EPSCO-RA
Maritime Cyber Security Solutions

CSN
CYPRUS SHIPPING NEWS

Cybersecurity as a Business Process

September 2020

EPSCO-RA
Maritime Cyber Security Solutions

Question

- Do you like lower operational costs?
- Do you like to save time and effort?
- Would you like audits and 3rd party inquires to be non-issue?
- Would you like to simplify IMO compliance?

EPSCO-RA
Maritime Cyber Security Solutions

Do this with ONE thing

Approach Cybersecurity as a Business Process focused on Digital Risk

EPSCO-RA
Maritime Cyber Security Solutions

Risk Management is a Familiar Process

Calibrated Risk Matrix

Calibrate the matrix to reflect your Operations business-wide impact of failure

The cost consequence is estimated on the DAFT Costing worksheet

The likelihood is determined from the historic frequency occuring in your Operation or from other comparable operations

			Likelihood of Equipment Failure Event per Year			**DAFT Cost per Event**	$30	$100	$300	$1,000	$3,000	$10,000	$30,000	$100,000	$300,000	$1,000,000	$3,000,000	$10,000,000	$30,000,000	$100,000,000	$300,000,000	$1,000,000,000
Probability (per Opportunity)	**Sigma Level**	**Event Count per**	**Time Scale**	**Descriptor Scale**	**Historic Description**		1.5	2	2.5	3	3.5	4	4.5	5	5.5	6	6.5	7	7.5	8	8.5	9
		100	Twice per week			2	3.5	4	4.5	5	5.5	6	6.5	7	7.5	8	8.5	9	9.5	10	10.5	11
		30	Once per fortnight			1.5		3.5	4	4.5	5	5.5	6	6.5	7	7.5	8	8.5	9	9.5	10	10.5
1		10	Once per month	Certain		1			3.5	4	4.5	5	5.5	6	6.5	7	7.5	8	8.5	9	9.5	10
0.3	2	3	Once per quarter			0.5					4	4.5	5	5.5	6	6.5	7	7.5	8	8.5	9	9.5
0.1	3	1	Once per year	Almost Certain	Event will occur on an annual basis	0						4	4.5	5	5.5	6	6.5	7	7.5	8	8.5	9
0.03		0.3	Once every 3 years	Likely	Event has occurred several times or more in a lifetime	-0.5							4	4.5	5	5.5	6	6.5	7	7.5	8	8.5
0.01	4	0.1	Once per 10 years	Possible	Event might occur once in a lifetime career	-1								4	4.5	5	5.5	6	6.5	7	7.5	8
0.003		0.03	Once per 30 years	Unlikely	Event does occur somewhere from time to time	-1.5									4	4.5	5	5.5	6	6.5	7	7.5
0.001		0.01	Once per 100 years	Rare	Heard of something like it occurring elsewhere	-2										4	4.5	5	5.5	6	6.5	7
0.0003		0.003	Once every 300 years			-2.5											4	4.5	5	5.5	6	6.5
0.0001	5	0.001	Once every 1,000 years	Very Rare	Never heard of this happening	-3												4	4.5	5	5.5	6
0.00003		0.0003	Once every 3,000 years			-3.5													4	4.5	5	5.5
0.00001		0.0001	Once every 10,000 years	Almost Incredible	Theoretically possible but not expected to occur	-4														4	4.5	5

Note:

Risk Level
Red = Extreme
Amber = High
Yellow = Medium
Green = Low
Blue = Accepted

1) Risk Boundary 'LOW' Level is set at total of $10,000/year

2) Based on HB436:2004-Risk Management

3) Identify 'Black Swan' events as B-S (A 'Black Swan' event is one that people say 'will not happen' because it has not yet happened)

4) DAFT Cost (Defect and Failure Total Cost) is the total business-wide cost from the event

1-RELIABILITY

Risk = Consequence of Failure x [No Opportunities x Probability of Failure at Opportunity]

