Cyber Risk Management in Practice

SMM

Maritime Cyber Resilience Forum

Babis Kalevrosoglou

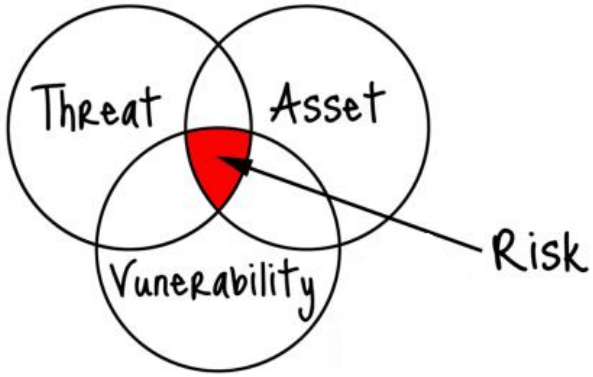
Information Security Manager

© ASPIDA CYBER SECURITY

aspida
CYBER SECURITY

What is Risk Management?

The efficient identification of Risks by defining …



- Risk description
- Risk owner
- Risk probability
- Risk Impact (reputation, cost, loss of assets)
- Risk mitigation (the mitigation cost should be relative to risk reduction)
- Contingency Plan

© ASPIDA CYBER SECURITY

Cyber Risk Management

When talking about Cyber Risk Management, we have to identify risks which impact :

- Confidentiality
- Integrity
- Availability

© ASPIDA CYBER SECURITY

aspida
CYBER SECURITY

Cyber Risk Management Goals

Effective Cyber Risk Management gives an organization the ability to **resist**, **respond** and **recover** from incidents that will impact the information they require to do business.

© ASPIDA CYBER SECURITY

aspida
CYBER SECURITY

Cyber Security Challenges

- 75% of companies in maritime industry do not retain a complete digital asset inventory
- 211 days is the average number of days it takes for an organization to identify that their systems were successfully compromised
- 70% of data security breaches are caused by human error or system failure
- 65% of large organizations do not have the resources and technical knowledge to address a cyber security incident
- 1 unaware employee is needed to enable a malicious actor compromise your systems and access sensitive information
- 54% of large organizations do not have a Security Operation Center (SOC)

© ASPIDA CYBER SECURITY

aspida CYBER SECURITY

Assets & Threats

What needs to be secured?

- Hardware, Software, Services
  - Servers, workstations, network devices, mobile devices
  - Operating Systems, Databases, Applications
  - Files, Data stored in Databases

- Who are the enemies?
  - External attacker
  - Insider

© ASPIDA CYBER SECURITY

aspida
CYBER SECURITY

Cyber Security Framework

	Function	Category
What processes and assets need protection?	Identify	Asset Management
		Business Environment
		Governance
		Risk Assessment
		Risk Management Strategy
What safeguards are available?	Protect	Access Control
		Awareness and Training
		Data Security
		Information Protection Processes & Procedures
		Maintenance
		Protective Technology
What techniques can identify incidents?	Detect	Anomalies and Events
		Security Continuous Monitoring
		Detection Processes
What techniques can contain impacts of incidents?	Respond	Response Planning
		Communications
		Analysis
		Mitigation
		Improvements
What techniques can restore capabilities?	Recover	Recovery Planning
		Improvements
		Communications

© ASPIDA CYBER SECURITY

aspida
CYBER SECURITY

Most common Cyber Attack Vectors

- Unpatched Vulnerabilities
- Poor Remote Access security
- Lack of security monitoring
- Weak network security
- Lack of accountability from third parties

© ASPIDA CYBER SECURITY

aspida
CYBER SECURITY

So… How to eliminate Cyber Risk?

© ASPIDA CYBER SECURITY

aspida
CYBER SECURITY

THE HUMAN FACTOR

© ASPIDA CYBER SECURITY

aspida
CYBER SECURITY

TRAINING

© ASPIDA CYBER SECURITY

The human factor

According to latest statistics in Cyber Security, the human factor is responsible for 90% of cyber security incidents globally. This is the most vital step to eliminate the overall Cyber Risk of an organization.

- Raise employees cyber security awareness
  - E-learning training
  - Classroom Based training
  - Phishing campaigns

© ASPIDA CYBER SECURITY

Cyber Risk – Technical Controls

First things first…

- Firewalls
- Intrusion Detection/Prevention Systems
- Antiviruses
- Encryption

© ASPIDA CYBER SECURITY

aspida
CYBER SECURITY

Cyber Risk – Technical Controls

Q: I have everything in place… Am I still exposed to any cyber threats?

A: Well, you will need to ensure also, that there are policies and procedures for update and patch management for your IT infrastructure.

Perform a Vulnerability Assessment !!!

© ASPIDA CYBER SECURITY

aspida
CYBER SECURITY

What is a Vulnerability Assessment?

