breach of security and the consequences of potential risks. It is intended that wherever appropriate, that the Cyber Security Plan (CSP) will build upon the existing Port Security Plan (PSP) or Port Facility Security Plan (PFSP).

A CSP should perform the same function as the security plan for the issues identified in the CSA, also taking into consideration the impact of measures set out in the security plan for the port/port facility. Its relationship to other key documents is illustrated in Figure 5.1. The recommended contents for a model CSP are set out in Appendix C.

▼ **Figure 5.1** Relationship of CSP to other documents



When developing the CSP, it is essential that a holistic approach is adopted, covering the people, process, physical and technological aspects of the port assets. From a cyber security perspective, the CSP should contain or reference:

(a) the policies that set out the security-related business rules derived from the relevant PSP or PFSP;
(b) the processes that are derived from the security policies and that provide guidance on their consistent implementation throughout the lifecycle and use of the port assets; and
(c) the procedures that comprise the detailed work instructions relating to repeatable and consistent mechanisms for the implementation and operational delivery of the processes.

With a large proportion of security breaches caused by people and poor processes, it is essential that personnel, processes and physical aspects directly related to the technological systems for which cyber security measures are required are also considered and appropriate measures put into place.

© The Institution of Engineering and Technology

The measures required for each of the aspects will also depend upon the level of resilience that the port/port facility can call upon. Appendix D provides guidance on how to identify and implement appropriate mitigation measures, which should inform the development of the CSP and the supporting policies, processes and procedures.

The completed CSP for the port or port facility should be protected from unauthorised access or disclosure and should form an annex to the PSP or PFSP, respectively.

5.1 Review of the CSP

The CSP should include a suitable mechanism for performing periodic (at least annual) reviews to verify that it remains fit for purpose. Where necessary, the CSP should be updated to reflect any identified gaps, shortcomings or organisational changes, or changes that have arisen for political, economic, social, technological, legal or environmental reasons, and which impact upon the port or port assets.

The CSP should also establish a suitable mechanism for performing ad-hoc risk reviews to identify and assess the impact of any changes on port assets and to update the CSA, as described in Appendix B.

5.2 Monitoring and auditing of the CSP

The CSP should set out the appropriate and proportionate monitoring and auditing measures that will take place across the lifecycle of all port assets; these should be aligned, where applicable, with the business risk strategy. This monitoring or auditing will be in addition to any actions that may result from an incident or breach. The CSP should require that only those who are suitably qualified and experienced undertake this monitoring and auditing work.

Measures should include assessing:

(a) the implementation of all security policies, processes and procedures affecting the port assets, including the handling or storage arrangements implemented for security-sensitive and other sensitive information;
(b) the compliance of the supply chain with the security policies, processes and procedures specified in the CSP, as a minimum, on a risk-based sampling approach; and
(c) the management of security controls that operate throughout the operational lifecycle of the port assets.

Monitoring should continue through an event that causes the failure or interruption of one or more systems. An extreme weather event or other such occurrence does not remove the need for effective security and how the systems perform will inform subsequent development and loss exposure.

Whilst the port/port facility operator may delegate some responsibility for compliance verification to a supplier, it should retain accountability for the overall effectiveness of security controls.

© The Institution of Engineering and Technology

SECTION 6

Managing cyber security

Having established the cyber security management framework through the creation of the CSA and CSP, it is important that appropriate management and operational arrangements are in place, including:

(a) the identification of the individual(s) responsible for the cyber security of the port and port facilities, with an individual fulfilling this role being designated as a Cyber Security Officer (CySO).
(b) the possible formation, if one does not already exist, of a Port Security Committee (PSC). Many PSCs have now been superseded by Port Security Authorities (PSAs), established under the Port Security Regulations 2009. Where a PSC does not exist, it may be appropriate to discuss cyber security matters at meetings of the PSA.
(c) the establishment of a Security Operations Centre (SOC).
(d) the arrangements for providing information to third parties.
(e) the arrangements for managing security incidents or breaches.

6.1 Role of the CySO

Where a CSP is in place, a CySO should be responsible for:

(a) ensuring the development and maintenance of the CSP; and
(b) implementing and exercising the CSP.

Where the CySO has insufficient knowledge of cyber security issues and solutions, they should seek specialist cyber security advice from an appropriate professional source.

The CySO should maintain awareness of legal and regulatory changes that could affect the cyber security of port assets and, where necessary, make adjustments in policies, processes and procedures to comply with those changes.

For the CSP and associated security policies, processes and procedures to be effective, it is essential that there is a top-down flow of responsibility within both the organisation and the contracts or supply chain. Responsibility for cyber security may be shared by the CySO with other managers and service providers, although ultimate responsibility should be retained by the CySO.

The CSP should detail the:

(a) maintenance of security accountability within the port/port facility operator's organisation; and
(b) management of security responsibilities within the supply chain, including the requirement for security to be retained at senior levels within the supply chain, with responsibility delegated appropriately, in order that it can be effectively and efficiently managed.

© The Institution of Engineering and Technology

Where the port or port facility operator makes extensive use of contract personnel, the CySO should ensure that appropriate measures are used for the secure procurement of contracting personnel, including appropriate screening or background checks. These checks should also be in place for staff employed through other mechanisms.

6.2 Port Security Committee (PSC)

Where a port has established a PSC, the scope of the committee should include cyber security. Model terms of reference for a PSC that addresses all aspects of security are provided in Appendix E.

Where a port does not have a PSC because a PSA has been established, the PSA can consider cyber security.

6.3 Security Operations Centre (SOC)

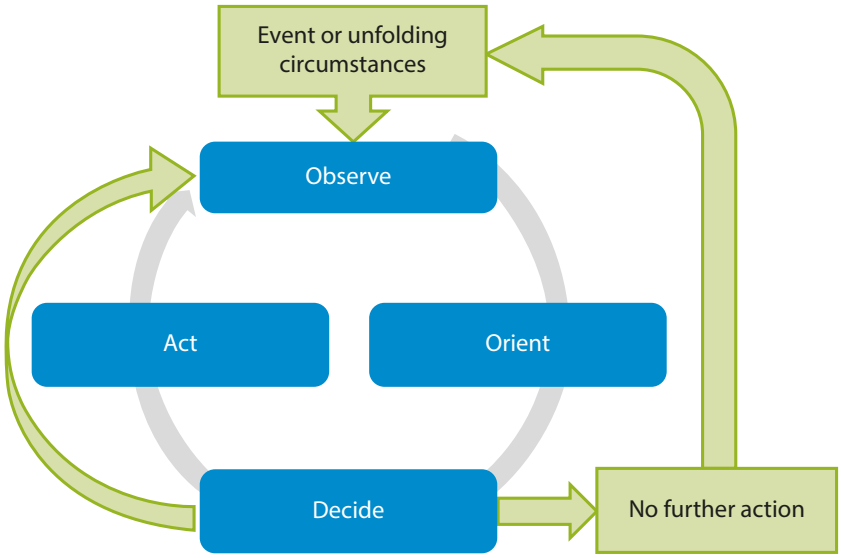
The SOC acts as a centralised unit dealing with security issues that affect a port/port facility, including those relating to cyber security, and may form part of an operations centre supervising the port, controlling access and managing business continuity and disaster recovery activities. Cyber security is an integral part of wider port security. It is about maintaining the integrity and availability of information and systems, ensuring business continuity and protecting cyber assets from the growing vulnerability arising out of the 'internet of things' (IoT).

The key functions of a SOC, as illustrated in Figure 6.1, are to:

(a) observe, by maintaining situational awareness: i.e., to understand potential, emerging and actual threats to the port/port facility operations. Observation includes detection of unauthorised changes to port systems or port data, non-secure modes of operation and unauthorised access to port assets.
(b) orient, by analysing the risk to operations from new or changed threats and determine whether proactive measures are required to reduce the risk to an acceptable level.
(c) decide, what action may be appropriate either to deny further access to the port asset or to respond to the event by identifying suitable controls and mitigations.
(d) act, by implementing the decision(s).

© The Institution of Engineering and Technology

Figure 6.1 Key functions of a SOC



When observing the operating environment, SOC personnel should maintain situational awareness of the general threat environment. From a cyber security perspective, this may involve accessing threat intelligence information from both public[1] and private-sector sources.

6.4 Provision of information to third parties

The port and port facility operators need to take appropriate measures to reduce the risk of sensitive information being released publicly or provided to unauthorised third parties. This can occur through public presentations, conference papers, marketing and publicity material, or using social media both by the organisation and its staff or by contractors and the supply chain. The implementation of an appropriate data loss prevention solution should also be considered. For further information, see Appendix F.

6.5 Handling security breaches and incidents

The CSA should detail the arrangements for handling security breaches and incidents, whether they occur accidentally or deliberately. A cyber security incident is likely to arise from unauthorised access to, misuse or fraudulent use of, port systems or related assets and may result in:

(a) loss or theft of assets, including documents and storage media;
(b) unauthorised access to data or information;
(c) loss, compromise, unauthorised manipulation or change of data or information;
(d) loss or compromise of port assets connected to its systems;
(e) planting of bugs or other surveillance devices;
(f) accidental or deliberate Global Navigation Satellite System (GNSS) jamming or interference; and
(g) insertion of malicious software.

For further information, see Appendix B.

1 In the UK, NCSC operates a joint industry and government Cyber-security Information Sharing Partnership (ciSP) to share cyber threat and vulnerability information.

© The Institution of Engineering and Technology

© The Institution of Engineering and Technology

SECTION 7

Terms and definitions

Definitions used in this Good Practice Guide are, as far as practicable, in keeping with those contained in the International Convention for the Safety of Life at Sea (SOLAS), 1974, as amended. For ease of reference, certain terms used are defined below.

7.1 Terms

Asset

Item, thing or entity that has potential or actual value to an organisation. (BS ISO 55000:2014, 3.2.1)

Asset information

Data or information relating to the specification, design, construction, acquisition, operation or maintenance of an item, thing or entity that has potential, or actual, value to an organisation. This also includes its disposal or decommissioning. It can include design information and models, documents, images, software, spatial information and task or activity-related information.

