The value of information sharing for the port sector

Chronis Kapalidis
Academy Associate, Chatham House
Europe Representative, HudsonAnalytix
World Economic Forum Report 2019
Our growing dependency on IoT

The number and type of IoT devices and associated services are growing rapidly, with forecasts suggesting that there will be approximately twenty to one hundred billion IoT devices worldwide in 2020.
Main aspects of digital transformation

- communication
- data management
- operations management
### Key findings (Facts & Figures)

<table>
<thead>
<tr>
<th>Date</th>
<th>Victim</th>
</tr>
</thead>
<tbody>
<tr>
<td>2010-11</td>
<td>Greek Shipping Company</td>
</tr>
<tr>
<td>Aug 2011</td>
<td>Iranian Shipping Line (IRISL)</td>
</tr>
<tr>
<td>2011-13</td>
<td>Port of Antwerp</td>
</tr>
<tr>
<td>2012</td>
<td>Australian Customs and Border Protection Service agency</td>
</tr>
<tr>
<td>2012-14</td>
<td>Danish Port Authority</td>
</tr>
<tr>
<td>Apr 2016</td>
<td>South Korea</td>
</tr>
<tr>
<td>Jun 2017</td>
<td>AP Moller Maersk</td>
</tr>
<tr>
<td>Jun 2017</td>
<td>Ships in Novorossiysk</td>
</tr>
<tr>
<td>Nov 2017</td>
<td>Clarksons</td>
</tr>
<tr>
<td>July 2018</td>
<td>Cosco US</td>
</tr>
<tr>
<td>Sep 2018</td>
<td>Ports of Barcelona &amp; San Diego</td>
</tr>
</tbody>
</table>

~97% of malware is designed to exploit social engineering weaknesses, not a technical flaw.
Port’s cybersecurity ecosystem
Chatham House Maritime Cybersecurity Research 2019: Vulnerabilities & Consequences
Chatham House Maritime Cybersecurity Research 2019: Affected Fields
It is all about the maritime supply chain risk....

Economic damage to the world economy on 15 Asian ports:

from $40.8 to $109.8 billion
Smart Marine Ecosystem

- The port as part of a modern integrated ecosystem
- Port applications include smart traffic lights, smart parking, predictive maintenance
- Benefits include: Facilitated Data Exchange, Improved Traceability, Optimized Navigation and Route Planning
Information Sharing

- The challenge has been to convince companies to share information
- Collaboration for IT and OT systems

- Benefits include:
  - Holistic view on IT/OT convergence
  - Raise awareness on threats & vulnerabilities
  - Smoother integration of systems
Sea Traffic Management

- Information exchange project between ships, service providers, ports and others
- Facilitates onboard and ashore decision-making based on real-time data
- Examples include: Route Optimisation, Ship2Ship route exchange, Enhanced Monitoring, Port Call Synchronisation, Winter Navigation
Who Owns Cyber Risk?

- **Shareholders, PE, Partners, Shipowners**: Evaluate and Fund Risk (In terms of Investment decisions)
- **Board of Directors**: Evaluate and Fund Risk (Minimize losses; support/protect shareholder equity)
- **Business Leaders (CEOs, MDs)**: Manage Risk (Profit and Loss / Balance Sheet)
- **Risk Leadership (Counsel, Risk Mgr.)**: Identify, Prevent, Accept, and Transfer Risk (Insurance; Agreements and Contracts in terms of and risk to Profit and Loss and Balance Sheet)
- **Security Leadership**: Validate Risk, Allocate Resources (In terms of cyber risk to operations and Profit and Loss)
- **Security Practitioners**: Communicate Needs, Solutions (In terms of cyber risk to operations that supports cash flow and profit and loss)
A security awareness program does not exist. Employees have no idea that they are a target, they do not know nor understand organization security policies, and they easily fall victim to cyber or human-based attacks.

**Compliance-focused:** Your security awareness program is designed primarily to meet specific compliance or audit requirements. Training is limited on an annual or ad-hoc basis. Employees are unsure of organization policies, their role in protecting their organization’s information assets, and how to prevent, identify, or report a security incident.

**Promoting awareness and behavioral change:** Your program identifies the training topics that have the greatest impact in supporting the organization’s mission and focuses on those key topics. The program goes beyond annual training to include continual reinforcement through the year. Content is communicated in an engaging and positive manner that encourages behavior change at work, home, and while traveling. As a result, employees are aware of organizational policies and actively recognize, prevent, and report incidents.

**Long-term sustainment and cultural change:** The program has processes and resources in place for a long-term life cycle, including (at a minimum) an annual review and update of both training content and communication methods. As a result, the program becomes an established part of the organization’s culture and has changed people’s beliefs, values, and perceptions on security. Keep in mind it takes 3-10 years to have a strong, measurable impact to culture.

**Metrics framework:** Your program has a robust metrics framework in place to track progress and measure impact. As a result, your program is continuously improving and can demonstrate return on investment. Note: Having metrics in the last stage does not imply metrics come into play only at the end of the maturity model. Metrics are an important part of every stage. However, this stage reinforces that to have a truly mature program, you must not only be changing behaviors and culture, but also have the metrics to demonstrate that.
WE THINK IT'S TIME FOR YOU TO COME SIT AT THE BIG KIDS' TABLE!!!