Collaborative Security Management Services for Port Information Systems

Theodoros Ntouskas, Dimitris Gritzalis

October 2015
Collaborative Security Management Services for Port Information Systems

Theodoros Ntouskas & Dimitris Gritzalis

Information Security & Critical Infrastructure Protection Laboratory
Dept. of Informatics | Athens University of Economics & Business

Ημερίδα Λιμενικού Σώματος - Ελληνικής Ακτοφυλακής
Athens, Greece
October 2015
Introduction

Current

Information Systems

Complex Architectures

Many end users

Distributed

Complex e-services

Interdependencies
Security Management: A world of ...acronyms!

- NIST SP 800-30
- ISO / IEC 27001:2013
- AS / NZS 4360
- ISO / IEC 27002:2013
- ISO / IEC 27005:2008

Security Management
- Identification
- Evaluation
- Mitigation
- Monitoring
- Business Risk
Transportation and Ports

- **Transportation** is a key economic sector, facilitating the movement of people, food, water, medicines, fuel, etc. **Port Authorities** play an important role in the international trade and economy environment.

- In EU >50% of the goods traffic (2010) was carried by Maritime Transport and 90% of the EU external trade took place through the Maritime Sector.

- Transportation infrastructures face **multiple threats**, ranging from physical disasters, sabotage, insider threats, terrorist attacks, etc.

- Examples are the events in New York and Washington (2001), Madrid (2004), London (2005) and Italy (2012). The common element of these incidents is the use of **transportation infrastructure components**.

- The increasing need for protecting transport infrastructures is recognized by most countries; the **transportation sector** is among the sectors recognized as **critical**.

- **Assessing risk** in critical infrastructures requires a novel approach due to the high complexity, multiple interdependencies and heterogeneity of the port environment.
Open issues

Users
(internal + all entities in the maritime environment)

Information/data
(traffic monitoring, marine, coastal, trade, lists, trade data...)

Services
(invoicing, navigation, luggage/cargo/vessel management, logistics, ...)

Software/systems
(transmission systems, maritime navigation, ERP, GIS, ticketing, ...)

ICT Infrastructure
(networks, satellites, relay stations ..)

Physical Infrastructure
(buildings, terminals, databases, servers, RFIDs, cameras, gates, ..)

Information Security

Physical Security
Existing Maritime legislation

- **MARPOL** (e.g. MEPC.: 189(60), 190(60), Annex VI) for the Sea Protection.

- **SOLAS** (e.g. MSc.: 286(86), 256(84), 46(66), 291(87), 216(82), 282(86), 291(87), 290(87)) for the safety of the ships, passengers and cargo and the ISPS addressing: Audit, secure access/handling of cargo, availability of telecom infrastructure, incident reporting, development of security team and training.

Existing Maritime Security Management methodologies

- **MSRAM** and its extended version MSRAM-PLUS/FORETELL address only physical security and they are compatible with the ISPS.
- **MARISA** concentrates on the safe navigation of ships during their presence in the port.
- **CMA** detects abnormal behavior of ships and identifies respecting threats.
- **SafeSeaNet** collects maritime information from National Authorities.
- **National methodologies** (e.g., Estonia, Jordan, Russia) concentrate only on the safety of ports.
Existing Risk Management methodologies

OCTAVE, CRAMM, EBIOS, ISO-15408-1, Mehari, MAGERIT, Austrian IT Security Handbook, BSI-Standard 100-3, Dutch A&K Analysis:

✓ Are mainly expert-driven
✓ Require the active involvement of security experts in various interviews
✓ Require extensive number of interviews and questionnaires
✓ Are time consuming and costly for the organizations
✓ Do not allow collaboration
✓ Do not collect all security knowledge of all participants
Baseline requirements

- Compatible with standards: ISO27001 and sector specific (e.g. CIIP standards and ISPS for maritime sector)
- Collaboration: Ensure collaboration among all ICT users
- Group decision making: Use group decision making algorithms
- Interdependencies: Interdependency analysis
- Broad analysis: Analyse interconnected and interdependent threats and evaluate direct and indirect risks
- Time and resource economical: Avoid the plethora of questionnaires and frustrating interviews with all participants
- Easy to implement: Expert should not need high level of expertise to apply the methodology
- Open: Avoid security through obscurity
Ideas and suggestions