Cyber Security Officer (CySO)

The person or persons tasked to manage and co-ordinate the cyber security in a port/port facility. For larger ports, the CySO Officer is likely to report to the Chief Information Security Officer (CISO). For smaller ports, the role is likely to report to the Head of Security.

High-risk position

A position that has access to the details of the PSP, CSP, PFSP or other information relating to sensitive assets, or a position that fulfils an IT system administration or information management role.

Personnel

Individuals employed by an organisation, including contractors or temporary staff, used to fill roles that may be undertaken by that organisation.

Port

The geographical area defined by the Member State or the designated authority, including port facilities as defined in the ISPS Code, in which maritime and other activities occur.

Note: Whilst this definition applies to an area, which may be enclosed within a physical boundary for the purposes of physical security, from a cyber security perspective the port will include the port systems wherever they may be located, for example, hosted in a remote data centre.

© The Institution of Engineering and Technology

Port assets

All port data, port facilities and port systems.

Port data

Any data, information, models and processes associated with the ownership, design and operation of a port.

Port facility

A location, as determined by the contracting government or by the designated authority, where the ship/port interface takes place. This includes areas such as anchorages, awaiting berths and approaches seaward, as appropriate (International Convention for the Safety of Life at Sea (SOLAS), 1974, Chapter XI-2).

Port systems

Systems that are used to manage or control operational technology in a port, which may include: access control systems; port facility management systems; goods handling systems; energy management systems; port fire, communications, safety and security systems; GNSS container tracking technology; and those systems used to manage the port business.

Risk appetite

A function of an organisation's capacity to bear risk.

Security-sensitive information

Information, the disclosure of which would compromise the security of the port, including, but not limited to, information contained in any personnel-related file or privileged or confidential information that would compromise any person or organisation.

Sensitive asset

An asset, as a whole or in part that may be of interest to a threat actor for hostile, malicious, fraudulent or criminal behaviours or activities.

Sensitive information

Information, the loss, misuse or modification of, or unauthorised access to, could: adversely affect the privacy, welfare or safety of an individual or individuals; compromise intellectual property or trade secrets of an organisation; cause commercial or economic harm to an organisation or country; or jeopardise the security, internal and foreign affairs of a nation, depending on the level of sensitivity and nature of the information.

Threat

A potential cause of an incident that may result in harm to a system or organisation.

Vulnerability

A weakness of an asset, or group of assets, that can be exploited by one or more threats.

© The Institution of Engineering and Technology

7.2 Acronyms

ANPR	Automatic number plate recognition
CCTV	Closed-circuit television
CSA	Cyber Security Assessment
CSP	Cyber Security Plan
DDoS	Distributed denial of service
DfT	Department for Transport
Dstl	Defence Science and Technology Laboratory
EDI	Electronic data interchange
GNSS	Global navigation satellite system
IET	Institution of Engineering and Technology
ILO	International Labour Organisation
IMO	International Maritime Organisation
ISPS	International Ship and Port Facility Security
ITU	International Telecommunication Union
NCSC	National Cyber Security Centre (includes emergency response team)
NIS	Networks and Information Systems Directive
PFSA	Port Facility Security Assessment
PFSP	Port Facility Security Plan
PMR	Personal mobile radios
PSA	Port Security Authority
PSC	Port Security Committee
SCADA	Supervisory control and data acquisition
SOC	Security Operations Centre
SOLAS	International Convention for the Safety of Life at Sea

© The Institution of Engineering and Technology

© The Institution of Engineering and Technology

APPENDIX A

Understanding cyber security

A.1 Cyber security attributes

The port environment involves a variety of technologies, both existing and emerging, and the cyber security approach adopted will vary from building to building and from system to system. It will depend upon the complexity, ownership and use of the supply chain supporting the design, construction, operation and occupation of each building and its use. In the port environment, cyber security is therefore best addressed by considering a set of security attributes, thus allowing appropriate solutions to be adopted based on the nature of the building, facility or system and potential threats.

The key attributes of cyber security as applied to cyber-physical systems are outlined below. When considering these attributes, a risk management approach should be adopted, which will inform the degree to which any preventative or protective measures are implemented and the degree to which any residual risk is accepted.

(a) Confidentiality: the control of access and prevention of unauthorised access to port data, which might be sensitive in isolation or in aggregate. The port systems and associated processes should be designed, implemented, operated and maintained to prevent unauthorised access to, for example, sensitive financial, security, commercial or personal data. All personal data should be handled in accordance with the General Data Protection Regulation (GDPR) and additional measures may be required to protect privacy due to the aggregation of data, information or metadata.

(b) Possession or control: the design, implementation, operation and maintenance of port systems and associated processes to prevent unauthorised control, manipulation or interference.

(c) Integrity: maintaining the consistency, coherence and configuration of information and systems, and preventing unauthorised changes to them. The port systems and associated processes should be designed, implemented, operated and maintained to prevent unauthorised changes being made to assets, processes, system state or the configuration of the system itself. A loss of system integrity could occur through physical changes to a system, such as the unauthorised connection of a Wi-Fi access point to a secure network, or through a fault such as the corruption of a database or file due to media storage errors.

(d) Authenticity: ensuring that inputs to, and outputs from, port systems, the state of the systems and any associated processes and port data, are genuine and have not been tampered with or modified. It should also be possible to verify the authenticity of components, software and data within the systems and any associated processes. Authenticity issues could relate to data, such as a forged security certificate, or to hardware, such as a cloned device.

© The Institution of Engineering and Technology

(e) Availability (including reliability): ensuring that the asset information, systems, and associated processes are consistently accessible and usable in an appropriate and timely fashion. To achieve the required availability may require each of these to have an appropriate and proportionate level of resilience. A loss of availability could occur through the failure of a system component, such as a disk crash, or from a malicious act such as a denial of service attack that prevents the use of a system connected to the internet.

(f) Utility: ensuring that asset information and systems remain usable and useful across the lifecycle of the port asset. The port systems and associated processes should be designed, implemented, operated and maintained so that the use of port assets is maintained throughout their lifecycle. An example of loss of utility would be a situation where a port system has been changed or upgraded and the file format of historic data is no longer intelligible to the system. There has been no loss of availability, but the data is unusable.

(g) Safety: the design, implementation, operation and maintenance of port systems and related processes to prevent the creation of harmful states that may lead to injury or loss of life, or unintentional physical or environmental damage. A safety issue could arise through malware causing a failure to display or communicate port systems' alarm states. For example, the failure of a motion or proximity detector or other sensors could result in damage to property or loss of life.

(h) Resilience: the ability of the asset information and systems to transform, renew and recover in a timely way in response to adverse events. The design, implementation, operation and maintenance of port systems and associated processes should be such that cascade failures are avoided. If either a system or associated process suffers disruption or impairment, or an outage occurs, it should be possible to recover a normal operating state, or acceptable business continuity state, in a timely manner.

A.2 Threat actor groups

A.2.1 An individual

The severity and sophistication of the threat will be determined by the individual's capabilities, for example:

(a) a negligent, careless or ignorant employee or contractor, who fails to follow acceptable use or other security policies, or through error or omission compromises system security.

(b) 'friendly' individuals, who are not seeking to harm systems or data, but may access the systems without the permission or knowledge of the owner and cause accidental damage. The motivation of such agents is generally to investigate weaknesses and vulnerabilities in systems.

(c) a disaffected employee or contractor with limited IT skills: motivations will vary. The intent may be to steal or leak sensitive information, or to sabotage or disrupt port occupancy or operations, etc. The amount of damage this person can inflict will depend on their role, system access rights and the efficacy of cyber security measures related to the port systems and data.

(d) a disaffected employee or contractor with significant IT skills, including system administrators: these individuals can do significant damage, particularly if they have wide-ranging systems access with administrative privileges. They may have sufficient knowledge and ability to bypass controls and protective measures, and may be adept at removing evidence of their activities, for example, deleting or modifying entries in system logs. For sensitive roles, there is a need to consider aftercare of disaffected individuals leaving the organisation, based on an assessment of risk and monitoring of social media feeds.

© The Institution of Engineering and Technology

(e) 'script kiddies': individual hackers with limited knowledge who use techniques and tools devised and developed by other people. The ready availability of hacking and denial of service tools on the internet (in some cases, distributed with technical magazines) means that the level of technical understanding required to launch an attack has been significantly reduced.

(f) 'cyber vandals': these individuals can be very knowledgeable and may develop or further expand their own tools. Their motives are neither financial nor ideological: they carry out hacks or develop malware because they want to show what they can do. They may, for example, deface a website or break into a server to steal user credentials, which are then posted on a public website to demonstrate their ability.

(g) a 'lone wolf': an individual outside of the organisation possessing advanced technical knowledge. Such an individual may be adept at removing evidence of their activities, for example, deleting or modifying entries in system logs. They may also have sufficient knowledge and ability to bypass controls and protective measures. The number of such individuals is currently small, but may expand because of increased awareness of technical systems amongst the general population, or as members of nation state groups leave government service.

A.2.2 Activist groups

Often referred to as 'hacktivists', these groups comprise ideologically motivated individuals that may form dynamic groups or sub-groups. Their actions are effectively online protests, which may have the aim of disrupting systems or acquiring confidential or sensitive information for publication or dissemination to embarrass their target(s). The impact of small activist groups can be significantly magnified when, as some groups have demonstrated, they recruit or persuade naïve third parties to join in by allowing the installation of malicious software on the recruits' computers, thus creating botnets[1] and magnifying the effect of any distributed denial of service (DDoS) attacks.

A.2.3 Competitors

This group is typically made up of large corporations seeking to create a competitive advantage. They may act directly or through third parties, with the aim of harming a rival by collecting business intelligence, stealing intellectual property, gathering competitive intelligence on bids or disrupting operations to cause financial or reputational loss. Depending on size, sector, geographic location and the sophistication of a large corporation's cyber capabilities, they may be able to perform sophisticated malicious activities to target and infiltrate their competitors.

