VICREVI COMMUNICATION

Market: UK
Sector: Maritime
Focus: Cyber Security Awareness
May 2019

Client: Swedish cyber security provider

Note: This is an abridged version of a longer report prepared for client

Contents of this Report

Introduction

Maritime transport is a strategically vital and large scale industry in the UK. Freight, passenger and port faciliity services operating 24/7 are of critical importance to the entire economy. The sector is complex and multidimensional with rapidly advancing technological development in some areas but significantly less technical innovation in others. Sub-sectors currently undergoing transformation, including the development of autonomous freight vessels, are high-risk in terms of vulnerability to cyber crime.

Ecosystem clusters in autonomous vessel development have grown strongly in recent years, in many cases linked to existing centres

of academic excellence. Private sector funding of research and development by sector MNE´s and other sources of investment is encouraged by very positive government policy as well as financial grants, in targeted areas of R&D. Support from public sector authorities is an additional positive factor in the growth of advanced technology competence in the maritime sector but much remains to be done in terms of recruitment and training of cyber security personnel in this sector.

---

1 Maritime Industry Structure

- Passenger
- Freight
- Onshore services
- Offshore / Oil & Gas
- Related Services / Business, Legal, Finance & Insurance

2 Facts & Statistics

2.1. Maritime Industry

- 95% of all freight into and out of UK is moved by sea.
- 65 million passengers travel on UK shipping each year.
- Contribution to UK GDP: 10 bn GBP
- Tax Revenues from this sector: 2.5 bn GBP
- Employment (direct & indirect): 240 000

Source: Maritime UK / MUK / https://www.maritimeuk.org/

2.2. Maritime Financial & Brokering Business: Global Market Shares

- Marine Insurance: 35%
- P&I Insurance / Protection & Indemnity: 60%
- Shipbroking: 26%

2.3. Legal Affairs

- UK is global market leader in maritime judicial settlements and legal transactions

2.4. Onshore

- UK Ports freight handling: 500 m tonnes / year
- UK Ports Sector: 120 commercial ports
- UK Ports Ranking: Top 20 ports handle 88% of UK freight traffic
- UK Ports Employment: 118 000

3 UK Government Policy on Cyber Security in CNI / Critical National Infrastructure

3.1. Background

- UK National Cyber Security Council / NCSC created in 2016 by government to upgrade cybersecurity in all CNI / system critical sectors including transportation.
- Government policy objective: "The Safest Nation on Earth to do Business"
- Development of a joint critical systems task force represents a 250 m GBP investment.

3.2. Government requirements placed on business & industry for the protection of CNI / Critical National Infrastructure

- Organizations and company boards are responsible for ensuring the security of all information and communication networks under their control.
- Critical systems must be clearly identified and regularly assessed for vulnerability against the constantly evolving technological landscape and threat patterns.
- Adequate investment must be made in technology and staff to reduce vulnerabilities in current and future systems, and in all related supply chains in order to maintain a level of cyber security proportionate to the risk.
- Capabilities in place must be regularly tested for capacity to respond in the event of a violation of information and communication networks.
- In the case of CNI, those responsible must implement action in respect of all requirements in cooperation with government bodies and regulators.
- Regulators must ensure cyber risk is properly managed and – if it is not – intervene in the interests of national security.

Source: UK National Cyber Security Strategy 2016

4 Cyber Threat to UK Business (All Sectors)

4.1 Areas of Weakness

- Private sector failing to match government policy and initiatives.
- Recent major breaches – British Airways, Marriott Hotels (Starwood), Amazon in the UK
- Cyber Security still a low corporate priority in most sectors.
- Lack of incentives to invest in cyber security.
- Senior management teams in many sectors lack understanding of the digital economy / Industry 4.0

4.2 Needs

- Strategic prioritisation, development of long-term cyber security commitment based on board-level engagement and focus.
- Cyber security must be implemented at every level of every organization due to the nature of the threat.
- This means staff training – Companies must acquire in-house expertise and must upgrade cyber security to strategic priority level.

4.3 Public Sector & Government

- Protection against election hacking etc must be prioritised
- Major focus on financial services and all CNI / Critical National Infrastructure.
- Impact on common crimes: Example: Dramatic increase in car theft via ”intelligent” systems – 34% increase last year.

