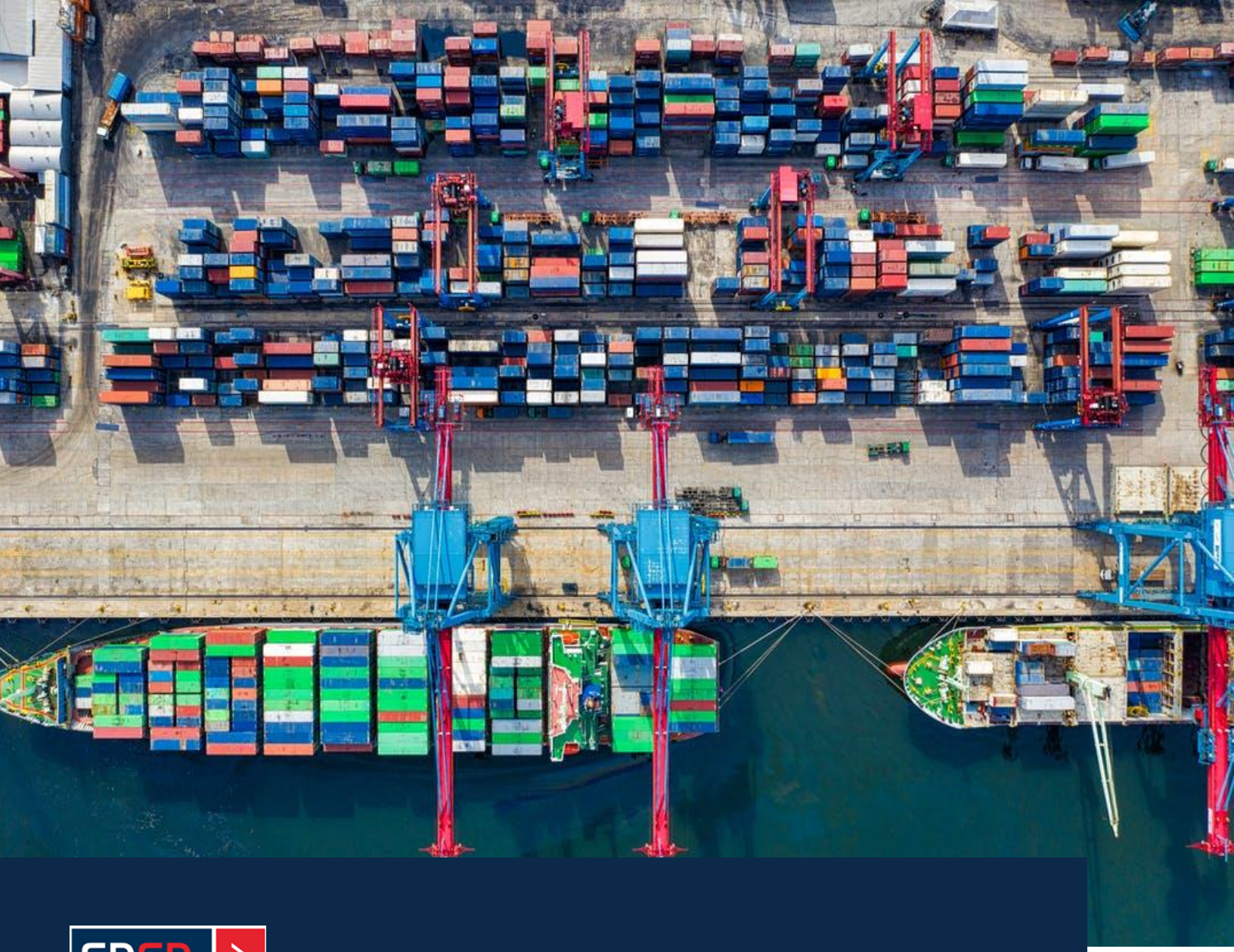


SDSD

SDSD Cyber Security Services

Protect your assets, and get compliance ready and prepared for audit

Cyber Security

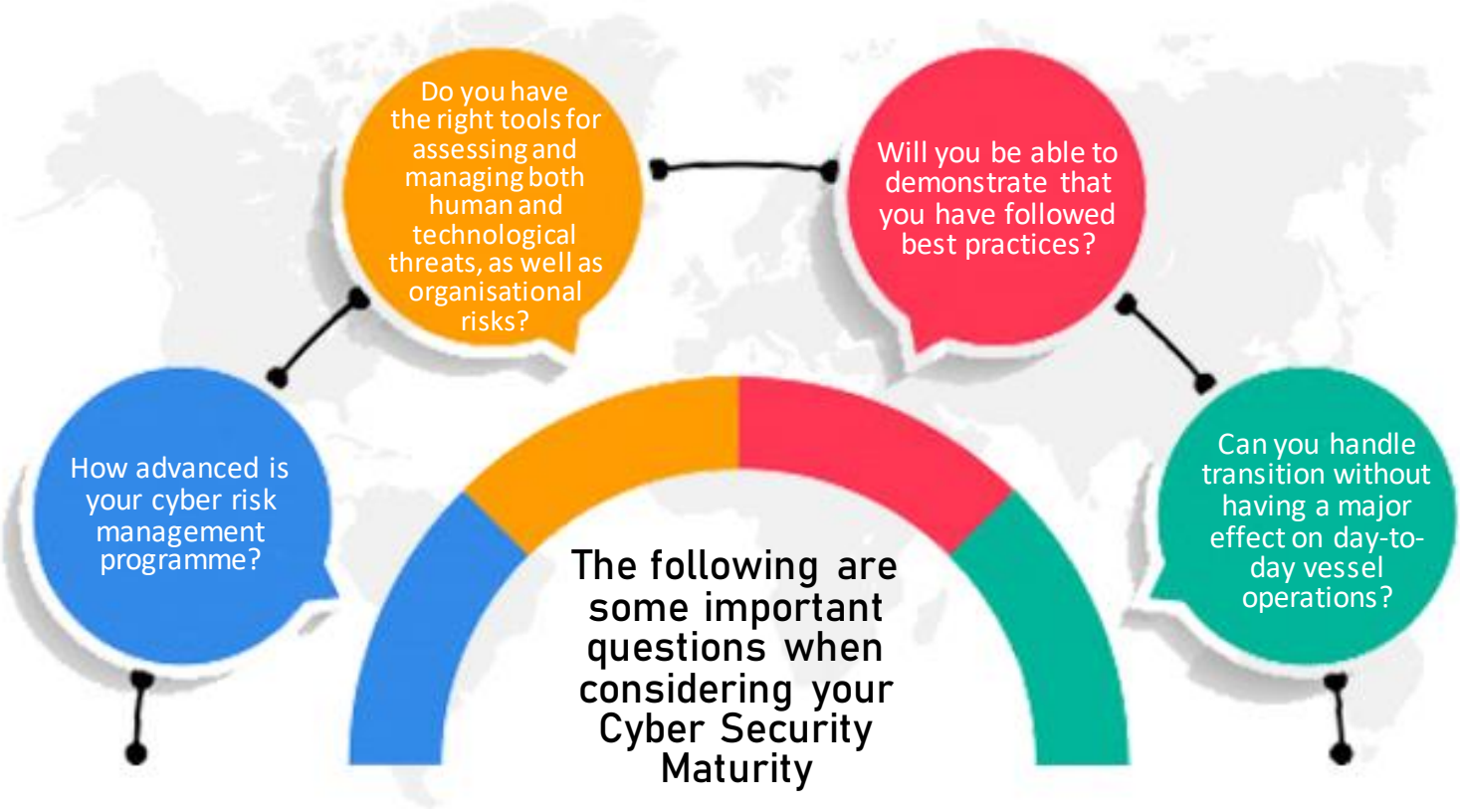
Cyberattacks can have a serious financial and reputational consequence for businesses. However, despite the clear risks within maritime due to increased digitalization and interconnectivity between OT and IT systems, nearly 90% of businesses are still not adequately shielded.

SDSD can help you develop a comprehensive and risk-based approach to effectively protect maritime IT and OT equipment, where threats are detected and managed across the three most important cyber security pillars: people, technology, and processes.