EPSCO - RA

Maritime Cyber Security Solutions

RISK FACTORS		RISKS	EVALUATION				PREVENTIVE MEASURES
			P	G	Priority		
1	Pilotage error	Dash / collision	4	4	16	A	Better communication between the pilot and the ship's captain
		Fire/ explosion	1	4	4	B	Fire training for special cargoes (gas, oil, chemicals)
		Grounding	1	3	3	C	Better mastery of manoeuvre
		Death / injury	3	4	12	A	Training emergency care
		Pollution	1	3	3	C	Adequate training on how to struggle against marine pollution
2	Failures with tugs / pilot boats	Dash / collision	3	2	6	B	Better control of the power of tugs
		Fire/ explosion	1	3	3	C	Fire training for special cargoes (gas, oil, chemicals)
		Grounding	1	3	3	C	A good knowledge of the depths of the harbour basin
		Death / injury	1	4	4	B	Training emergency care
		Pollution	1	2	2	C	Adequate training on how to struggle against marine pollution
3	Equipment failures and port facilities	Dash / collision	4	3	12	A	Clear unobstructed docks and building mooring hooks and decencies
		Fire/ explosion	1	4	4	B	Equipment and fire-fighting training
		Grounding	2	3	6	B	Dredging of the harbour basin
		Death / injury	2	4	8	B	Training emergency care
		Pollution	1	3	3	C	Adequate anti-pollution equipment
4	Damage to the ship / crew errors	Dash / collision	3	2	6	B	Engine maintenance
		Fire/ Explosion	1	4	4	B	Fire management according to the requirements of SOLAS
		Grounding	2	3	6	B	Better mastery of ship handling
		Death / injury	3	3	9	A	Crew training in emergency care
		Pollution	2	3	6	B	Pollution prevention as MARPOL
5	Weather conditions	Dash / collision	3	3	9	A	Mastery of manoeuvring a ship in case of strong wind
		Fire/ explosion	1	2	3	C	Mastery of the effect of wind on fire
		Grounding	2	3	6	B	A ship in bad weather
		Death / injury	1	4	4	B	Particular attention to the crews in case of bad weather
		Pollution	4	3	12	A	Calculating the direction of the drift of oil slicks / wind
6	Organizational gaps	Dash / collision	2	3	6	B	Plan docking manoeuvres
		Fire/ explosion	1	2	2	C	Team training for fire fighting
		Grounding	2	3	6	B	Bathymetric Surveys updated
		Death / injury	2	3	6	B	Training of port personnel in emergency care
		Pollution	1	3	3	A	Raising awareness against the effects of marine pollution

EPSCO - RA
Maritime Cyber Security Solutions

EPSCO - RA

Maritime Cyber Security Solutions

Identify

- Asset Management
- Business Environment
- Governance
- Risk Assessment
- Risk Management Strategy

Protect

- Access Control
- Awareness and Training
- Data Security
- Information Protection Processes and Procedures
- Maintenance
- Protective Technology

Detect

- Anomalies and Events
- Security Continuous Monitoring
- Detection Processes

Respond

- Response Planning
- Communications
- Analysis
- Mitigation
- Improvements

Recover

- Recovery Planning
- Improvements
- Communications

EPSCO-RA
Maritime Cyber Security Solutions

The Tools are Freely Available

- Vast Control Inventory (NIST 800-53)
- Published Use Cases and Examples
- Freely Available Documentation (NIST CSF)
- What’s the Catch?

EPSCO-RA
Maritime Cyber Security Solutions

Getting Started and Operating

- Steep Learning Curve
- Expensive Software Tools
- Opaque ROI
- Specialist Manpower Intensive

EPSCO-RA
Maritime Cyber Security Solutions

The more defined the process is, the more commoditized it becomes.

EPSCO-RA
Maritime Cyber Security Solutions

So the more mature the process becomes, more and more of it is outsourced. Because…

The number of specialist skills involved is so numerous that most companies train employees to do multiple tasks or jobs.

The employee who *wears multiple hats* will never be as efficient or proficient as a specialist on any given subject.

EPSCO-RA
Maritime Cyber Security Solutions

Save Time, Effort and Money?

Define It
Refine It
Outsource It

EPSCO-RA
Maritime Cyber Security Solutions

Full Disclosure: Sales Pitch

Epsco-Ra will save you money and accelerate your digital risk management program no matter where you are along the path.

Governance with NIST CSF

- Regardless of the certification or recommendation you have chosen
- IMO recommended
- Proven Turn-Key Process
- Takes you from “nothing formal” to a fully documented governance framework in about 90 days

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
	Access Control				
AC-1	Access Control Policy and Procedures	P1	AC-1	AC-1	AC-1
AC-2	Account Management	P1	AC-2	AC-2 (1) (2) (3) (4)	AC-2 (1) (2) (3) (4) (5) (11) (12) (13)
AC-3	Access Enforcement	P1	AC-3	AC-3	AC-3
AC-4	Information Flow Enforcement	P1	Not Selected	AC-4	AC-4
				AC-5	AC-5
				(1) (2) (5) (9) (10)	AC-6 (1) (2) (3) (5) (9) (10)
				AC-7	AC-7
				AC-8	AC-8
				Selected	Not Selected
				Selected	AC-10
				C-11 (1)	AC-11 (1)
				AC-12	AC-12
				—	—
				AC-14	AC-14
				—	—

