MARITIME CYBER SECURITY

MARKO OSTRIC
DAVOR SVAST

Foreword

The shipping industry forms the basis of the development economies of countries around the world. With the growth of the global market, the need for freight transport also grew, and maritime transport gained in importance. As the main force of world trade, ships play an important role in all above-mentioned and have become the most common means of transportation. Accordingly with market growth and demand for larger ships, grew also the need for qualified personnel on ships.

Due to the highly responsible and the variety of required work on ships, officers have to be ready at any moment to adequately respond to all the challenges that appear. A part of them lies in the growing threat to maritime cyber security. In the upcoming years cyber security will present new challenges for both shipowners and crews.

This guide is primarily addressed to all those who will operate ship's IT systems and to those who primarily care for ships' cyber security, both on board and on shore. It is adviseable to get familiar with all the possible threats so it would be easier to avoid them and be prepared in case some potentially hazardous situation appears.

1 Cyberspace and Cyber Security 12
1.1 What is Cyberspace? 12
1.2 Cyberspace vs. Physical World 13
1.3 Cyber Security and Cyber Laws 14
1.4 Cyber Law 16
1.5 Cyber Security Myths & Reality 17
1.6 Social Engineering 19
2 Phishing 25
2.1 Phishing Attack Examples 26
2.2 Phishing Techniques 28
2.3 Spear Phishing 29
2.4 How to Prevent Phishing 30
3 Malware 31
3.1 How to Recognize and Detect Malware 31
3.2 How to Remove Malware from Your Computer 32
3.3 Types of Malware 33
4 Phishing Prevention 41
4.1 How Can You Identify a Phishing Email? 42
4.2 Phishing Prevention Best Practices 44
4. 3 Spear Phishing vs. Phishing 46
5 How to Prevent Malware from Infecting Your Computer 48
6 Use of Strong Passwords 49
7 Keep Your Business Safe from Cyber Threats 53
7.1 Back Up Data 53
7.2 Secure Your Devices and Network 54
7.3 Encrypt Important Information 56
7.4 Ensure You Use Two-Factor Authentication (2FA) 56
7.5 Manage Passwords 57
7.6 Administrative Privileges 57
8 What to Include in Your Cyber Security Policies? 59
8.1 Set Password Requirements 60
8.2 Outline Email Security Measures 60
8.3 Explain How to Handle Sensitive Data 61
8.4 Set Rules Around Handling Technology 61
8.5 Set Standards for Social Media and Internet Access 62

8.6 Be Prepared for an Incident 63
8.7 Prepare a Cyber-Security Incident Response Plan..... 63
8.8 Prepare and Prevent 64
8.9 Check and Detect 64
8.10 Identify and Assess 65
8.11 Respond..... 65
8.12 Review 66
9 Types of Hackers.....67
9.1 What is a Script Kiddie? 67
9.2 Should You Worry About Script Kiddies? 67
9.3 Hackers..... 68
9.4 Black Hat Hackers 69
9.5 White Hat Hackers..... 70
9.6 Grey Hat Hackers..... 70
10 Phishing Examples.....71
11 Mobile Security Threats.....72
11.1 Data Leakage..... 72
11.2 Unsecured Wi-Fi..... 74
11.3 Network Spoofing..... 74
11.4 Phishing Attacks 75
11.5 Spyware..... 75
11.6 Improper Session Handling..... 76
12 Introduction to Maritime Cyber Security 77
13 IT and OT Systems 81
14 International Rules and Guidelines.....82
14.1 Plans and Procedure..... 84
15 Company Risk Assessment Procedure.....87
15.1 Third-Party Access..... 92
15.2 Impact Assessment..... 95
15.3 Third-Party Risk Assessment..... 97
15.4 Risk Assessment Process 98
16 Risks Related to Ship-Port Interface.....103
16.1 Shutdown of Operations, Port Paralysis 103
16.2 Human Injuries or Death, Kidnapping..... 104
16.3 Sensitive and Critical Data Theft..... 104

16.4 Cargo and Goods Stealing 104
16.5 Illegal Trafficking 105
16.6 Financial Loss and Costs 105
16.7 Fraud and Money Stealing 105
16.8 Systems Damages or Worst, Destruction 105
16.9 Tarnished Reputation, Loss of Competitiveness 106
16.10 Environmental Disaster 106
17 Assessment of Identified Cyber Risks 109
17.1 Effective Response 109
17.2 Recovery Plan 112
17.3 Losses Arising from a Cyber-incident 114
18 Identify Threats and Vulnerabilities 115
18.2 Stages of a Cyber-Attack 117
18.3 Identify Vulnerabilities 121
18.4 Ship to Shore Interface 126
18.5 Common Vulnerabilities 128
19 Incident Management? 130
19.1 Preparation 130
19.2 Preparing to Handle Incidents 130
19.3 Detection and Analysis 131
19.4 Containment 133
19.5 Resolution and Recovery 135
19.6 Post-Incident Activities 136
20 Emergency Preparation 138
20.1 Business Critical Information 138
20.2 Detection and Containment Methods 139
20.3 Internal and External Stakeholders 139
20.4 Circle of Trust 139
20.5 Fight Bad Tech with Good Tech 140
21 Steps for Cyber Security Plan Preparation 141
22 Onboard Networks 143
22.1 Physical Layout 144
22.2 Network Management 145
22.3 Network Segmentation 145
22.4 Monitoring Data Activity 148

22.5 Protection Measures 149
25 Acknowledgements **..... 156**
26 LITERATURE 157