4.4 Penalties for Negligence in CNI Sectors

- Regulations introduced in 2018 applying to CNI sectors including transportation.
- Companies & organisations can be fined up to 17 m GBP if they ”fail to demonstrate” that their information systems are adequately protected against cyber attacks (source: Maritime Executive)

4.5 Cyber Security Providers in the UK
Complete list of NCSC-approved professional CS service and product providers and other organisations: https://www.ncsc.gov.uk/marketplace

4.6 Cyber Security in the Maritime Sector: Government Report
Future of the Sea – Cybersecurity Dimension / Official Government Report
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/671824/Future_of_the_Sea_-_Cyber_Security_Final.pdf

4.7 Focus areas of the above report

- Communication
- Sensing
- Autonomous Control

4.8 Priority Areas for Cyber Security

- Secure enterprise IT and operational systems
- Robust information and resource access control
- Robust design and deployment of information exchange services and supporting infrastructure to ensure integrity, availability, authentication, and privacy
- Minimum level of user awareness and training to ensure compliance and operational vigilance.

Source: UK National Cyber Security Council / NCSC Report 2017-2018
https://www.ncsc.gov.uk/cyberthreat

5 Maritime Sector - International Dimension
Given the large role of the UK maritime service industry in the global maritime business the facts and developments below are of relevance.

- 50 000 UK-flagged commercial vessels in shipping traffic worldwide
- Navigation equipment and capabilities judged to be highly vulnerable
- The international maritime industry is behind the curve in terms of cybersecurity.
- The sector has been slow to realize the scale and nature of the threat and there is signficant catching up to be done

- The global maritime industry lags other transportation sectors such as aerospace, land-based logistics etc in focusing on cybersecurity.
- The International Maritime Organization / IMO, which is part of the United Nations, issued regulations on cybersecurity, agreed among its members, in 2016.

6 Challenges to Cyber Security in the Maritime Sector

- Extremely large number of vessel categories.
- Wide range of operating systems.
- Computer systems in use are, in many cases, old and not regularly updated.
- Low proportion of fully-trained IS/OS users
- Frequent personnel turnover of crews.
- In many cases no relationship is maintained between crew selection & deployment on the one hand and training in IS/OS on the other
- Lack of training among officers & crew in computer systems and information security.
- Possibly dysfunctional relationship between onboard systems and systems in use by maritime operators.
- ”Always-on” satellite services entail high degree of vulnerability of shipping to the risk of viruses, malware and hacking attacks.
- GDPR and NIS directives bring in common data breach protection notification. All companies & organizations must report data breaches within 72 hours. There are questions regarding the level of awareness of this requirement across the global maritime sector.
- NIS directive requires following: Have the right staff in place and appropriate software to mitigate potential cyber attacks and intrusion. Private and public companies in each sector will be evaluated by regulators who will vet infrastructure and may issue fines for commercial operations which are found to be non-compliant with regulations. Again, questions have been raised concerning the degree of awareness of the above measure across the maritime sector.
- Trained and certified data protection officers should be hired by freight and passenger service operators to ensure compliance.
- Shipping companies with EU-based crews are subject also to Personal Impact Assessments as part of GDPR.
- Port systems are governed by IMO but additional land-based systems in use by maritime operators are outside IMO jurisdiction. Threat: Lack of uniform standards could lead to migration of malware etc. from one system to the other.
- IMO amended two* of their general security maritime codes in 2017 to include cybersecurity. Necessary and welcome but late in taking action on the cybersecurity challenge.
- ISPS and ISM, issued by IMO (see below) regulate how shipping companies and ports should conduct information risk management.

- Cyber security specific amendments of ISPS and ISM come into force in 2021. There remains a lack of urgency. This places the maritime sector somewhat behind, for example, aerospace.
- Cyber security will be fundamental in fully autonomous vessels.
- Conversely slow or weak development of cyber security in maritime could hold back development and deployment of fully autonomous vessels.

7 Opportunities

- Next steps for cyber security providers in maritime: Harmonising equipment requirements with cyber security standards already in force in other sectors.
- CSO Alliance / Company Security Officers Alliance and Airbus Defence & Space have initiated a global cyber security initiative targetting the maritime sector.
- International Ship and Port Facility IMO Security Code / ISPS
- International Security Management IMO Code / ISM
- IMO codes provide guidance in detail on how port and ship operators should structure and conduct risk assessment / risk management processes
- Objective: Make cyber security an integral part of these processes.
- Knowledge gained from cyber security asessments may help IMO develop broader and more comprehensive cybersecurity regulations.

