A Holistic Approach to Maritime Cyber Risk Management and Proactive Pre-Breach Preparation

13 – 15 November 2019
Who We Are

Who We Are:
• Trusted Best-in-Class partners
• Technology / vendor agnostic
• Global Reach

What We Offer:
• Enterprise assessment approach - the HACyberLogix
• Tailored cyber threat intelligence - informed by “attack side”
• Customized Cyber Training
Current State: Low Cybersecurity Capability Translates into High Organizational Cyber Risk

Objective: To bring Maritime Organizations Down the Cyber Risk Reduction Curve

Investing in the right combination of technology and insurance maximizes risk reduction.

1. Technology Risk Reduction
2. Insurance Risk Reduction

Image Courtesy of Axio

© 2019 HudsonAnalytix, Inc.
Limited Experience, No Historical Precedent and Resource Misalignment

Common questions we get from our clients include:
• *Where do we start?*
• *What do we invest in first?*
• *How much do we budget?*
• *What are our priorities?*
• *How can we measure the effectiveness of our investments?*
• *Are our investments sustainable?*
• *Who owns cybersecurity?*
So What’s Vulnerable to Cyber Threats in the Maritime Industry?  (Hint: Everything)

- Supervisory Control & Data Acquisition (SCADA) equipment and Industrial Control Systems (ICS) for loading / unloading of bulk / containerized cargo
- Cargo / Terminal Operating Systems
- Domain Awareness Systems - RADAR, AIS, VTS/VTMS, GIS Systems
- *Any* Business Software Application (e.g. email, financial, human resources, finance, logistics, business operations. Think “ERP”)
- *Any* Operating System (e.g. Microsoft, Linux)
- *Any* Security System - CCTV, Access/Gate Control
- *Any* Mobility device and platform (RFID)
- Communications Systems
- Employees (insiders) and Contractors
<table>
<thead>
<tr>
<th>NIST CSF Functional Category</th>
<th>CSF Category</th>
<th>IMO Clause (Category)</th>
<th>IMO Clause Description</th>
</tr>
</thead>
</table>
| **Identify**                | • Asset Management  
• Business Environment  
• Governance  
• Risk Assessment  
• Risk Management Strategy | Identify (3.5.1)      | Identify: Define personnel roles and responsibilities for cyber risk management and identify the systems, assets, data, and capabilities that, when disrupted, pose risks to ship operations |
| **Protect**                 | • Access Control  
• Awareness & Training  
• Data Security  
• Information Protection Processes & Procedures  
• Maintenance  
• Protective Technology | Protect (3.5.2)       | Protect: Implement risk control processes and measures, and contingency planning to protect against a cyber event and ensure continuity of shipping operations |
| **Detect**                  | • Anomalies & Events  
• Security Continuous Monitoring  
• Detection Processes | Detect (3.5.3)        | Detect: Develop and implement activities necessary to detect a cyber event in a timely manner.                                                                                                                        |
| **Respond**                 | • Response Planning  
• Communications  
• Analysis  
• Mitigation  
• Improvements | Respond (3.5.4)       | Respond: Develop and implement activities and plans to provide resilience and to restore systems necessary for shipping operations or services impaired due to a cyber event. |
| **Recovery**                | • Recovery Planning  
• Improvements  
• Communications | Recover (3.5.5)       | Recover: Identify measures to back-up and restore cyber systems necessary for shipping operations impacted by a cyber event.                                                                                 |
Characterizing Notable Cyber Events in the Maritime Sector and Their Consequences

IRISL – Enterprise Business Interruption (2011)
Entire fleet of 172 vessels and all shore-based systems impacted; servers compromised; logistics systems crashed; and key data manipulated and monitored. Consequences: Unknown

Antwerp – Threat Ecosystem Convergence (2011-13)
Hacking technique involved physical access to computer networks and installation of snooping devices. Organized criminals and hackers maintained persistent access to terminal operating systems. Consequences: Liability Exposure, Crime

Maersk – Nation State Attack / Collateral Damage (2017)
NotPetya attack encrypted master boot records (destructive); required 4,000 new servers, 45,000 new PCs, and 2,500 applications. Consequences: Uninsured losses likely 350 million+.

