Challenges in Maritime and Supply Chains' Security



1st NMIOTC CYBER SECURITY CONFERENCE



Associate Professor N. Polemi, Director of UNIPI Security Lab

4-5/10/2016



- **S-Port** (national project) and E.C. project **CYSM**: Static Ports' RM methodology and tool (ISO27001, 27005, ISPS, CIIP)
- E.C. project <u>MEDUSA</u>: Static SC RM' methodology and tool (ISPS, CIIP, ISO28000)
- E.C. project **MITIGATE**: Dynamic evidence-driven Maritime SC RM environment (simulation, crowd-sourcing, open data) (ISO27001, 27005, ISPS, CIIP, ISO28000)
- E.C. project **FASTPASS** on Automated Board Control systems

The Policy / Legislation Challenge



- IMO: MARPOL for the sea protection; SOLAS for the safety of the ships, passengers and cargo and the ISPS (formulated in 2004) address the organisational aspect of security.
- WCO SAFE Framework of standards (2015) to Secure and Facilitate Global Trade
- USA, 2016 House of Representatives <u>H.R. 3878</u>, "Strengthening <u>Cybersecurity Information Sharing and Coordination in Our Ports Act</u> <u>of 2015</u>"



- CIIP Directive (2012) <u>Critical information infrastructure protection:</u>
 <u>towards global cyber-security</u>
- The <u>Cybersecurity Strategy for the European Union</u> (2013) and the <u>European Agenda on Security (2015)</u> provide the overall strategic framework for the EU initiatives on cybersecurity and cybercrime.
- <u>eIDAS Regulation (2014)</u> on electronic identification and trust services for electronic transactions in the internal market
- <u>European Parliament</u> 2015 concerning measures to ensure a high common level of network and information security across the Union
- <u>NIS Directive 2016</u> applies only to those public administrations which are identified as operators of essential services
- <u>cPPP</u> Initiative 2015 ensures that Europe will have a dynamic, efficient and effective market in cybersecurity products and services.
- <u>Enhanced Privacy Directive</u>, 2016 Mandatory reporting of security breaches

PLETHORA OF STANDARDS



- ISO/IEC <u>27001:2005</u> / <u>ISO/IEC 27001:2013</u> (building a SM system)
- ISO/IEC 27005:2011 guidelines for information security risk management
- NIST SP 800-128, 2011 Guide for Security-Focused Configuration Management of Information Systems
- ISO 31000:2009 Principles and Guidelines on Implementation
- ISO/IEC 31010:2009 Risk Management Risk Assessment Techniques
- ISO/IEC 27002:2005 (best practice recommendations)
- AS/NZS 4360:2004 (Australian/New Zeland standard for RM)

The above standards are supported by a variety of methodologies (see <u>ENISA repository</u>)

- ISO 28000:2007 ISO 28001:2007, ISO 28003:2007, ISO 28004:2007 for supply chain security
- IMO 2016 cyber security guidelines for maritime companies and ships

THE SECURITY AWARENESS CHALLENGE



- We have enough security standards/policies/regulations, we need targeted Market-driven "easy to use" risk assessment tools for maritime operators assessing and mitigating their physical/cyber risks. Insurance companies and auditors may require risk assessment and mitigation of cyber risks in their insurance policies.
- Collaboration among maritime and security regulators standardization bodies and associations (IMO, NATO, EMSA, IPCA, EPCSA, ENISA, DGMARE, DGMOVE, DGCONNECT etc.)
- Enhanced academic programs in the maritime academies and universities
- Open IMO/NATO/EMSA cyber/physical exercises targeted to the commercial maritime sector (ports, maritime companies, ships, industry etc).

THE RISK ASSESMENT CHALLENGE FOR PORTS' CIS









GEMENT SYSTE

							E			
Home Sites A	e-Library Coll CYSM Pilot Port	Home e-Lib CYSM R.A. E Back	MARITIME SAFETY C 95th session Agenda item 4 ME	OMMITTEE EASURES TO ENHAN	E CE MARITIME SECURITY	MSC 14 ENGLI	95/INF.19 April 2015 SH ONLY	l		
Carsen As	CYSM Port of Carrara	Asset Identification Register Infrastructu	CYSM project – "	Reporting						
V Vendaport	Port of Valencia	Register Physical (Non ICT) Assets Register HW	10,000,000	ulnerability Vul. Level Controls						
۷	Port-of-Mykonos	Assets Register Software Assets	Executive summary:	European Commission security related to the	gaps in	of software rensive security aining program or controlling copyrights	5 5 5	er than eighty percent		
		Register Information Data	High-level action:	6.1.1		es of sensitive files es of files e control of outbound	5 5 5	+		
		L	Action to be taken:		ntitlement review process ess rights of the organization's premises entication	5	•			
		Heiated document: WISO 94/21, paragraph 4.7								
	Telecommunication Room Theft and Fraud 3 Lack of ap								5	•
				Telecommunication Room	Theft and Fraud	3	Inadequate m premises	onitoring of the organization	5	