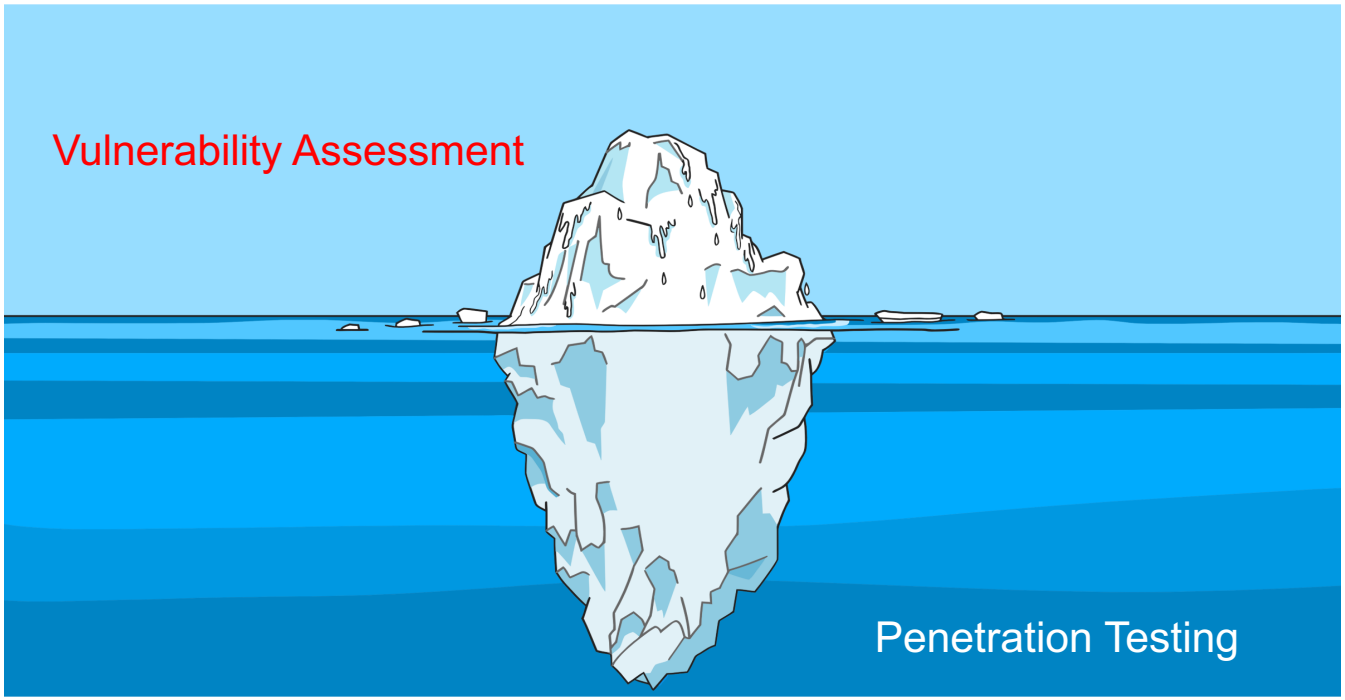
- Is the process of identifying, quantifying and prioritizing the vulnerabilities in a system
- It consists of four phases
  - Asset discovery
  - Definition of asset importance
  - Vulnerability identification
  - Vulnerability management
- It has many things in common with Risk Assessment.
- Performing a Vulnerability Assessment not only can discover the risk for a system, but also the consequences that the specified risk would have on the whole infrastructure.

© ASPIDA CYBER SECURITY

aspida
CYBER SECURITY

Cyber Risk – Technical Controls

Vulnerability Assessment is a great start, but it focuses on what can be seen with a naked eye. If you want to assess the security in every layer you have to simulate attacks against your infrastructure.



© ASPIDA CYBER SECURITY

aspida
CYBER SECURITY

What is Penetration Testing?

- It is a simulated attack on a system which aims to evaluate its security.
- It gives in depth insights about system security weaknesses
- It can be mainly performed as
  - White Box (Technical information are provided before engagement)
  - Black Box (Only limited information are provided, such as Company Name)
- It consists of five phases
  - Reconnaissance
  - Vulnerability identification
  - Exploitation
  - Cleanup
  - Reporting

© ASPIDA CYBER SECURITY

aspida
CYBER SECURITY

Cyber Risk – Technical Controls

Q: Why cleanup is needed during Penetration Testing?

A: We need to ensure that the logs produced during Penetration Test attempts are stored so as to be able to trace back every action. Also during Penetration Test we can evaluate our security mechanisms that are in place (IPS, IDS, Antivirus) by monitoring their behavior.

© ASPIDA CYBER SECURITY

What is SIEM?