A.2.4 Cyber criminals

These are sophisticated criminal groups perpetrating a wide range of illegal IT-enabled crime. The motivation is to profit from illegal activities and their focus has mainly been on fraud, thefts from accounts and theft of intellectual property. However, cyber-criminal activities also include blackmail and extortion, using malware to encrypt data or threats of DDoS attacks on corporate websites. In respect of ports, cyber criminals may seek to intercept or access information related to cargo shipments or to security arrangements as a precursor to criminal activities or a physical attack on these premises. The sophistication of the malware used by these groups is increasing and there is evidence of a cyber-crime market, where developers, providers and operators create, supply and operate sophisticated malware and cyber-crime tools on a commercial basis, making their tools available to third parties.

---

1 A botnet is a network of computers infected with malicious software (malware) and controlled as a group without the users' or owners' knowledge; they may be used to send spam or in DDoS attacks.

© The Institution of Engineering and Technology

A.2.5 Terrorists

Terrorists are becoming increasingly IT aware, and already make extensive use of the internet to distribute propaganda and for communications purposes. Well-funded groups could take advantage of the service offered by cyber criminals, seek support from a nation state or encourage internal members to adopt these methods of attack. With the widespread use of electronic- and computer-based technologies in the port environment, terrorist groups could rely on the various toolkits available for download to disrupt or damage ports by attacking port systems. Terrorists may also exploit poorly secured port data to enable remote hostile reconnaissance of targets, thus reducing the time they need to spend in or near their target.

A.2.6 Proxy terror threat actor with nation state support

This is, in effect, state-sponsored terrorism, where the proxy party is used to provide deniability. This type of group effectively has the capacity and sophisticated technical support available to a nation state, made available by the sponsoring nation. This group could include cyber fighters: groups of nationally motivated individuals who threaten or attack other groups, businesses and the infrastructure of other nation states. These cyber fighters may be seen as a type of 'hacktivist', but their interest is the support of a nation state and as such they may enjoy significant sophisticated technical support from that nation state.

A.2.7 Nation states

It is acknowledged that some nation states are actively involved in cyber-attacks on a wide range of organisations to acquire state secrets or sensitive commercial information and intellectual property. They may also threaten the availability of critical infrastructure in other nation states. During periods of heightened international tension and conflict, these activities may include more widespread attacks as evidenced by malware such as Stuxnet[2], Duqu[3] and Flame[4].

A.3 Port assets and cyber security

For the purposes of developing appropriate and proportionate cyber security measures, each of the technical systems in place can be considered as largely located in, or directly related to:

(a) buildings;
(b) linear infrastructure;
(c) plant and machinery; or
(d) information and communication systems.

A.3.1 Buildings

Port facilities will include a variety of buildings, requiring security, access control and varying levels of technical infrastructure. Specialist buildings that may be found on a port include:

2 For further information, see: http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet
3 For further information, see: https://resources.infosecinstitute.com/duqu-2-0-the-most-sophisticated-malware-ever-seen/#gref
4 For further information, see: http://www.wired.com/2012/05/flame/

© The Institution of Engineering and Technology

(a) maritime control centres hosting the systems, terminals and displays used to manage vessel traffic both within the port and along the approaches to it;
(b) data centres;
(c) maintenance sheds or workshops;
(d) warehouse and other storage accommodation, some of which may require specific environmental control, for example, cold stores;
(e) administrative accommodation for port staff and any government services operating within the port; and
(f) offices which host container location systems.

These buildings are typically serviced by IT-based building management systems (including GNSS container management systems) and may have wired or wireless networking installed.

A.3.2 Linear infrastructure

Port facilities will include a variety of types of linear infrastructure, requiring control systems, security monitoring and access control. Types of infrastructure that may be found in a port include:

(a) roads;
(b) rail systems;
(c) internet access and other utilities;
(d) cargo handling systems such as pipelines and conveyer systems; and
(e) dockside linear infrastructure.

A.3.3 Plant and machinery

Ports utilise a diverse range of plant and machinery for the management of the port and for cargo handling, which may include:

(a) tidal locks and any associated pumps that are used to permit access from tidal waters and to maintain water levels within the docks;
(b) automatic barriers/gates to control vehicular and pedestrian access to areas within the port;
(c) cranes and conveyer systems used for the handling of dry bulk cargos;
(d) vehicles or non-fixed cranes that move containers and cargo; and
(e) gauges, pumps and valves used to control the flow of wet bulk cargos.

A common feature of this plant and machinery is the use of industrial control systems and supervisory control and data acquisition (SCADA). Some of these systems may be standalone, but increasingly they are connected to the port's enterprise network.

A.3.4 Information and communication systems

Within a port there will be a range of data, including information used to support decision-making and data that is used to affect a physical outcome (for example, to control movement of cargo and containers). The sensitivity of individual systems will depend on whether they create, process, store or provide access to security-sensitive or other sensitive information.

© The Institution of Engineering and Technology

Within cargo operations, IT is an essential part of the rapid and accurate transfer and processing of significant data volumes, relating to shipments, customs clearance, vessel itineraries and crew information, processed by international transport firms and port organisations. This applies both to container traffic and to other cargos, including vehicles, bulk material, ferry and cruise traffic, etc.

Operations require significant levels of planning and co-ordination, encompassing:

(a) the scheduling of land-side container arrival and collection at the port, which, along with the cargo information, includes data about the delivery vehicle, driver, container number, container size and scheduled arrival window;
(b) planning and organising container locations in the stacking area, including tracking any moves;
(c) planning and scheduling container loading onto vessels, with the aim that a container's position in the on-board stacks minimises the amount of temporary off-loading at the destination port; and
(d) providing information to customs authorities to enable payment of any duties and grant of customs clearance.

These are managed using an asset management system, potentially in combination with a yard management or container traffic management system. Together, they may include:

(a) real-time information terminals at:
  (i) entry gates for booking containers into the port; and
  (ii) container loading/unloading bays;
(b) automatic number plate recognition (ANPR) for lorries entering and leaving the container terminal, including:
  (i) closed-circuit television (CCTV); and
  (ii) video analytics;
(c) automatic container number reading and optical inspection for damage and presence of seals both on arrival and departure from the port;
(d) detailed position tracking of containers when placed/moved in the dockside storage areas;
(e) provision of movement and loading instructions to handling systems (for example, gantry cranes, straddle carriers, rubber tyre gantry units, etc.); and
(f) records of receipt of customs clearance to authorise the land-side release of imported containers.

The communications medium(s) used for exchanging the necessary data include voice, email, electronic data interchange (EDI) and web portals. The level of sophistication of these exchanges will vary considerably, depending on the degree of automation of any cargo handling and the IT capabilities of the relevant shipping community. The communications systems associated with control systems may use a variety of communications technologies, including IP and non-IP based networking, wireless and wired media and protocols.

© The Institution of Engineering and Technology

Whatever the means of communication, the integrity of the asset database and the associated transactions is critical for the smooth operation of the container terminal.

Similar operations and systems are required for the handling of non-container cargos, for example, vehicles, bulk material, ferry and cruise traffic, etc. These will be handled within specific port facilities, with systems tailored to the management, movement, handling and storage or marshalling of either the cargo or passengers, and include:

(a) security control: the port and cyber-physical systems that may be used to:
- **(i)** provide access control for staff, contractors and visitors;
- **(ii)** secure either the port or the port facility perimeter;
- **(iii)** control access by vehicles and pedestrians; and
- **(iv)** prevent or deter either theft of goods or damage to port facilities;

(b) port control and administration: the facilities used to manage the day-to-day operations of the port, including:
- **(i)** scheduling of cargo;
- **(ii)** movement and storage of cargo;
- **(iii)** vehicle and passenger movements through the port; and
- **(iv)** potentially managing vessels in the approach to the port;

(c) police, customs and border control: while these systems may largely operate independently, some access is generally required to the port's facilities (for example, warehouses) and systems (for example, read access to the operations database and access to CCTV feeds and telemetry);

(d) supply chain facilities: while some may act independently of the port's information and communications infrastructure, with very limited access granted in relation to information about vessel movements, others may be integrated into the operation of the port or one of its port facilities; and

(e) cargo reception, storage and handling: the precise nature of these systems will vary, according to the nature of the cargo being handled.

© The Institution of Engineering and Technology

© The Institution of Engineering and Technology

APPENDIX B

Process for developing a Cyber Security Assessment (CSA)

The port and port facility should first assess each of the vulnerabilities, controls or mitigations identified in the respective latest port or port facility assessment reports to establish whether there are cyber security implications arising from them. For example, the deployment of technology-based security systems as controls and mitigations to specific security threats or vulnerabilities may introduce or increase cyber security vulnerabilities.

The port and port facility should then review their overall business risk assessment to assess the level of exposure and whether there are any additional potential cyber-related threats and vulnerabilities across the full range of port systems and data (for example, cargo handling systems, security systems, industrial control systems, etc.) not identified in the security assessments for a port/port facility, but which nevertheless impact upon the cyber security of each or both.

Where the security assessments for a port or port facility do not cover the full range of potential cyber security threats, the port or port facility should produce a CSA. This CSA should cover and document the same aspects as the security assessments for a port/port facility, as described in Section 4.

The completed CSA for the port or port facility may form an annex to the security assessments for the port or port facility.

B.1 Identification and evaluation of important cyber assets and infrastructure

It will first be necessary to understand:

(a) how the different assets support the port's operational use;
(b) the criticality of different areas within the port/port facility; and
(c) the systems that support or protect these critical assets or areas.

From a cyber security perspective, the business critical or sensitive elements of a port are likely to include:

(a) those assets that have been judged to have the potential to be used to significantly compromise the integrity of the port as a whole or the ability of a specific facility or system to function as required. Consideration should be given to:
  (i) configuration, identification and use of control systems;
  (ii) critical permanent plant or machinery;
  (iii) security or other control rooms, including guarding;
  (iv) security, alarm and access control systems, CCTV and video processing;
  (v) reliance on GNSS technology for port operations; and
  (vi) cabling routes and their containment (for example, ducts and trunking).