STORM-RM methodology

- Uses multi-criteria collaborative decision making technique: *Analytic Hierarchy Process* (AHP)
- Takes into account the knowledge of all organizational users
- Enables all users (internal & external) to evaluate the security impacts
- It is algorithmic
- Allows parameterization (change no. of participants, weights, criteria, etc.)
The S-PORT project

- **Objectives**
  - Development of a security management collaborative methodology for critical PIT-systems
  - Collaborative generation, monitor, and update of security management docs in the open source S-Port system

- **Funded by**
  General Secretariat for R&D, Ministry of Development

- **Partners**
  - Univ. of Piraeus (PM)
  - Athens Univ. of Economics & Business
  - INTRASOFT International
  - MVNS
  - Piraeus Port Authority
  - Thessaloniki Port Authority
  - Mykonos Municipal Port Fund
S-PORT: Objectives and requirements

**Security Team**
- ICT Cartography
- Criticality of E-Services (AHP)
- Model Business Processes
- Impact Analysis
- Treat Analysis
- Vulnerability Analysis
- Risk Management (STORM-RM)
- Design Security Policy
- Security Awareness
- Training

**Managers**
- Web 2.0 Technologies
- Content Management System
- Business Processes Modeling
- Online Questionnaires

**Administrators**
- User Friendliness
- Collaboration
- Scalability
- Security
- Interoperability

**Local Users**
- User Groups
S-PORT: Services

Risk Assessment Services (STORM-RM)
- Cartography
- Impact Analysis
- Threat Analysis
- Vulnerability Analysis
- Risk Analysis

Risk Management
- Proposed Countermeasures
- Selection of Countermeasures

Collaborative Services
- Forum
- Wiki
- E-Library
- Chat Rooms
- Blog

Security Documents
- Design Security Policy
- Design DRP

Security Team
Managers
Administrators
Local Users

Local Users
## List of E-Services

<table>
<thead>
<tr>
<th>Code</th>
<th>Name</th>
<th>Description</th>
<th>Manager Name</th>
<th>Manager Last Name</th>
<th>Manager Email</th>
<th>Created at</th>
<th>Updated at</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>service1</td>
<td>service1</td>
<td>Description</td>
<td>Manager</td>
<td>Lastame</td>
<td>email1</td>
<td>10/24/2011</td>
<td>06/02/2012</td>
<td></td>
</tr>
<tr>
<td>service2</td>
<td>service2</td>
<td>Description</td>
<td>Name</td>
<td>Lastame</td>
<td>email3</td>
<td>10/24/2011</td>
<td>06/02/2012</td>
<td></td>
</tr>
<tr>
<td>service3</td>
<td>service3</td>
<td>Description</td>
<td>Name</td>
<td>Lastame</td>
<td>email4</td>
<td>10/27/2011</td>
<td>06/02/2012</td>
<td></td>
</tr>
<tr>
<td>service4</td>
<td>service4</td>
<td>Description</td>
<td>Name</td>
<td>Lastame</td>
<td>email</td>
<td>11/03/2011</td>
<td>06/02/2012</td>
<td></td>
</tr>
</tbody>
</table>
## Final Impact Results

<table>
<thead>
<tr>
<th>Availability</th>
<th>Confidentiality</th>
<th>Integrity</th>
<th>Total Value</th>
<th>Asset</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.5</td>
<td>1.9</td>
<td>2.5</td>
<td>2.6</td>
<td>Financial Data</td>
<td>Organization 1</td>
</tr>
<tr>
<td>0.4</td>
<td>3</td>
<td>0.6</td>
<td>3</td>
<td>Customer Data</td>
<td>Organization 1</td>
</tr>
<tr>
<td>0.4</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>Data2</td>
<td>Organization 1</td>
</tr>
<tr>
<td>0.4</td>
<td></td>
<td></td>
<td>0.4</td>
<td>data1tris</td>
<td>Organization 1</td>
</tr>
</tbody>
</table>

### Impact Assessment for the assets of SERVICE:

#### Bar Graph

**service1**
- **Financial Data**
  - Availability: 2.6
  - Confidentiality: 1.9
  - Integrity: 2.5

**Customer Data**
- Availability: 0.4
- Confidentiality: 3
- Integrity: 0.6
Risk Assessment Results: June 2, 2012 10:36:58 AM EEST

Risk Assessment Results - Per Asset

Click the columns to view the risk values. Click again to view max values of assets.

