cyberprism

www.cyberprism.net
contact@cyberprism.net
+44 (0) 207 873 2413

Ports
Cyber Security

Protecting Your Operational Technology and IT from Cyber-Attack

Don't risk the operation of the port, the safety of shipping traffic and the huge potential cost of a cyber-attack

Options available to give different levels of protection and recovery:

- **Cyber Threat Intelligence**
- **Staff Training to reduce human error**
- **OT & IT Protection measures**
- **24/7 Monitoring**
- **Attack Response Plan – be ready**
- **Restore data and operations**
- **NIS Directive compliance**
- **Facilitation cyber insurance cover**

The Threat is Real – the risk of cyber-attack is very high and potentially very damaging. Recent attacks causing major damage affected AP Moller Maersk, Port of Antwerp, Port of San Diego, Long Beach Port and Port of Barcelona and with many other incidents not being reported. Costs can run into hundreds of millions of dollars.

Our Team has worked at the highest level in Government Security Agencies and in the maritime industry. We understand the vulnerabilities of IT and have specialist expertise in the Operational Technology (OT) that operates ports and keeps them safe.

International Ship and Port Facility Security (ISPS) Code (2004): an extension of SOLAS, ISPS is a comprehensive set of measures to enhance the security of ships and port facilities.

Networks and Information Security Directive (2018): the NIS Directive is now UK law and mandates essential service providers (including ports) to take effective cyber security action.

Insurance Exclusions

Cover for cyber-attack is not included in standard insurance policies.

INTERNATIONAL INSTITUTE OF MARINE SURVEYING

WARSASH MARITIME ACADEMY

cyberprism

www.cyberprism.net
contact@cyberprism.net
+44 (0) 207 873 2413

Ports Cyber Security

Cyber Prism Delivering Cyber Security Solutions

Cyber Risk & Threat Assessment

- Identify the specific threat vectors
- Document assets to be protected
- Assess consequences of an attack
- Establish risk tolerance and policy

Surveys

- Survey of critical OT and IT systems
- Critical Assets Register & vulnerabilities
- Access controls & data security
- Staff (insider threat) & supply chain

Protection

- Cyber harden survey vulnerabilities
- OT and IT systems protection
- Networks security, eg ProcessGuard
- Secure Communications

Monitoring, Response & Restoration

- 24/7 monitoring for cyber-attack incidents
- Base systems configuration & backup
- Develop Incident Response Procedure
- Restore data & operations expediently

Training & Compliance

- Port-side and e-Learning Cyber Training
- Cyber-attack on control room simulator
- Policies, Procedures incl. Social Media
- Compliance Reviews & Audits

For more information:
www.cyberprism.net
contact@cyberprism.net

INTERNATIONAL INSTITUTE OF MARINE SURVEYING

WARSASH MARITIME ACADEMY