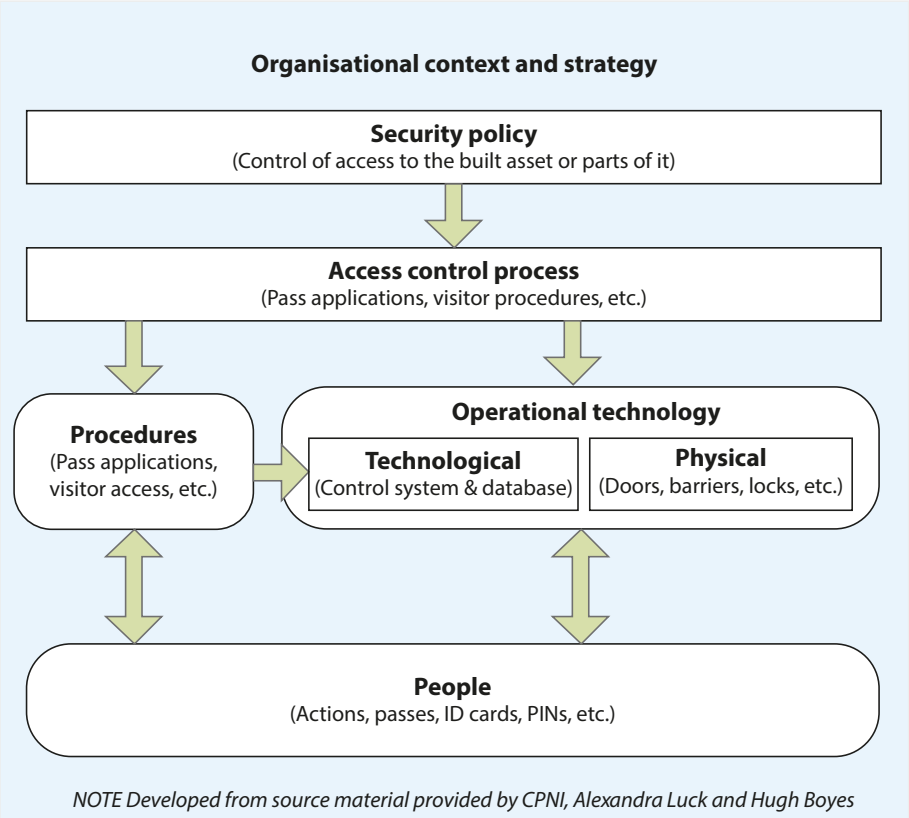
© The Institution of Engineering and Technology

(b) key spaces and facilities used by law enforcement and security service personnel operating in, or visiting, the port.
(c) port data relating to the location, identification, technical specification and operation of business critical and sensitive assets.
(d) port systems, wherever they are hosted, used for planning, scheduling and receipt of ships and cargo.
(e) assets or systems upon which the business critical or sensitive elements are dependent for their normal operation and resilience.

B.2 Identification of the port business processes

The operation of a port or port facility will depend upon a set of business processes that rely upon port data for the safe, secure and efficient movement of cargo through the port and enable supporting processes such as asset management, resource scheduling, financial and business planning, procurement and the human resource processes. Having identified and assessed the important assets and infrastructure, the next step is to identify the port business processes that use the cyber assets and infrastructure, as illustrated in Figure B.1.

▼ **Figure B.1** Example of components supporting access control process, courtesy of BSI



NOTE Developed from source material provided by CPNI, Alexandra Luck and Hugh Boyes

This information should be used to assess the criticality of assets and to understand the interdependencies of the data and systems within the overall business processes of the port. By so doing, the real impact of failure or compromise of individual components can be understood.

© The Institution of Engineering and Technology

B.3 Identification and assessment of risks arising from potential threats and vulnerabilities

The potential threats should already have been identified in the Port Security Assessment (PSA) and Port Facility Security Assessment (PFSA). However, it will be necessary to understand the degree to which individual threats and combinations of them may impact on the cyber security of the port/port facility.

When considering threat scenarios and types of undesired events, the port or port facility operator should include incidents and factors such as:

(a) unauthorised access to sensitive port data (commercial, personal or security-related);
(b) theft of sensitive port data;
(c) deletion, unauthorised modification or corruption of port data;
(d) infection with malware;
(e) loss of service from systems due to loss of connectivity or power;
(f) loss of service from systems due to software or hardware failures;
(g) compromise of port security systems;
(h) denial of service (externally hosted systems);
(i) denial of service (port systems);
(j) jamming or interference with timing or positioning systems (GNSS); and
(k) the efficacy of system operation (for example, coverage and performance of CCTV and intruder detection systems).

The identification of vulnerabilities should include consideration of:

(a) the relationships between systems;
(b) the technical composition of systems in terms of hardware and software components and the builds or revisions that are being used;
(c) the physical robustness of enclosures (for example, cabinets, ducts, trunking, etc.);
(d) the relationships between systems and associated business processes;
(e) the existing security measures and procedures, including the presence and permeability of any secure perimeter that prevents or limits access to the port, port facility and associated utilities, plant and machinery;
(f) the reliance on automation of equipment;
(g) the level of resilience within the port or port facility, including the level of dependency of systems on infrastructure, for example, utilities;
(h) any conflicting policies between safety and security measures and procedures;
(i) any enforcement and personnel constraints;
(j) any deficiencies identified during daily operation or following incidents or alerts, the report of security concerns, the exercise of control measures, audits, etc; and
(k) what could happen to container management systems if GNSS was denied for extended periods.

The cyber security risk assessment should consider the nature of harm that could be caused to:

(a) personnel and other occupants or users of the port and its services;
(b) the port and port assets; and
(c) the benefits the port exists to deliver, whether societal, environmental or commercial.

© The Institution of Engineering and Technology

The degree of cyber security risk will depend on the likelihood that a threat actor can exploit one or more vulnerabilities and cause the nature of harm identified.

Throughout the process, it will be essential for the port and port facility to liaise with each other to identify common risks, as well as where a risk in one may compromise the security of the other.

B.4 Identification, assessment, selection and prioritisation of countermeasures

For every cyber security vulnerability not already addressed by the security assessments for a port/port facility, the port/port facility operator should identify and record possible mitigation or countermeasures.

The assessment of each countermeasure should identify and record:

(a) the cost of the countermeasure and its use and maintenance;
(b) other impacts the countermeasure might have, for example, on asset or system usability and efficiency, business processes and port operations;
(c) wherever possible, to support the business justification for investment in the countermeasure:
  (i) the risk reduction that could be achieved; and
  (ii) the predicted cost saving;
(d) the potential for the countermeasure to create further vulnerabilities; and
(e) whether the countermeasure delivers any other business benefits, for example:
  (i) reduction of overall business risk; or
  (ii) aiding the development of efficient, robust and repeatable business processes.

The countermeasures that are chosen for implementation should be appropriate and proportionate to the risk that they are intended to mitigate. The selected measures should be listed in the CSA and should include a record of where co-operation is required between the port or port facilities for their successful implementation.

B.5 Review acceptability of residual risk

The assessment process should continue until a point is reached where the level of residual risk does not exceed the risk appetite of the port/port facility (i.e. the steps outlined in Sections B.3 and B.4 should be repeated). The remaining residual risks should be listed in the CSA.

B.6 Review of the Cyber Security Assessment (CSA)

As with the security assessments for a port/port facility, the CSA should be periodically reviewed and updated, taking account of:

(a) changes in previously identified risks;
(b) new threats or vulnerabilities;
(c) changes in the port and port facility;
(d) the success of implemented countermeasures; and
(e) new, and potentially more effective, countermeasures.

© The Institution of Engineering and Technology

The port or port facility operator should establish a suitable mechanism for performing ad-hoc risk reviews to identify and assess the impact of any changes on the port and port assets that should be reflected in the CSA. The triggers for initiating such a review and the timetable for its completion should be set out within the CSP. Triggers should include, as a minimum, the following events:

(a) a significant security incident at a port facility;
(b) a significant security incident affecting an externally hosted port system;
(c) a change in the shipping operations undertaken at the port;
(d) a change in the location, hosting or support of port systems;
(e) a project initiated to significantly change the port or its operations; and
(f) a change of port/port facility owner or operator.

Where the port contains many port facilities with different risk profiles, the CSA may need to be reviewed at a higher frequency in relation to any port assets that are deemed to be more sensitive. It is especially true of cyber security that any risk assessment represents a snapshot of a particular moment, which may change dramatically with the emergence of a new vulnerability.

B.7 Model port cyber security assessment

PART 1: INTRODUCTION

The importance of undertaking preventative cyber security measures has been highlighted over the past few years, with numerous high-profile cyber-attacks taking place. These attacks have at times created havoc – such as in the ransomware attacks on the NHS – or caused huge business losses. There have also been several malicious attacks undertaken by unfriendly nations where the intent has simply been to disrupt normal life or the processes of government.

Most cyber-attacks are relatively unsophisticated. Cyber Essentials, a service provided by the NCSC, offers advice and guidance on the basic steps any business can take to improve cyber security in their operations through self-assessment and cyber security certification. Clearly, different ports will want to evaluate what level of response may be most relevant to their business. The guidance can be viewed on the Cyber Essentials website: https://www.cyberessentials.ncsc.gov.uk/.

The CSA is an essential and integral part of the process of developing and updating Cyber Security Plans (CSPs). It provides a basis for determining the exact nature of the cyber security measures and procedures that should be introduced at each port or facility to minimise the chances of a successful cyber-attack taking place.

Ports vary in considerable ways and the CSA is thus designed to be easily used by any operator of a port, port facility or any other body that is connected to a port to assess the vulnerability of their own assets to cyber threats and attacks. There is no legislative requirement to complete a CSA, but the completion of one on a regular basis could help to identify areas where improved cyber protection could be of benefit to the port or organisation's everyday business.