Various – Spear-Phishing / Business Email Compromise (BEC) (Ongoing)
Nigerian fraudsters, through such global campaigns as Gold Galleon and the Daily Show, represent chronic threats to the maritime industry. The harvesting, curating and re-sale of valid credentials contributes to the dark web economy and continued growth of the cyber threat landscape. Consequences: Chronic
Can Cyber Threats Affect a Vessel’s Seaworthiness?

Courtesy: US Coast Guard
Past as Future? The Mortgage Crisis and the “Cyberization” of Risk

Bankers concentrated risks via “securitization”
- Risks were repackaged/sold to others.
- Buyers continued the process of repackaging
- Eventually no one knew:
  - Who owned the final risk?
  - Who was exposed?
  - Where and how the risks were concentrated?
Estimating the Cost of Cybercrime

It’s estimated that 0.8 per cent of global GDP is now being lost to cybercrime. - McAfee

Over the next 5 years, companies in the private sector risk losing an estimated USD $5.2 trillion in value creation opportunities from the digital economy – almost the size of the economies of France, Italy and Spain combined – to cyber attacks.

- Accenture

Revenue generation in the cybercrime economy takes place at a variety of levels – from large multinational operations that generate profits over $1 billion, to smaller scale operations where profits of $30,000 – 50,000 are the norm.

- Bromium
So Who Owns Cyber Risk?

- Shareholders, PE, Partners, Commissioners: 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)
“Ten years ago you couldn’t defend yourself. Today there are companies successfully defending themselves. We know what the solutions are – they’re no secret. **If you don’t spend money to defend yourself you will be hacked.**”


---

**Notable Fines***:

- Equifax: $575-700 million
- British Airways: £183 million
- Uber: $148 million
- Yahoo: $85 million
- Tesco Bank: £16.4 million

*Currently being negotiated as of July 2019

(Source: https://www.youtube.com/watch?v=CxMBVboJTo)
Consider cyber risk in terms of *money*

*The cyber-risk-to-money intersection offers measurable value to inform resource prioritization*

Financial grounding translates cyber risk into common language

Empowers decision-makers with relevant context and inputs so as to make informed decisions on cyber risk
The volume of IoT attacks remained high in 2018. **Routers and connected cameras** were the most infected devices and accounted for 75 and 15% of the attacks, respectively.

- Symantec 2019 Internet Security Threat Report
Key Challenge: Business Leaders Require the Insights Necessary to Make Informed Decisions

- What is my cyber exposure (internally? externally?)?
- What are my most critical assets and are they at risk?
- Are my cyber defense and response capabilities mature?
- Do I have the financial ability to recover from an event?
Enterprise Cybersecurity Capability Maturity defines an organization’s *cyber ecosystem*, identifies the depth and breadth of deployed capabilities, establishes benchmarks to support long-term measurement, and serves as the primary mechanism for sustaining the organization’s cybersecurity strategy and investments.
Cybersecurity capability maturity analysis provides:

- A *structure for consistently assessing* all functional areas of the business
- A *methodology that supports* benchmarking and trend analysis
- A means for *identifying strengths and weaknesses across the entire business*
- A *method for prioritizing investments and allocating resources*
- A mechanism for *sharing knowledge and driving cultural change*
Thank You!

Ferry Terminal Building
Suite 300
2 Aquarium Drive
Camden, NJ 08103

Office: +1.856.342.7500
Mobile: +1.609.505.6878
Email: cynthia.hudson@hudsonanalytix.com

Cynthia Hudson
Founder & CEO

© 2019 HudsonAnalytix, Inc.