- SIEM stands for Security Incident & Event Management
- It provides real time cyber security monitoring
- SIEM should be monitored by a Security Operation Center (SOC), on 24* 7 * 365 basis.
- Correlation of data between multiple sources (workstations, firewalls, email security, antivirus etc.)
- Threat Intelligence, data ingestion
- Compliance with standards such as HIPAA, PCI DSS etc
- Long term storage of security logs
- Visualizations in dashboards for efficiency in incident detection and handling

© ASPIDA CYBER SECURITY

Cyber Risk – Technical Controls

Q: Our business include operations off-shore. How can we mitigate cyber risk on vessels?

A: The approach for cyber risk management on vessels should be similar to offices.

First you will need to evaluate current vessel's cyber risk and then you will need to ensure that the remaining risk will not be exploited.

© ASPIDA CYBER SECURITY

Cyber Security Assessment onboard

© ASPIDA CYBER SECURITY

aspida
CYBER SECURITY

Cyber Risk on Vessels – Technical Controls

Consider having a security professional assess the current cyber risk for your vessels.

- Various realistic attack scenarios
  - External Wi-Fi Attacker
  - External Internet Attacker
  - Internal Attacker

© ASPIDA CYBER SECURITY


Nemesis
Managed Security Services for Vessels

aspida
CYBER SECURITY

Cyber Risk on Vessels – Technical Controls

Achieve security in depth for vessels, integrating **security incident detection** and **security compliance** mechanism.

- Intrusion Detection in real time
- Threat Intelligence
- Client Portal (with dashboards for all your vessels)
- Alerting System
- Security Operations Center
- Emergency Response

© ASPIDA CYBER SECURITY

Cyber Risk – Technical Controls

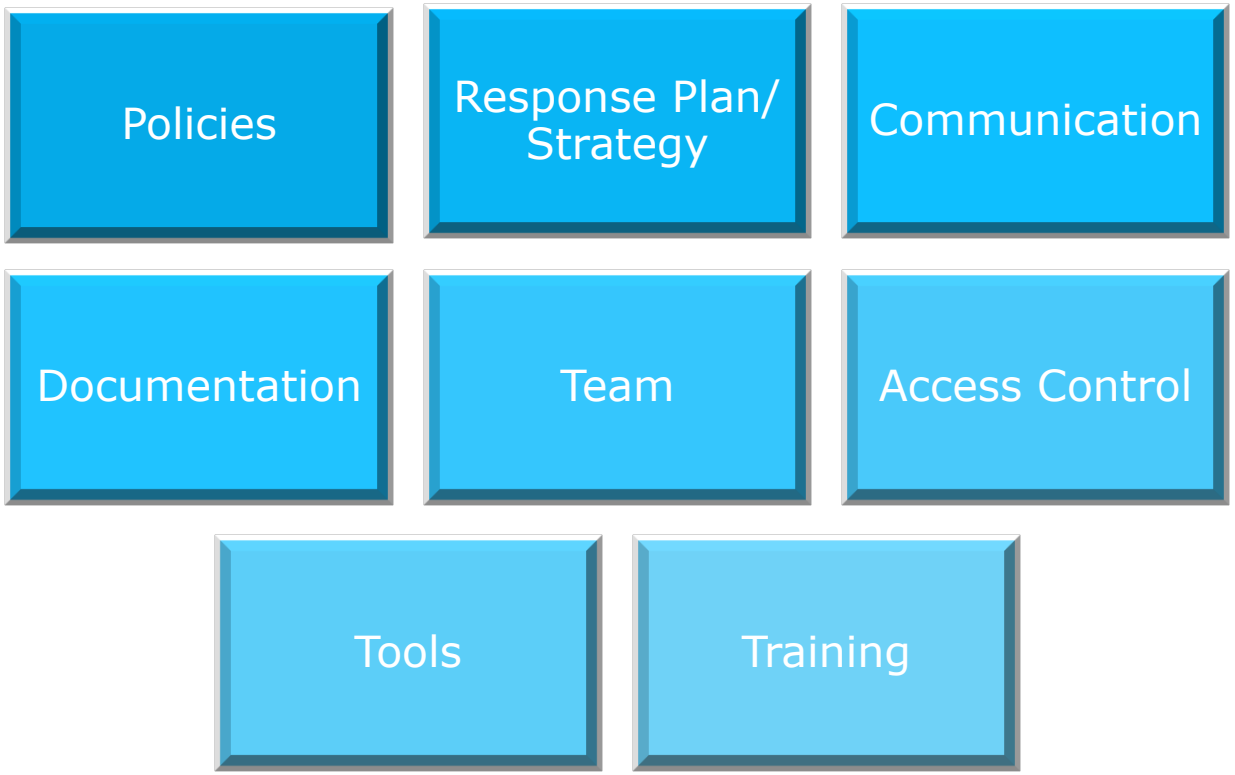
You have achieved security in depth!

But even if the risk has extremely eliminated, you will need to be ready for anything bad that may happen.

© ASPIDA CYBER SECURITY

aspida
CYBER SECURITY

Incident Response Plan



© ASPIDA CYBER SECURITY

aspida
CYBER SECURITY

THANK YOU!

© ASPIDA CYBER SECURITY