It is worth noting that due to the diversity of port activities, it is quite possible that a single port may have several CSAs covering the whole port or parts of the port, or even overlapping CSAs, where port facilities rely on each other.

© The Institution of Engineering and Technology

Port authorities may ask their individual tenants to complete a CSA to ensure that the whole port is considering the matter of cyber protection to a reasonable standard.

[Insert name of port or facility] was assessed during the on-site assessment and survey that took place on [insert date].

The CSA should help to:

1. identify and evaluate the most important assets and infrastructure;
2. identify weaknesses, including human factors, safer IT policies and procedures;
3. identify, select and prioritise effective countermeasures and procedural changes in reducing vulnerability.

PART 2: PORT OR FACILITY DETAILS

Operational Overview and Port Management

[Insert appropriate text here]

PART 3: ASSETS

Identification and evaluation of important assets and infrastructure that could contain a cyber vulnerability.

The table below helps identify key assets and infrastructure vital for the continuation of core business. How important are the following assets and infrastructure to the facility's day-to-day business?

	Asset/ Infrastructure Present within the port/facility (Yes/No)	Criticality to facility operations (Low, Moderate, High, Very High)	Could the facility operate without the asset? (Yes/No)	Is this asset connected to an IT network? (Yes/No)	Does the asset have good cyber protection? (Yes/No/N/A)
Lockgate machinery					
Linkspans					
Floating dry dock/ slipways					
Pipelines					
Bulk liquid manifolds					
Bunkering facilities					
Conveyor loaders					
Gantry cranes					
Mobile cranes					
Fixed cranes					
Straddle Carriers/top lifters					

© The Institution of Engineering and Technology

	Asset/ Infrastructure Present within the port/facility (Yes/No)	Criticality to facility operations (Low, Moderate, High, Very High)	Could the facility operate without the asset? (Yes/No)	Is this asset connected to an IT network? (Yes/No)	Does the asset have good cyber protection? (Yes/No/N/A)
Other bulk handling machinery					
Vehicles – Ro-Ro & Yard Tugs					
Vehicles – Other					
Marine launches/craft					
Radar equipment					
Cargo processing plant					
Other plant/ equipment/ workshops					
LPG Gas					
Mains electrical substation					
Locally generated electricity					
Hydraulic/ Pneumatic power					
Mains water supply					
Mains gas supply					
Firefighting equipment					
Emergency water supplies					
Fuel/oil storage					
IT Networks					
IT Servers					
Internet access					
Mobile phones					
Landline telephone					
Fax					
Radio system					
CCTV Cameras (operations)					
Radiation Detection System					
Refuse management					
VTS/Port Information System					

© The Institution of Engineering and Technology

	Asset/ Infrastructure Present within the port/facility (Yes/No)	Criticality to facility operations (Low, Moderate, High, Very High)	Could the facility operate without the asset? (Yes/No)	Is this asset connected to an IT network? (Yes/No)	Does the asset have good cyber protection? (Yes/No/N/A)
Weighbridges					
Marine Traffic Signals					
Navigation lights					
Dock lighting					
Passenger Terminal buildings					
Security/ Operations buildings					
Other Office buildings					
Railway lines					
Port Staff					
Access or Internal Roads					
Approach Channel					
Unique to Port					

PART 4: VULNERABILITIES

Identification of weaknesses, including human factors, in the infrastructure, policies and procedures

This table outlines vulnerabilities identified with current cyber security measures considered. A description of the vulnerabilities should be set out below in the table, where appropriate. How vulnerable are the following assets/infrastructure?

Asset/Infrastructure	**N/A**	**Very Low**	**Low**	**Moderate**	**High**	**Very High**
Lockgate machinery						
Linkspans						
Berths/jetties						
Floating dry dock/slip-ways						
Pipelines						
Bulk liquid manifolds						
Bunkering facilities						
Conveyor loaders						
Gantry cranes						
Mobile cranes						
Fixed cranes						

© The Institution of Engineering and Technology

Asset/Infrastructure	N/A	Very Low	Low	Moderate	High	Very High
Straddle Carriers/top lifters						
Other bulk handling machinery						
Vehicles – Ro-Ro & Yard Tugs						
Vehicles – Other						
Marine launches/craft						
Radar equipment						
Cargo processing plant						
Other plant/ equipment/ workshops						
LPG Gas						
Mains electrical substation						
Locally generated electricity						
Hydraulic/ Pneumatic power						
Mains water supply						
Mains gas supply						
Firefighting equipment						
Emergency water supplies						
Fuel/oil storage						
IT Networks						
IT Servers						
Internet access						
Mobile phones						
Landline telephone						
Fax						
Radio system						
CCTV Cameras (operations)						
Radiation Detection System						
Refuse management						

© The Institution of Engineering and Technology

Asset/Infrastructure	N/A	Very Low	Low	Moderate	High	Very High
VTS/Port Information System						
Weighbridges						
Marine Traffic Signals						
Navigation lights						
Dock lighting						
Passenger Terminal buildings						
Security/ Operations buildings						
Other Office buildings						
Railway lines						
Port Staff						
Access or Internal Roads						
Approach Channel						
Unique to Port						

PART 5: COUNTERMEASURES

Identification, selection and prioritisation of countermeasures and procedural changes and their level of effectiveness in reducing vulnerability

Insert text here suggesting suitable measures that can be undertaken to reduce the vulnerability of important port assets to cyber threats and attacks

PART 6: SIGN OFF BY MANAGEMENT OR BOARD MEMBER

The CSA of [insert name of port or facility] was undertaken on [insert date here]. It was conducted by [add names and roles]. The CSA also considered the particular circumstances of the port/facility and the port/facility's assets, infrastructure and vulnerabilities.

It is expected that CSAs are periodically reviewed and updated and are always revised when major changes to the port facility take place. It is therefore essential that a new CSA is undertaken in the event of any such changes, which might include a change of ownership, a change in types of cargo handled, or major structural or other changes that may impact on the cyber vulnerabilities of the port.

The next review of this CSA is due on [insert date here].

© The Institution of Engineering and Technology

APPENDIX C

Contents of a Cyber Security Plan (CSP)

The port security standards define the term 'security level' to mean the degree of risk that a security incident will occur or be attempted. The CSP needs to be developed to cover the three levels of risk that are defined as:

(a) security level 1: the level for which minimum appropriate protective security measures shall be implemented always;
(b) security level 2: the level for which appropriate additional protective security measures shall be maintained for a period of time because of heightened risk of a security incident; and
(c) security level 3: the level for which further specific protective security measures shall be maintained for a limited period of time when a security incident is probable or imminent, although it may not be possible to identify a specific target.

The recommended contents of the CSP should include, as a minimum:

(a) information on cyber security responsibilities and links to organisations that will assist the port/port facility in the event of a cyber security incident.
(b) how the communications systems and equipment identified in the CSA will be maintained.
(c) the cyber security drills to be practiced, testing the port's response to cyber security incidents.
(d) the cyber security of communications, including those:
  (i) between personnel with security responsibilities;
  (ii) between those responsible for technical security and the wider security team; and
  (iii) that provide information about the port and port assets to third parties.
(e) cyber security measures required for any connection between ship systems and those of the port/port facility.
(f) processes and procedures for approving the electronic or wireless connection of ship and port systems.
(g) any changes to systems or system operations required at higher security levels, including any increased security measures required for admission of IT and systems maintenance contractors to the port/port facilities when the port is operating at security levels 2 and 3.
(h) access control measures relating to cable ducts, trunking and cabins of equipment boxes located within the port, irrespective of whether they are in restricted or open areas.
(i) access control measures to sensitive IT systems and accommodation, for example, networking, communications and server rooms.
(j) cyber security measures pertinent to the protection and assurance of cargo-related data and the systems that process, store and transmit it (for example, GNSS container management systems). Where the port has automated systems handling cargo movement or storage, the plan should address the security measures required to protect the operational IT systems.
(k) cyber security measures pertinent to the protection and assurance of ships' stores and bunkering data and any systems that process, store and transmit it.

© The Institution of Engineering and Technology

(l) cyber security of port lighting, electronic access, security and monitoring systems and any specialist systems required to support security patrols or law enforcement authorities, for example, radiation detectors.
(m) response to cyber security threats, breaches and security incidents.
(n) arrangements for auditing of cyber security measures.
(o) contractual measures for the adoption of relevant cyber security measures within the supply chain to the port/port facility.
(p) cyber security awareness and training required by staff.

The section of the CSP that addresses security breaches and incidents should enable an effective and coordinated response. This will require an assessment of potential risks to the port/port facility, its function, port assets, personnel and third parties in the event of a security breach or incident. The section should include:

(a) the risk mitigation measures, including:
  (i) the forensic readiness measures required to enable the capture of forensic information about an incident for use by law enforcement and for the detailed analysis of the root causes of the incident;
  (ii) the process to be followed on discovery of a breach/incident (including near misses – that is, narrow avoidance of a security breach/incident);
  (iii) business continuity measures required in the event of port system failure, impairment or non-availability;
  (iv) the disaster/incident recovery actions required in the event of serious failure scenarios; and
  (v) steps to be taken to contain and recover from the event;
(b) the review process following a security breach or incident, including both an assessment of any ongoing risk and an evaluation of the response to the breach or incident by the port/port facility and, where appropriate, the supply chain;
(c) the need for contractual provisions to handle breaches/incidents caused by a third party connected to the port, for example, a professional advisor, contractor or supplier;
(d) the mechanisms for reviewing and updating the CSA, CSP and security procedures following a significant security breach or incident:
  (i) at the port or one of its port facilities; or
  (ii) at another port/port facility; and
(e) the arrangements for conducting cyber security incident response exercises, which the port/port facility may handle in conjunction with existing business continuity planning and exercises.