Financial Data: 4 Risk Value
Click to view Financial Data risk values

3 Risk Value

2 Risk Value
## Forums

<table>
<thead>
<tr>
<th>Forum</th>
<th>Topics</th>
<th>Messages</th>
<th>Last Message</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Public Boards</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Cartography</strong></td>
<td>1</td>
<td>2</td>
<td>test no222 4 days ago by demo</td>
</tr>
<tr>
<td><strong>Risk Assessment</strong></td>
<td>1</td>
<td>1</td>
<td>test2 4 months ago by teo</td>
</tr>
<tr>
<td><strong>Disaster Recovery Plan</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Disaster Recovery Managers

<table>
<thead>
<tr>
<th>DRP Phase</th>
<th>Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Development</td>
<td>• Oversee the documenting, publishing and dissemination of DRP</td>
</tr>
<tr>
<td></td>
<td>• Update the DRP manual when infrastructure, operations or organisation changes in Computer Centre impact the DRP.</td>
</tr>
<tr>
<td>Testing</td>
<td>• Schedule, organise and staff DR tests in collaboration with Disaster Recovery teams, on fixed schedule or when need arises</td>
</tr>
<tr>
<td>Normal Operation</td>
<td>• Update DRP and DR Handbook via Change Management procedures when infrastructure, operations or organization changes in Computer Centre impact the DRP</td>
</tr>
<tr>
<td></td>
<td>• Ensure DRP terms and policies are applied at all levels in Computer Centre</td>
</tr>
<tr>
<td></td>
<td>• Escalate issues to DR Steering Committee, when its intervention is needed. Issues may involve policy or technical aspects</td>
</tr>
<tr>
<td></td>
<td>• Meet DR team members at regular intervals for update on issues potentially impacting the viability of the DRP</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Role</th>
<th>Name</th>
<th>Address</th>
<th>Cell Phone</th>
<th>R/S Desk Loc</th>
</tr>
</thead>
<tbody>
<tr>
<td>DR Coordinator</td>
<td>Theodore Ntouskas</td>
<td>karaoli 2</td>
<td>25252525</td>
<td>main site</td>
</tr>
</tbody>
</table>

**PDF**
1. Introduction

This section provides an introduction to the principles of risk management. The vocabulary of risk management is defined in ISO Guide 73, "Risk management: Vocabulary." [2] home

In ideal risk management, a prioritization process is followed whereby the risks with the greatest loss and the greatest probability of occurring are handled first, and risks with lower probability of occurrence and lower loss are handled in descending order. In practice, the process can be very difficult, and balancing between risks with a high probability of occurrence but lower loss versus a risk with high loss but lower probability of occurrence can often be mishandled.

Intangible risk management identifies a new type of a risk that has a 100% probability of occurring but is ignored by the organization due to a lack of identification ability. For example, when deficient knowledge is applied to a situation, a knowledge risk materializes. Relationship risk appears when ineffective collaboration occurs. Process-engagement risk may be an issue when ineffective operational procedures are applied. These risks directly reduce the productivity of knowledge workers, decrease cost effectiveness, profitability, service, quality, reputation, brand value, and earnings quality. Intangible risk management allows risk management to create immediate value from the identification and reduction of risks that reduce productivity.

Risk management also faces difficulties allocating resources. This is the idea of opportunity cost. Resources spent on risk management could have been spent on more profitable activities. Again, ideal risk management minimizes spending and minimizes the negative effects of risks.

Method

For the most part, these methods consist of the following elements, performed, more or less, in the following order.

1. Identify, characterize, and assess threats
2. Assess the vulnerability of critical assets to specific threats
3. Determine the risk (i.e. the expected consequences of specific types of attacks on specific assets)
4. Identify ways to reduce those risks
5. Prioritize risk reduction measures based on a strategy
Generic conclusions and some proposals

- S-Port is a useful asset for the security management of the PIS, providing continuity and rendering of services.
- With S-Port, Port Authorities and their IS will adopt all the rules and procedures of the ISPS Code, thus reducing possibility of threats and maximizing their productivity.
- Collaborative Risk Management methodologies need to be further developed.
- Maritime interoperable Security Management Tools (MSMT) (like S-Port) should be developed so as to:
  - Implement the MSMM as collaborative friendly interoperable services (based on open standards)
  - Be cost effective (open source)
  - Enable collaboration among users in the maritime environment.
References