Our process starts with a simple 60-minute check-up to help you understand the cyber-maturity of your organisation. Our Consultants then work with stakeholders across your business to review existing documents and processes, as well as technical spot checks using automated tools to identify the current threat environment and vulnerabilities that could be exploited by malicious actors.

We work to internationally approved standards and frameworks including IMO, BIMCO, TMSA, NIST, ISO27001, and ISO22301, as well as the guidelines and resolutions of various ship classification societies.

We find the gaps and put in place the documentation, processes and risk mitigation measures required for you to keep your business cyber-secure and compliant and ready for audit.



Cyber Readiness Review

Is your Safety Management System fully up to date for an audit? SDSD can help understand your cybersecurity posture and review your readiness.

The readiness assessment is a two-step method for determining your organization's cyber readiness, incorporating standard industry frameworks and the functional elements of IMO guidelines — identify, protect, detect, respond, recover.

Cyber-readiness evaluation:

Engage in a 60-minute cyber security assessment with an SDSD Cyber Security Consultant, focused on the most widely used model in the shipping industry today. The evaluation includes a primer on IMO 2021 enforcement and maritime sector-specific considerations. Get answers to your compliance questions and make sure your cyber security risk plan in good shape.

Readiness with suggestions:

Get a cyber security readiness report with actionable suggestions. Assess your company's compliance with the major cyber security frameworks and get a roadmap for effective improvements and compliance.

Our Services

We tailor our services to help clients meet their compliance and audit needs, our consultants are fully experienced in IMO, BIMCO, TMSA, NIST, ISO27001, and ISO22301 standards. We explore the important impact of technology, procedures, governance, and people to protect your maritime systems – ensuring our recommendations fit with your cyber maturity, compliance requirements and budget.

LEVEL ONE

Peace of mind that your assets are secure, in line with IMO standards and standard cyber security frameworks.

For smaller shipping companies

Secure Email Configuration

Mail Servers and user workstations running mail clients are frequently targeted by attackers. Whether it is business email compromise, ransomware attacks or targeted phishing attacks, such attacks are on the rise and in their sophistication.

It is imperative that every organization whether their mail server on cloud or on-premises, should have robust security reviews and controls to protect from external threats.

Every email incident has unique circumstances that must be evaluated, processed, and addressed to quickly move to a state of resolution.

IT/OT Vulnerability Assessment

Identifying the vulnerability in an environment with a clear understanding of the business and technical risk is the key to success to uphold and review the appropriate security controls.

We assess the current IT security infrastructure and give an analytic based report which helps customers to focus on high-risk vulnerabilities.

SDSD's core strength is on manual validation of the environment by reviewing configuration rather than just running the automated vulnerability scanner. It will help your organization prevent:

- Malware distributed throughout the organization via email.
- Spam emails sent to users to perform actions that further an attack.
- Internal user sending confidential and proprietary information to external organization.
- Misconfiguration allowing an attacker to use the organization's mail server and send phishing emails to other organizations.
- Denial of service (DoS) attack directed to the on-premise mail server, denying or hindering valid users from using the mail server.

Cyber Security Awareness & Training

Security awareness training is the process of providing formal cybersecurity education to the workforce about a variety of cyber-threats and outlines the company's policies and procedures for addressing them.

Security awareness training provides workers with the skills they need to combat these threats. Crew and office staff cannot be expected to be aware of threats or to know how to respond to them on their own.

Our training sessions ensure staff understand their responsibilities in keeping your cyber-assets secure, and help avoid common errors that lead to costly attacks. Training modules include:

- Phishing
- Mobile device
- Safe web browsing
- Desktop/ laptop best practices
- Email security
- Physical security

Basic Policy and Procedures Requirement

We support you in analyzing the requirements and creating the right procedures and documentation to reach compliance with the IMO mandatory guidelines for your ISM.

- Information security objectives -CIA
- Authority and access control policy
- Data classification
- Data support and operations
- Responsibilities, rights, and duties of personnel.