C.1 Model port cyber security plan

This model plan is included as a guide to help you create your own cyber security plan specific to your own port/port facility's requirements. It is not a 'one size fits all' document. Once completed, the DfT recommends that a printed hard copy of this plan is stored in a safe place, in case your cyber systems should become unavailable.

© The Institution of Engineering and Technology

SECTION 1: PORT CYBER SECURITY DETAILS	Enter local information below
Name of Port or Facility	
Name of operating company	
Full postal address	
General telephone and e-mail contact details	
Name of Cyber Security Officer (CySO)	
Cyber security training courses undertaken	
Date:	
Location:	
Training Provider:	

CySO contact details
Postal address:
Telephone:
Fax:
E-mail:

SECTION 2: MANAGEMENT OF CYBER SECURITY	
Brief summary of port cyber operations, including port control and administration, security control and administration, customs and border control, cargo reception handling and storage, supply chain facilities and any unusual characteristics. This needs to be a holistic approach covering people, processes, physical and technological aspects of the port's assets.	*These details can be copied from Part 2 of the port Cyber Security Assessment (CSA) or be completed in new or greater detail in this section, depending on your needs and preference*
Port Cyber Security Committee or Port Cyber Security Authority	*Each port or facility should have some authority that has an overarching responsibility for cyber security. A Port Cyber Security Committee provides a mechanism for: aiding communications regarding the flow of responsibility; sharing of security-related information; increasing overall accountability; and the embedding of security-minded behaviour into day-to-day operations.*
Name and company details (where applicable) of Committee/ Authority Chair / Port Cyber Security Authority	
Names of organisations permanently represented at the Committee/ Authority	*This could be several organisations such as port facilities within a single port, or several ports within a group or a single port*

© The Institution of Engineering and Technology

SECTION 2: MANAGEMENT OF CYBER SECURITY	
General procedures for convening the Committee/Authority	
Procedures for convening the Committee/Authority at times of heightened vulnerability	
Procedures for recording Committee/ Authority meetings, circulating minutes and informing members of actions required	
Port Cyber Security Operations Centre (PCSOC)	*A PCSOC acts as a centralised unit dealing with cyber security issues affecting a port or port facility. Cyber integrity can only be maintained with effective monitoring of potential, emerging and actual threats to the port or port facility cyber operations. Observation includes detection of unauthorised changes to port systems or port data, unsecure modes or operation and unauthorised access to port assets. Should a risk be identified, proactive measures should be taken to reduce the risk to an acceptable level by denying further access to port assets or by identifying suitable countermeasures. This is the role that a PCSOC undertakes.*
Location details	
Procedures for receiving and disseminating vulnerability information to relevant staff	
Personnel with Cyber Security Duties	*The roles and structure of port facility personnel with cyber security responsibilities (preferably a flow diagram)* *[Insert diagram]*
Duties and responsibilities of the CySO, including details of working hours allocated to cyber security matters	*List of cyber security duties of permanent port facility personnel (other than the CySO or details shown in flow diagram)*
Details of cyber security contractors (if applicable) and their contracted duties	

© The Institution of Engineering and Technology

SECTION 2: MANAGEMENT OF CYBER SECURITY	
CSP Review, Amendment and Audit	
CSP review procedures (Code 5.1), CSP amendment procedures and CSP audit procedures (Code 5.2)	*Insert the details of the mechanism for performing ad-hoc risk reviews to identify and assess the impact of any changes on port assets and to update the Cyber Security Assessment (CSA)*
Response to and Reporting of Cyber Security Threats, Incidents and Breaches of Cyber Security	*Insert procedures for responding to cyber security threats or breaches of cyber security, including details and links to other Port Emergency / Contingency Plans and how the CSP interacts with them* *Insert procedures for the recording of cyber security incidents* *Insert cyber security incident investigation procedures*
Details for reporting procedures to National Cyber Security Centre (https://www.ncsc.gov.uk) and other relevant authorities	*Insert list of organisations that will assist the port/port facility in the event of a cyber security incident*

The section of the CSP that addresses security breaches and incidents should enable an effective and co-ordinated response. This will require an assessment of potential risks to the port/port facility, its function, port assets, personnel and third parties in the event of a security breach or incident. The section should include:

(a) forensic readiness measures required to enable the capture of forensic information about an incident for use by law enforcement and for detailed analysis of the root causes of the incident;
(b) the process to be followed on discovery of a security breach or incident (including near misses – that is, narrow avoidance of a security breach or incident);
(c) business continuity measures required in the event of port system failure, impairment or non-availability, noting what alternative measures can be employed and what impact the incident has on the capacity at which the port can realistically operate;
(d) disaster/incident recovery actions required in the event of serious failure scenarios;
(e) steps to be taken to contain and recover from the event;
(f) the review process following a security breach or incident, including both an assessment of any ongoing risk and an evaluation of the response to the breach or incident by the port/port facility and, where appropriate, the supply chain;
(g) the need for contractual provisions to handle breaches/incidents caused by a third party connected to the port, for example, a professional advisor, contractor or supplier;
(h) mechanisms for reviewing and updating the CSA, CSP and security procedures following a significant security breach or incident at the port or one of its port facilities;
(i) mechanisms for reviewing and updating the CSA, CSP and security procedures following a significant security breach or incident at another port/port facility; and
(j) arrangements for conducting cyber security incident response exercises, which the port/port facility may handle in conjunction with existing business continuity planning and exercises.

© The Institution of Engineering and Technology

CSP security breaches and incidents response

Insert details of:

Forensic readiness measures
Breach/incident discovery processes
Business continuity measures
Disaster/incident recovery actions
Contain and recover steps
Review process
Contractual provisions to handle breaches/ incidents
Reviewing and updating mechanisms at your port/facility
Reviewing and updating mechanisms at another port/facility
Arrangements for conducting cyber security incident response exercises

Information Security

Security procedures for hard copy information considered security sensitive

Storage for hard copy information considered security sensitive

Port control and administration information

Insert details of:

- *cyber security drills to be practiced testing the port's response to cyber security incidents;*
- *cyber security of communications between personnel with security responsibilities;*
- *cyber security of communications between those responsible for technical security and the wider security team;*
- *cyber security of communications between those providing information about the port and port assets to third parties;*
- *access control measures relating to cable ducts, trunking and cabins of equipment boxes located within the port, irrespective of whether they are in restricted or open areas; and*
- *access control measures to sensitive IT systems and accommodation, for example, networking, communications and server rooms.*

© The Institution of Engineering and Technology

Security control and administration
Insert details of: • *maintenance procedures for the cyber security of security and communications systems and equipment;* • *the management of any changes to systems or system operations required at higher security levels, including any increased security measures required for admission of IT and systems maintenance contractors to the port and port facilities when the port is operating at security levels 2 and 3;* • *cyber security of port lighting, electronic access, security and monitoring systems, and any specialist systems required to support security patrols or law enforcement authorities, for example, radiation detectors; and* • *cyber security awareness and training required by staff .*
Cargo reception handling and storage
Insert details of: • *cyber security measures required for any connection between ship systems and those of the port/port facility;* • *processes and procedures for approving the electronic or wireless connection of ship and port systems;* • *cyber security measures pertinent to the protection and assurance of cargo related data and the systems that process, store and transmit it. Where the port has automated systems handling cargo movement or storage, the plan should address the security measures required to protect the operational IT and cyber physical systems; and* • *cyber security measures pertinent to the protection and assurance of ships' stores and bunkering data and any systems that process, store and transmit it*
Supply chain facilities
Insert details of contractual measures for the adoption of relevant cyber security measures within the supply chain to the port/port facility

Security needs to be retained at senior levels within the supply chain, with responsibility delegated appropriately to ensure effective management.

Insert details of communication links between port facility personnel with security duties and insert details of the following contacts, so that you have access to them in the event of a disturbance to your cyber systems in the table below.

SECTION 3: COMMUNICATION
Port Facility Communication Links (PFSI Ch4)
Response Agencies and Control Authorities

© The Institution of Engineering and Technology

SECTION 3: COMMUNICATION
National Cyber Security Centre
Contact name:
Address:
Telephone number:
24 hr. telephone number:
Fax:
E-mail:
Department for Transport
Contact name:
Address:
Telephone number:
24 hr. telephone number:
Fax:
E-mail:
Police
Contact name:
Address:
Telephone number:
24 hr. telephone number:
Fax:
E-mail:
Other
Name of authority:
Contact name:
Address:
Telephone number:
24 hr. telephone number:
Fax:
E-mail:

SECTION 4: Any miscellaneous information
This section should be used if you wish to provide any additional information you feel is relevant to the cyber security of your port or port facility that is not recorded elsewhere.

© The Institution of Engineering and Technology

APPENDIX D

Identifying and implementing mitigation measures

This Appendix provides a framework for the identification of mitigation measures to be applied to the people, physical, process and technological aspects of a port/port facility. When choosing mitigation measures, a balance will need to be struck on a case-by-case basis between optimum risk reduction and minimising the overall impact on the business of the port/port facility.

D.1 People

People are often the weakest element in any secure system or operation and the interaction of people with the port systems needs to be understood. It is advised that the answers to the following questions are established as the first stage in the process of deciding upon the appropriate and proportionate mitigation measures:

(a) who needs access to the port data and systems?
(b) what types of access are required?
(c) how is this access provided, and is remote access required?
(d) what access controls will be required (for example, can an individual create, read, update or delete the port data, and what level of control does an individual have)?
(e) what level of cyber security awareness and understanding of cyber security is required by individuals?
(f) are contractors and temporary and agency staff provided with cyber security awareness training as part of their induction?
(g) do individuals understand the port operator's policies, processes and procedures for the creation, use and maintenance of port data and the operation and maintenance of port systems?
(h) are methods in place to update individuals about any changes in policies, processes and procedures?
(i) are individuals briefed in a timely manner on changes in threats, risks and the required countermeasures?
(j) are port service operators and container transport companies aware of the threat posed by GNSS jammers?
(k) are rules in place around the use of removable media?