EPSCO-RA
MARITIME CYBER SECURITY SOLUTIONS

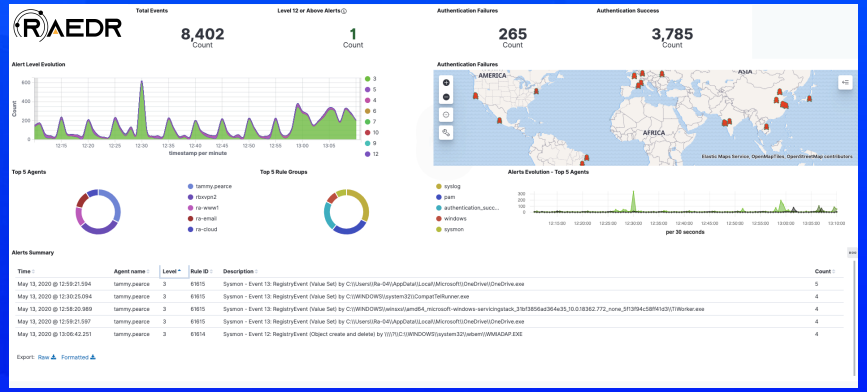
NIST Cybersecurity Framework - Profile - DO
NIST Framework Version 1.1 (issued April 10, 2018) https://doi.org/10.6028/NIST.CSWP.04162018

NIST Function	NIST Category (Activity/Outcome)	NIST Subcategory (Objective)	DO Controls
IDENTIFY (ID) Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried	1005 End Point Protection 1006 Desktop/Laptop Asset Tracking & Software Update/Licensing Management 1007 Network Equipment Asset Tracking & Software Update/Licensing Management
IDENTIFY (ID)	**Asset Management (ID.AM)**	**ID.AM-2:** Software platforms and applications within the organization are inventoried	1005 End Point Protection 1006 Desktop/Laptop Asset Tracking & Software Update/Licensing Management 1007 Network Equipment Asset Tracking & Software Update/Licensing Management 1049 Business Process Owner (BPO) Approval of Logical Access to IT Systems
IDENTIFY (ID)	**Asset Management (ID.AM)**	**ID.AM-3:** Organizational communication and data flows are mapped	1031 System Documentation
IDENTIFY (ID)	**Asset Management (ID.AM)**	**ID.AM-4:** External information systems are catalogued	1026 Third-party Risk Management Program (TPRM)
IDENTIFY (ID)	**Asset Management (ID.AM)**	**ID.AM-5:** Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	1012 Subject Matter Expert (SME) Team 1036 Strategic IT Plan 1038 IT Organizational Structure 1037 IT Risk Assessment
IDENTIFY (ID)	**Asset Management (ID.AM)**	**ID.AM-6:** Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	1012 Subject Matter Expert (SME) Team 1036 Strategic IT Plan 1038 IT Organizational Structure 1037 IT Risk Assessment 1039 Information Security Awareness Training 1041 Emergency (EMP) Security Access Procedure 1042 Emergency Changes to Production 1026 Third-party Risk Management Program (TPRM) 1050 SOC 1 Review 1051 SOC 2 Review
	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and	**ID.BE-1:** The organization's role in the supply chain is identified and	1012 Subject Matter Expert (SME) Team 1026 Third-party Risk Management Program (TPRM)

							AC-8
							Not Selected
							AC-10
							AC-11 (1)
Network?	1002	AC-12	(Session Termination	P0	Not Selected	AC-12	AC-12
		AC-13	**Withdrawn**		—		
	1050	AC-14	Permitted Actions without Identification or Authentication	P5	AC-14	AC-14	AC-14
		AC-15	**Withdrawn**		—	—	—
	1004 1020 1026	AC-16	Security Attributes	P0	Not Selected	Not Selected	Not Selected
	1017	AC-17	Remote Access	P1	AC-17	AC-17 (1) (2) (3) (4)	AC-17 (1) (2) (3) (4)
	1050	AC-18	Wireless Access	P1	AC-18	AC-18 (1)	AC-18 (1) (4) (5)
		AC-19	Access Control for Mobile Devices	P1	AC-19	AC-19 (5)	AC-19 (5)
	1001 1014 1015 1046	AC-20	Use of External Information Systems	P1	AC-20	AC-20 (1) (2)	AC-20 (1) (2)
	1003 1043	AC-21	Information Sharing	P2	Not Selected	AC-21	AC-21
		AC-22	Publicly Accessible Content	P3	AC-22	AC-22	AC-22
	1020 1025 1026	AC-23	Data Mining Protection	P0	Not Selected	Not Selected	Not Selected
		AC-24	Access Control Decisions	P0	Not Selected	Not Selected	Not Selected
		AC-25	Reference Monitor	P0	Not Selected	Not Selected	Not Selected
		* The security control baselines in Table D-2 are the initial baselines selected by organizations prior to conducting the tailoring activities described in Section 3.2. The control baselines and priority codes are only applicable to unclassified security c					
		AT	**Awareness and Training**				
	1046	AT-1	Security Awareness and Training Policy and Procedures	P1	AT-1	AT-1	AT-1
	1043	AT-2	Security Awareness Training	P1	AT-2	AT-2 (2)	AT-2 (2)