Security Level & Technical

We analyze and recommend the required security level to ensure a robust network.

- Product description (Network devices, AV) – recommendations on appropriate products for a secure environment/network.
- Operating Environment – Many organizations are not aware of the right operating system to use, we recommend the best OS required/suited to the organisation.
- IMO Regulatory Requirements – We ensure that technical requirements are appropriately addressed in existing safety management systems.

LEVEL TWO

Based on the services included in the level two category plus the following:

For medium sized companies

Penetration testing

The major goal is identifying security weaknesses in an application or a piece of software. Based on the application, around 400-500 checks will be carried out, enabling us to identify threats and provide recommendations that will protect your organization from major attacks. Penetration testing is one of the mandatory requirements by the IMO.

Cyber Security On-Site/On-Board Pre-audit

Our consultants will visit the office and vessel and ensure all documentation is correct prior to audit.

Secure Network Configuration

Secure configuration refers to the security steps taken when designing and upgrading computers and network equipment in order to minimise cyber vulnerabilities. One of the most common security flaws that criminal hackers look to exploit is security misconfigurations.

SDSD Cyber Risk Analysis Process

- Take inventory of systems and resources.
- Identify potential weaknesses and threats.
- Determine the risk impact.
- Develop and set cybersecurity controls.
- Evaluate the effectiveness and repeat. We ensure that the network configuration is secure enough to protect it from cyber criminals, in line with the IMO requirements.

Development of Cyber Security Documents

We help you create and maintain the required security documents to meet the IMO guidelines.

- Information security policies
- Incident management plan
- Disaster recovery & business continuity plans
- Critical asset inventory
- Risk assessment documents

Cyber Risk Analysis

A cybersecurity risk analysis will assist the business in identifying, managing, and safeguarding data, information, and assets that may be vulnerable to a cyber-attack. This type of analysis enables you to identify systems and resources, assess risk, and devise a strategy for implementing security controls that will help protect your company. We ensure that the network configuration is secure enough to protect it from cyber criminals, in line with the IMO requirements.

LEVEL THREE

All the services mentioned in level one and two categories, plus the following:

For large shipping companies

User Access Review

Frequently during user access analysis, businesses discover users who have left the company or been transferred to another team within the company still have access to applications or infrastructure. This weakness may be abused, causing financial and/or reputational harm to the company. We ensure that the network configuration is secure enough to protect it from cyber criminals, in line with the IMO requirements.

The User Access Review is to monitor and ensure that only approved users have access to applications or resources on a regular basis.

We will review and provide the best practices to meet the IMO Guidelines.

Incident Response and Recovery

Incident Response is a set of measures companies take to cope with various security breaches. Such cases, also known as IT and security incidents, must be managed in a manner that minimizes recovery time and costs.

Our incidence response team has the ability to react to multiple, often combined cyber-attacks, such as Ransomware, DDoS etc. and prepare the organization to have a proper plan for it.

One of the important guidelines of IMO is to have a proper response and recovery plan.

SOC Implementation

A Security Operations Center (SOC) is a centralized unit that uses personnel, procedures, and technology to continually track and enhance the security position of the company while preventing, detecting, analyzing, and reacting to cybersecurity incidents.

Configuration Review

A Secure Configuration analysis tests and verifies the configuration settings of IT infrastructure components such as systems, network devices, and applications to determine the IT environment's security effectiveness.

Our recommendations for configuration settings will reduce the attacks in an organisation. We will review and provide the best practices to meet the IMO Guidelines.

Compliance Assessment

The constantly changing regulatory environment increases the vulnerability of most organizations to compliance risk. Our compliance assessment is a technical gap assessment. Looking to identify gaps between the existing control environment and what is required.

We will help understand the top compliance risks and develop effective mitigation strategies to reduce the likelihood of a major noncompliance event.

SDSD

DIGITAL SOLUTIONS FOR MARITIME

UK: +44 20 3588 6740
Singapore: +65 3158 7545
Greece: +30 21 1198 4479
UAE: +971 529957617

www.sdsd.com
sales@sdsd.com

Copyright © 2021 SDSD. All rights reserved.