The answers to the first four questions will also enable the port and port facility to identify high-risk positions. The individuals holding those positions should be subjected to appropriate pre-employment/pre-contract security screening and vetting checks, with appropriate ongoing monitoring.

High-risk positions will include those with:

(a) IT or operational system administration responsibilities;
(b) security roles;
(c) information management roles;
(d) purchasing, finance and contract management roles; and
(e) personnel management roles (regarding handling of security-breach-related disciplinary matters and management of the insider threat).

© The Institution of Engineering and Technology

D.2 Physical

To enhance the achievable level of cyber security, it is necessary to have in place physical security that:

(a) prevents unauthorised access to sensitive port systems, for example:
- **(i)** IT equipment accessing, processing or storing sensitive information;
- **(ii)** systems fulfilling critical port functions; and
- **(iii)** port security and control systems;

(b) prevents theft of, or damage to:
- **(i)** IT equipment, storage media, cables, etc.;
- **(ii)** port data, in particular, that pertaining to the safe and secure operation of the port; and
- **(iii)** systems that can detect and locate the use of GNSS jammers;

(c) protects network and communications infrastructure from:
- **(i)** accidental damage;
- **(ii)** deliberate/malicious damage; and
- **(iii)** tampering, GNSS jamming or denial of service; and

(d) protects the utilities, heating, ventilation and cooling systems required to:
- **(i)** operate the sensitive port systems;
- **(ii)** operate the network and communications infrastructure; and
- **(iii)** maintain a safe and secure working environment.

Some port systems may need to be accorded the same level of physical protection as key operational spaces, with security perimeters defined and implemented to protect not only the systems, but also their cabling and any associated plant and machinery.

It will therefore first be necessary to establish:

(a) what physical and electronic infrastructure is used to create, access, process and store port data, including any communications and networking components;
(b) the infrastructure that is critical to ensuring the ongoing operation of port systems and any processes or services they support;
(c) the dependencies that parts of the infrastructure have on other critical services or infrastructure;
(d) the extent to which this infrastructure is dedicated to port systems or shared with different activities;
(e) the extent to which this infrastructure is shared with third parties; and
(f) the availability of port personnel and external agencies for reaction and response and their ability to access the functional areas.

This information should then be used to decide where physical protective measures are required.

Where it is decided that secure perimeters are needed, these should be designed to prevent unauthorised access or tampering and, depending on the location and criticality, may need to be alarmed and monitored. When considering the level and type of protection to be provided, a defence-in-depth approach is more reliable than a single protective barrier.

© The Institution of Engineering and Technology

Process

The failure to develop and maintain appropriate policies and their supporting processes that reflect the operating culture of the organisation can result in them being ignored, or lead to the adoption of informal local practices, with the security or operation of the site or key port assets being undermined.

It is therefore important that processes specific to cyber security are in place, which, as a minimum, detail:

(a) the use of externally hosted systems or business portals employing web-based interfaces.
(b) communications and networking links, whether from externally hosted systems or services, or those hosted at the port.
(c) wireless networking and communications technologies, for example, Bluetooth and Wi-Fi.
(d) the configuration of protective software, such as firewalls, anti-malware products and intrusion detection applications.
(e) the connection of new computers, mobile devices or IT-controlled operational equipment to the port's IT infrastructure.
(f) the use of personal mobile radios (PMR) within the port.
(g) the configuration and management of user and systems account privileges, including those of third party personnel with access to port systems, particularly those controlling power, heating, ventilation and cooling systems for accommodation containing on-site IT systems, or port security systems, for example, access control, security barrier control, CCTV, etc.
(h) the connection of personal IT devices or removable media to port systems.
(i) access to emails, instant messaging services, external websites or file sharing services from workstations on operational systems (control systems, security systems, etc.).
(j) mobile time-critical access to data during an emergency. It will also be necessary to have processes in place for:
  (i) regularly reviewing access privileges to ensure that individuals' privileges are consistent with their job roles and functions; and
  (ii) regularly reviewing systems logs and the investigation of anomalies.

D.3 Technological

In deciding upon technical mitigation measures that are needed to address cyber security risks, it will first be necessary to gain an understanding of:

(a) the systems in use (including GNSS tracking technology);
(b) the channels used by systems, sensors and actuators to communicate;
(c) the segregation and touchpoints of non-corporate networks; and
(d) the information and data held.

© The Institution of Engineering and Technology

Systems may operate across a whole port, within a single port facility or across several facilities. They may be located on-site or hosted remotely, for example, as a cloud service or within a data centre. To establish the nature of systems in use, the following questions will need to be answered:

(a) what port systems are involved in the creation, use, maintenance, storage and transmission of port data?
(b) to what extent are each of these systems dedicated to a single port/port facility?
(c) are the port systems shared by different activities?
(d) are the systems accessible by any third parties, either within or outside the port?
(e) what is the typical operating life of each system?
(f) when is it likely that each system will become unsupportable, obsolete or need to be replaced for business or operational reasons?

The channels by which systems, sensors and actuators communicate can be vulnerable to attacks and interference. The answers to the following questions should therefore be sought:

(a) what channels, technologies and parts of the overall spectrum are used to communicate and share port data between port systems and with any users who need to access or use it?
(b) what channels, technologies and parts of the electromagnetic spectrum are used to control and integrate port systems?
(c) to what extent are the communications confined to the port/port facility, and will remote access to, or remote processing of, communications be required?

The information and data that is created, used or processed by the port systems needs to be understood. To do this, the answers to the following questions should be established:

(a) what information and data, including sensor data, do the port systems require to function?
(b) what other information and data is held, for example, personally identifiable information?
(c) what legal requirements are there with regard to the information and data held?
(d) how is information and data encoded?
(e) how and where is information and data stored?
(f) what will the consequences be if information or data is lost and therefore no longer available?
(g) who owns the information and data?
(h) how is information and data made available and what restrictions are there on its use?
(i) how long does information and data need to be kept?
(j) what information and data needs to be securely removed when no longer required?
(k) is a data classification policy in place?

When designing, procuring, implementing and operating physical security systems that operate using IT networks, the port or port facility operator should consider how the systems will be protected from cyber security attacks or incidents. This is particularly important given the trend of convergence of physical security and IT infrastructure, for example, the use of a shared enterprise network and access to security systems from the corporate desktop environment.

© The Institution of Engineering and Technology

Where such convergence occurs, or has occurred, the port/port facility operator should ensure that:

(a) an appropriate architecture is employed;
(b) appropriate management, support and maintenance is available from both the port's IT team and the system vendors, to maintain system security and performance;
(c) appropriate protection is provided to prevent IT control and security systems becoming infected with malware; and
(d) wherever possible, the critical security systems operate over a segregated infrastructure.

D.4 Resilience

Resilience is the ability to adapt, respond and recover rapidly from disruptions and maintain continuity of business operations.

In the event of an incident, it is vital, from a business perspective, that a port can operate without disruption or compromise of the services provided to its users.

A port should therefore have in place an incident management plan that is based upon an understanding of:

(a) the potential causes of disruption, both human and natural;
(b) the essential systems required to keep the port operating safely;
(c) the nature and practicality of alternative methods that can be employed to maintain operations in the event of an incident; and
(d) the capacity at which the port can realistically operate under such arrangements.

It will also be necessary for the port to have in place systems and processes that enable the timely detection of disruptive events, to enable the correct response, as set out in the incident management plan, to be initiated as quickly as possible.

Emergency plans should be exercised on a regular basis to test communication, co-ordination, resource availability, procedures and response. The exercises may be:

(a) full-scale or live;
(b) table-top simulation or seminar; or
(c) combined with other resilience exercises, such as emergency response, etc.

© The Institution of Engineering and Technology

© The Institution of Engineering and Technology

APPENDIX E

Model terms of reference for a Port Security Committee (PSC) or Port Security Authority (PSA)

At the port level, there will be a need to establish clear communications between key stakeholders, including those responsible for operating both the port and port facilities and a few external stakeholders. Such stakeholders may include government organisations operating within the port and local law enforcement agencies. By establishing a PSC or PSA, those responsible for the development and implementation of security policies, processes and procedures will have a representative group who can review documents and advise on the practical aspects of their implementation.

The PSC/PSA should consist of representatives from the port/harbour authority, the port facilities within the port, government organisations operating within the port, local law enforcement agencies, those employed in the port and port users. This provides a mechanism for: aiding communications related to the flow of responsibility; sharing of security-related information; increasing overall accountability; and the embedding of security-minded behaviour into day-to-day operations.

The terms of reference for a PSC could typically include:

(a) promoting a security-minded culture throughout the port;
(b) designing and evaluating security-awareness programmes;
(c) identifying security threats: physical, people, process and technology-related;
(d) reporting and assessing recent security incidents at the port;
(e) assessing the potential implications of security incidents at other ports;
(f) enhancing co-ordination in the application of security procedures and countermeasures;
(g) planning, co-ordinating participation in and evaluating security drills and exercises;
(h) co-ordinating port and port facility security assessments (PFSA) and cyber security assessments (CSA);
(i) co-ordinating, communicating and facilitating implementation of applicable security measures specified in the PSP and the CSP; and
(j) sharing best practice and experience in the implementation of security plans.

The DfT's UK maritime security measures include further requirements relating to PSCs and PSAs.

© The Institution of Engineering and Technology

© The Institution of Engineering and Technology

APPENDIX F

Handling release of information to third parties

There are several situations where a port/port facility may be asked or required to publish information about its plans and operations. These can include provision of information to support a planning application, release of information to regulators, and presentations about the port or port facility. The operator of the port or port facility needs to be aware that public release of information can enable a party undertaking hostile reconnaissance to obtain sensitive information or, through data aggregation, to deduce sensitive information.

Where a port falls within the scope of regulations or legislation requiring public disclosure of information, for example, Planning Regulations, Environmental Information Regulations or Freedom of Information legislation, the CySO should ensure that the CSP details the approach to be taken to protect sensitive data or information. As a minimum, the approach should:

(a) consider the impact of releasing data, including the potential issues arising from data aggregation;
(b) prevent leakage of security-related information;
(c) protect commercially sensitive data and intellectual property; and
(d) safeguard personally identifiable information, considering the range of attributes that can be used to identify individuals.