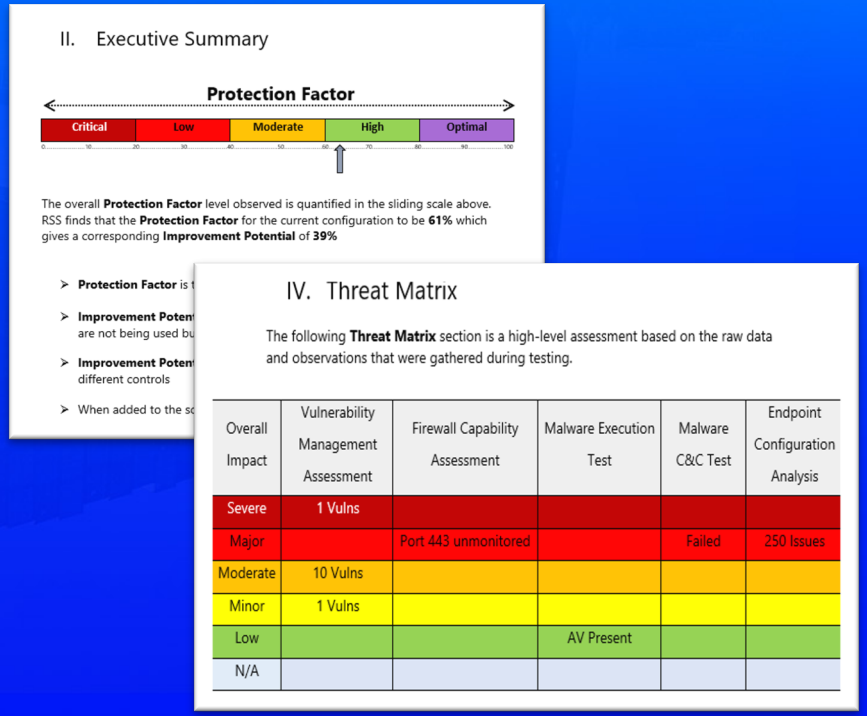
Managed Security with RaEDR

- Managed SIEM with a Customer Portal
- Continuous Vulnerability Assessment
- Continuous Security Configuration Assessment
- Deploys remotely in about an hour
- No equipment required onboard



Penetration Testing with RASP

- Rapid Attack Simulation Penetration test
- Remotely Conducted
- FW and AVS Functionality
- Security Configuration and Vulnerability Assessment
- Quantitative Scoring



II. Executive Summary

Protection Factor

Critical | Low | Moderate | High | Optimal

0 10 20 30 40 50 60 70 80 90 100

The overall **Protection Factor** level observed is quantified in the sliding scale above. RSS finds that the **Protection Factor** for the current configuration to be **61%** which gives a corresponding **Improvement Potential** of **39%**

- **Protection Factor** is t
- **Improvement Potent** are not being used bu
- **Improvement Potent** different controls
- When added to the sc

IV. Threat Matrix

The following **Threat Matrix** section is a high-level assessment based on the raw data and observations that were gathered during testing.

Overall Impact	Vulnerability Management Assessment	Firewall Capability Assessment	Malware Execution Test	Malware C&C Test	Endpoint Configuration Analysis
Severe	1 Vulns				
Major		Port 443 unmonitored		Failed	250 Issues
Moderate	10 Vulns				
Minor	1 Vulns				
Low			AV Present		
N/A					

EPSCO-RA
Maritime Cyber Security Solutions

As a Token of our Appreciation

https://www.epsco-ra.com/contact

Request a quote or schedule a demo for one of our services and mention Cyprus Shipping News for a chance to win a free RASP (winner selected Friday Sept. 25).

Follow us on FB and LinkedIn