8 Research

8.1 University of Plymouth Maritime Cyber Security Research Group
https://www.plymouth.ac.uk/your-university/about-us/university-structure/faculties/science-engineering/cyber-ship-lab

- University of Plymouth Cyber Ship Lab - A National Resource for Research & Training
- Stakeholders in CSL: Insurers, Shipping Companies, Equipment Suppliers, Classification Societies
- Focus: Logistics, Business, Medical (Psychological aspects to safeguard maritime operations)
- Research Reports – Patterns of threat / cyber risk assessment for autonomous ships / modelling of frameworks for maritime cyber risk assessment / cyber risk policy – scope & impact of evolving technology on global shipping industry
- Also serving MAS / Mayflower Autonomous Ship project – due for completion and launch 2020. World´s first full-sized, fully autonomous, unmanned vessel intended for transatlantic service.
- MAS - https://www.plymouth.ac.uk/business-partners/partnerships/business-partnerships/mas

8.2 IEEE - Autonomous Vessels: Forget Autonomous Cars – Autonomous Ships Are Almost Here.IEEE Spectrum.
http://spectrum.ieee.org/transportation/marine/forget-autonomous-cars-autonomous-ships-are-almost-here

9 Key Contacts

- Harry Theocari, Chair, Maritime UK / Also Global Head of Transport at Legal Practice Norton Rose Fulbright – highly specialised in Maritime Law
- Sarah Kenny, Vice-Chair Maritime UK / Formerly senior manager at defence systems provider QinetiQ
- Mark Sutcliffe, Managing Director, CSO / Chief Security Officers Alliance
- Ciaran Martin, CEO, U.K. National Cyber Security Centre / NCSC
- Kewal Rai, Policy Adviser for Cyber Security with the Department of Transport
- Ben Brabyn, Executive Director, Level39, major technology cluster, based in Canary Wharf, London
- Kevin Forshaw / Director of Industrial & Strategic Partnerships / Faculty of Science & Engineering, Plymouth University & Contact Point for CSL / Cybership Lab
- Keith Martin, Professor & former Director of Information Security Group
- Dr. Rory Hopcraft, Royal Holloway, Univ of London – Conducting research focused on cybersecurity in the maritime sector.
- Walter Hannemann, Product Manager, Dualog Protect UK
- Olivier Surly, Head of Maritime Solutions, Airbus Defence & Space UK

10 News

- Initiative from Maritime Executive – Cyber Security at Sea https://www.maritime-executive.com/blog/cyber-security-at-sea-the-real-threats
- Maritime Cyber Alliance launched - Concept: Connecting all CIS officers in shipping and at ports plus oil & gas terminal operators via a secure & private platform
- Cyber intrusions will be reported instantly and anonymously on this platform.
- Maritime Cyber Alliance members will be provided with threat alerts & all necessary tools to combat malware & update themselves and the organizations they represent on the latest counterattack and prevention actions.
- Maritime Cyber Alliance will offer regular workshops promoting best practice cybersecurity measures.
- Maritime Cyber Alliance will constantly gather and make available to members information on cyber incident reports & statistics.
- Cybership Lab - Open invitation to new partners in continuing development of CSL / Cybership Lab - Contact: Kevin Forshaw / Director of Industrial & Strategic Partnerships / Faculty of Science & Engineering, Plymouth University
- Cybercrime in the Maritime Sector - https://www.cyberscoop.com/maersk-notpetya-300-million-loss/
- Cybersecurity Risk in the Maritime Sector -https://www.maritime-executive.com/blog/cyber-security-at-sea-the-real-threats

- Dualog Expands Market Presence in the UK - https://www.maritime-executive.com/corporate/dualog-takes-cyber-security-to-higher-level-with-dualog-protect
- Cyber security degree apprenticeships. Highly qualified personnel training available now - Contact: Kevin Forshaw / Director of Industrial & Strategic Partnerships / Faculty of Science & Engineering, Plymouth University

11 Events

- CyberUK (Annual Event)/ Glasgow – 24-25 April, 2019 – 2 000 participants- https://www.ncsc.gov.uk/information/cyberuk-2019
- Telegraph Cyber Security Conference, London, May 20-22, 2018 - https://www.idecsi.com/the-telegraph-cyber-security-conference-15-16-may-2018/
- InfoSecurity Europe (Annual Event) / London – 4-6 June, 2019 https://www.infosecurityeurope.com
- Global Conference on Innovation in Marine Technology - https://globalmaritimeconference.org/
- Maritime Cyber Alliance - Regular workshops around the UK - https://maritimecyberalliance.com/news_events

---

Need more information on any item in this report?
Contact us.
info@vicrevi.se /www.vicrevi.se

VICREVI
COMMUNICATION