Based on an assessment of the risk of disclosing detailed information about the port or a port asset, it might be necessary and appropriate to adopt measures to reduce the detail. Such measures might include:

(a) limiting access to certain types of port data;
(b) redacting sensitive information, for example, description of the functions of individual port facilities or components of them;
(c) providing the information in an unstructured format[1]; and
(d) sanitising metadata associated with documents.

1 Use of unstructured formats such as hard copy, images, and non-interactive PDF formats may reduce the risks associated with data aggregation, making it more difficult to search for specific terms or to develop associations between data items that relate to sensitive aspects of the port/port facility.

© The Institution of Engineering and Technology

© The Institution of Engineering and Technology

APPENDIX G

Handling security breaches and incidents

It will be necessary for the port and port facility to have in place appropriate measures that can be implemented in the event of an incident to reduce its impact on the port's operations and to aid recovery. These are likely to include:

(a) incident response plans, which include liaison, where appropriate, with the NCSC, ICO (GDPR), Action Fraud or CA (if under NIS);[1]
(b) communication plans to reassure and inform stakeholders, during and after any incident or breach, as well as handling any third party, regulator, media or public interest issues;
(c) risk assessment and mitigation plans to enable the impact to be assessed over both the short and medium to longer terms; and
(d) disaster recovery and business continuity plans affording the same level of security for the port data as the processes and systems in use on a day-to-day basis.

It will also be necessary for consideration to be given as to when and how forensic evidence will be preserved to aid any investigation into the cause of the event or the perpetrators. Where evidence collection is for law enforcement purposes, it should be in accordance with the relevant national guidelines.[2]

In the event of an incident involving the loss or theft of port data, unauthorised access to port data or systems, or interference with computer systems, the CySO should notify the relevant parties[3] and law enforcement agencies.

When identifiable personal information is lost, stolen or compromised, the CySO should ensure that the relevant information commissioner or data protection authority,[4] and the affected individuals, are notified.

The CySO should ensure that discovery procedures are established in all appointment documents and contracts, including, where applicable, in non-disclosure agreements.

Following any security breach or incident, an important post-incident activity is the formal evaluation of the way the event was handled, to determine lessons that can be learned and to review whether any changes are required to the security assessments, security plans or supporting policies, processes and procedures.

---

1 The NCSC [https://report.ncsc.gov.uk/] has four main responsibilities that flow from the UK's Cyber Security Strategy: national cyber security incident management; support to critical national infrastructure companies to handle cyber security incidents; promoting cyber security situational awareness across industry, academia and the public sector; and providing the single international point of contact for co-ordination and collaboration between UK NCSC and comparable international agencies.

2 In the UK, these are found in the Association of Chief Police Officers (ACPO) Good Practice Guide for Digital Evidence (2012), which is available from https://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf.

3 In the UK, incidents affecting ports covered by the ISPS Code or by the International Labour Organisation (ILO)/International Maritime Organisation (IMO) Code of Practice on security in ports should in the first instance be notified to the NCSC.

4 In the UK, incidents involving the loss or compromise of personally identifiable data should be notified to the Information Commissioner (https://ico.org.uk/).

© The Institution of Engineering and Technology

© The Institution of Engineering and Technology

APPENDIX H

Bibliography

This Appendix lists standards that are relevant to the design and operation of information and communications systems used in the management and operation of the port environment. It should be noted that this list is not exhaustive and references may become obsolete over time.

H.1 General IT and cyber security standards

Reference	Title/Description
ISO/IEC 13335	*IT Security Management – Information technology – Security techniques – Management of information and communications technology security*
ISO/IEC 15408	*Common Criteria for Information Technology Security Evaluation*
ISO/IEC 27000	*Information security management systems – Overview and vocabulary*
ISO/IEC 27001	*Information security management systems requirements*
ISO/IEC 27002	*A code of practice for information security management*
ISO/IEC 27003	*Information security management system implementation guidance*
ISO/IEC 27004	*Information security management – Measurement*
ISO/IEC 27005	*Information security risk management*
ISO/IEC 27006	*Requirements for bodies providing audit and certification of information security management systems*
ISO/IEC 27007	*Guidelines for information security management systems auditing*
ISO/IEC TR 27008	*Guidance for auditors on ISMS controls*
ISO/IEC 27010	*Information security management for inter-sector and inter-organisational communications*
ISO/IEC 27013	*Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1*
ISO/IEC 27014	*Information security governance*
ISO/IEC 27017	*Code of practice for information security controls based on ISO/IEC 27002 for cloud services*
ISO/IEC 27018	*Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*
ISO/IEC 27031	*Guidelines for information and communication technology readiness for business continuity*
ISO/IEC 27033-1	*Network security – Part 1: Overview and concepts*
ISO/IEC 27033-2	*Network security – Part 2: Guidelines for the design and implementation of network security*

© The Institution of Engineering and Technology

Reference	Title/Description
ISO/IEC 27033-3	*Network security – Part 3: Reference networking scenarios – Threats, design techniques and control issues*
ISO/IEC 27033-5	*Network security – Part 5: Securing communications across networks using Virtual Private Networks (VPNs)*
ISO/IEC 27035	*Information security incident management*
ISO/IEC 27036-3	*Information security for supplier relationships – Part 3: Guidelines for information and communication technology supply chain security*
ISO/IEC 27037	*Guidelines for identification, collection, acquisition and preservation of digital evidence*
Supplier Information Assurance Tool (SIAT) – Summary	*A brief summary of the Supplier Information Assurance Tool (SIAT) Community of Interest set up to drive development of a supplier Information Assurance model. ISAB Approved.*
NCSC Cyber Essentials	*Cyber Essentials is a simple but effective, Government backed scheme that will help you to protect your organisation, whatever its size, against a whole range of the most common cyber attacks. See: https://www.cyberessentials.ncsc.gov.uk*

H.2 Security and safety of Industrial Control Systems (ICA & SCADA)

Reference	Title/Description
IEC 61508	*An international standard published by the International Electrotechnical Commission consisting of methods on how to apply, design, deploy and maintain automatic protection systems called safety-related systems.*
IEC TS 62443-1-1	*Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models*
IEC 62443-2-1	*Industrial communication networks – Network and system security – Part 2-1: Establishing an industrial automation and control system security program*
IEC TR 62443-2-3	*Security for industrial automation and control systems – Part 2-3: Patch management in the IACS environment*
IEC 62443-2-4	*Security for industrial automation and control systems – Part 2-4: Security program requirements for IACS service providers*
IEC TR 62443-3-1	*Industrial communication networks – Network and system security – Part 3-1: Security technologies for industrial automation and control systems*
IEC/TS 62443-3-2 Ed. 1.0	*Network and system security – Part 3-2: Technical requirements – Target security levels*
IEC 62443-3-3	*Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels*
ANSI/ISA-99.00.01	*Part 1: Terminology, Concepts, and Models*
NIST IR 7176	*System Protection Profile – Industrial Control Systems – V1.0* Incorporates industrial control systems into Common Criteria
NIST SP 800-82	Guide to Industrial Control Systems (ICS) Security
IEC 61508	Functional Safety if Electrical/Electronic/Programmable Electronic Safety-related Systems

© The Institution of Engineering and Technology

H.3 Business-related security guidance

Reference	Title/Description
Board Toolkit	*Cyber risk management: a Board-level responsibility. Explains the benefits of cyber risk management to senior executives.* *(For further information, see* https://www.ncsc.gov.uk/collection/board-toolkit
ISO 20000 BS 15000	*IT Service Management Standards* based on ITIL.
BS 7858	*Code of Practice for Security Screening of Individuals Employed in a Security Environment*
COBIT 5	A Business Framework for the Governance and Management of Enterprise IT (Control objectives for information and related technology.)
PAS 555:2013	*Cyber security risk. Governance and management. Specification*

H.4 Other standards and guidance

Reference	Title/Description
PCI DSS	*Payment Card Industry Data Security Standard*
NIST SP 800-61	*Computer Security Incident Handling Guide*
PAS1192-5:2015	*Specification for security-minded building information modelling, digital built environments and smart asset management*
PAS 754:2014	*Software Trustworthiness. Governance and management. Specification*
PAS 97:2012	*A specification for mail screening and security*
RFC 2196	*Site Security Handbook* From IETF (The Internet Engineering Task Force)
RFC 2350	*Expectations for Computer Security Incident Response* From IETF (The Internet Engineering Task Force)
DfT Guidance Version 1.1	*Implementation of the NIS Directive* *An overview of the implementation of the Network and Information Systems Directive (the NIS Directive) in the transport sector.*
BS ISO/IEC 42010	*Systems and software engineering – Architecture description*
	EACOE Enterprise Framework
	IET Code of Practice for Cyber Security in the Built Environment

© The Institution of Engineering and Technology

© The Institution of Engineering and Technology

Good Practice Guide

Cyber Security for Ports and Port Systems

A number of incidents at European ports have significantly raised the profile of cyber security and the risks associated with the complex systems used by port owners and operators. To help senior port personnel address this emerging security issue the Institution of Engineering and Technology (the IET) have worked in close association with the Department for Transport (DfT) and the Defence, Science and Technology Laboratory (Dstl) to produce this new Guide.

This Good Practice Guide provides actionable good practice advice on areas such as:

- Developing a cyber vulnerability assessment and plan
- Devising the most appropriate mitigation measures
- Having the correct structures, roles, responsibilities and processes in place
- Handling security breaches and incidents
- Highlighting the key national and international standards and regulations that also need to be reviewed and followed

This new guidance will be of real value to all those responsible for security and business continuity in ports and can be used as an integral part of an organisation's overall risk management system.

The Institution of Engineering and Technology
Michael Faraday House
Six Hills Way
Stevenage
Herts
SG1 2AY

theiet.org/standards