 \mathbb{M}

YSI

THE RISK ASSESMENT CHALLENGE FOR MARITIME SUPPLY CHAINS











		- Marchall					FUNDACIÓN Valencia port						
Medusa Administr	ation Ini	itialization	SCS Risk Assessment	SCS R	RA Results	Evaluation			Danaos	Shipping Company User Pilot +			
					Thre	at Assessment	Contro	l in Place	Cons	equence Assessment	Finish Calculate		
Threat Scenarios (TS) -		Sea BP E	valuation		Search		٩		LNG S	CS RA			
Security Controls (SC) -	BP Results Code Statistics			# Results		Se		NameQ				Export Table Data	
Business Partners Types		TS1.1 Mitig	ation Plan -		Statistics				Code	Description		Over. Risk	R. Threshold
ependency Types		TS1.			Cascading	g Dependency Risk			TS1.1	Destroy a major / critical SC infrastructure		High	High
/eight		TS2:							TS4.2	Use the supply chain as a means of smuggling. Suspected or confirmed unsuthorized access to SC hifrastructures		Medium	Medium
									TS1.2			Low	Medium
isk Assessment Elements -		TS2.							TS4.1	Intrude and/or take control of an asset (including conveyances) within the supply chain.		Low	Low
					2				TS2.1	Information tampering		Low	Medium
		TS2.			3				T\$3.2	Misuse / abuse of SC procedures		Low	Medium
					4				TS3.1	People under attack		Low	Medium
					5				TS2.2	Information loss		Low	High
									TS2.3	Communication interruption or loss		Low	Low
									TS2.4	Software/system abuse		Low	High



THE RISK ASSESMENT CHALLENGE FOR MARITIME SUPPLY CHAINS' INTERCONNECTED CYBER ASSETS MITIGATE





MITIGATE PROJECT



- MITIGATE methodology for assessing the complex, propagated risks of the interconnected supply chains' cyber assets
- MITIGATE dynamic, risk assessment tool
- MITIGATE forecasting, simulation, crowed sourcing and risk assessment services utilizing open security data

www.mitigateproject.eu

THE CHALLENGE OF PHYSICAL-CYBER MARITIME RISKS





MARITIME COMPUTER INCIDENT RESPONSE CENTERS



The national or European CERTs do not guide maritime operators on how to manage security incidents. A trusted body need to undertake this role in order to:

- thoroughly assess the vulnerabilities
- forecast and evaluate the probability of hybrid attacks;
- access/receive warnings for upcoming attacks and vulnerabilities;
- recreate, visualize and forecast propagation/cascading effects;
- provide guidance on investigating and handling complex, interrelated physical/cyber maritime security incidents;
- combine and analyze all security incident
- receive guidelines, share information and warnings

AUTOMATED BORDER CONTROL SYSTEMS (ABCS)



The FRONTEX requirements (FRONTEX, 2012) for the ABC systems need to be enhanced in order to address the remaining challenges:

- Mobility
 - Interoperability
- Multimodality-Interconnection
 - Indoor ABC gates
 - Mobile ABC gates
- ABC portable devices held by the patrol controllers
- Large ABC gates for vehicle
- ABC systems for cargo





The E.C. **FastPass** project is considering the above needs

MARITIME SOFTWARE CODE AUDITING



- Innovative maritime source code auditing tools are required in order to find security flaws (e.g. authentication, access control, cryptography problems).
- Maritime software (for ship management, marine navigation, shipping ERPs,..) need to be audited by certification bodies
- Port Community Systems / National Single Windows security is treated as a "black box".

COST IS A CHALLENGE



Accountability needs to complement Security. Commercial maritime Cls (ports, companies etc) can not afford to become military camps. Security needs to be viewed as a shared responsibility.

(e.g. If a navigation system is vulnerable to interruption, the provider is responsible for the mitigation of its vulnerabilities and not the maritime company or the port authority)

Accountability technologies, enhanced SLAs and insurance policies are proposed measures.

Security & Privacy as Cloud Services hosted and operated by a trusted party (e.g. IMO, EMSA, NATO) will minimize the security costs of the commercial maritime entities

CONCLUSIONS







Thank YouN. Polemi- dpolemi@gmail.com