Framing the Discussion: A World of Cybersecurity Risks

John Duncan
Vice President
Global Government Sector
ABS Group
Basic Elements of Risk

Risk Understanding

How likely is it?  
What can go wrong?  
What are the impacts?

Risk = $\Phi$ [Threat, Vulnerability, Consequence]

Foundation for Risk Assessment

<table>
<thead>
<tr>
<th>Historical Experience</th>
<th>Analytical Methods</th>
<th>Knowledge &amp; Intuition</th>
</tr>
</thead>
</table>

ABS Group
Simple Security Risk Model

Risk = \( f \) [Threat, Vulnerability, Consequence]

- **Scenario** – combination of a target and attack mode
- **For each scenario, assess the following:**
  - **Threat** – likelihood of a specific attack
  - **Vulnerability** – probability that the attack will be successful
  - **Consequence** – level of impact associated with a successful attack
NIST Framework Overview

• In February 2013, President Obama issued Executive Order 13636: *Improving Critical Infrastructure Cybersecurity*

• Called for NIST to lead a collaborative effort to develop voluntary, risk-based Cybersecurity Framework
  – Set of existing standards, guidelines and practices to help organizations manage cyber risks.
### NIST Framework Core

- Developed as guidance for a specific critical infrastructure component
- Contains valuable information for government agencies
- NIST framework identifies 5 major cybersecurity functions

<table>
<thead>
<tr>
<th>Functions</th>
<th>Categories</th>
<th>Subcategories</th>
<th>Informative References</th>
</tr>
</thead>
<tbody>
<tr>
<td>IDENTIFY</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PROTECT</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DETECT</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RESPOND</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RECOVER</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Includes a Risk Assessment Category
Cyber Threats to Maritime Entities

Tiffany Jones, CISSP, CIPP
SVP & Chief Revenue Officer, iSIGHT Partners
tjones@isightpartners.com
Primary Threat Categories

Cyber Crime

Hacktivism

Cyber Espionage
Scenarios: Setting the Geopolitical Context

Geopolitics drives espionage activity
Naval and Coast Guard Threats
Benign lure document from Mirage RAT sample deployed ahead of US-Philippine defense agreement (iSIGHT Partners)
The 2015 Arctic Energy Summit is a multi-disciplinary event expected to draw several hundred industry officials, scientists, academics, policy makers, energy professionals and community leaders together to collaborate and share leading approaches on Arctic energy issues.
Chinese New Year-themed lure document sent to Japan Maritime United Corporation employee (iSIGHT Partners)
• 3+ year Cyber-espionage campaign with links to Iran
• Targeting high and low ranking personnel in multiple countries – US, UK, Israel, Saudi Arabia, Iraq
  – U.S. military
  – Congressional personnel
  – Washington D.C. area journalists
  – Diplomatic corps
  – U.S. Defense contractors
  – Israeli Defense contractors
  – Members of the U.S./Israeli lobby

• Utilizing social media platforms as targeting platform
  – Facebook
  – LinkedIn
  – YouTube
  – Etc.

• More than 2,000 targets and legitimate individuals caught in the net
  – Credential harvesting
  – Access to corporate and personal emails
  – Malware with data exfiltration capabilities
Risk Panel - Vulnerabilities

Ronin Security Solutions
Andrew N Bertolazzi
Environment

• Ever-expanding cyber tools and connections
• Most popular passwords in 2013: “password”, “123456”
• “We aren't even doing the simple stuff” Sen. Coburn-2014
• CIOs: Hacking is going to happen. Plan for it (2015)
• All software has flaws
• Macro versus micro vulnerabilities
• People are the critical common factor
Maritime Terminal Realities

- Reliance on cyber-linked tools, equipment, systems
- e-Commerce and online filings
- Increasing need for tech-savvy workforce
- Shrinking margins, reduced staff, higher workload
- Make-up of IT and Security organizations
- Divergent priorities, mandates, and funding
- Port focus has been primarily on physical security
- Few Business Continuity or Disaster Recovery Plans
Typical Vulnerabilities

- Economic and strategic “soft” targets
- Flat, lean organizations – single point failures
- Cyber-connected control systems, equipment, data
- Low security of networks, WiFi, back-up, hardware
- Inadequate password practices
- Limited funds, shrinking PSGP pool
- Security is a cost – financial and operational
- People
What Can Be Done?

Processes
- Robust plans for Business Continuity & Disaster Recovery
- Regular, secure, offsite back-up
- Access controls for data – physical and cyber
- Password discipline

Tools
- Firewalls, segmented networks, intrusion detection
- Timely and complete updates, patches, & fixes

People
- Awareness, training, exercises
- Security consciousness (a bit of paranoia goes a long way)
- Outside help
Resources

- Homeport Cyber-Security Webpage
  https://homeport.uscg.mil/mycg/portal/ep/home.do

- US Computer Emergency Readiness Team (US-CERT)
  https://www.us-cert.gov

- Industrial Control Systems - Cyber Emergency Readiness Team
  https://www.ics-cert.us-cert.gov

- National Institute of Standards and Technology (NIST)
  http://www.nist.gov/cyberframework/index.cfm

- Software & Supply Chain Assurance Clearinghouse (DHS)
  https://buildsecurityin.us-cert.gov/swa/cwe
Risk Panel - Consequences

Captain Joe Kramek
Eleventh Coast Guard District
Legal Officer & Staff Judge Advocate
# Case Study – National Impact of West Coast Port Stoppage (29 ports)

<table>
<thead>
<tr>
<th></th>
<th>5 Days</th>
<th>10 Days</th>
<th>20 Days</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cost to U.S. Economy</td>
<td>$1.9 B</td>
<td>$2.1B</td>
<td>$2.5B</td>
</tr>
<tr>
<td>Loss of Imports</td>
<td>$1.8 B</td>
<td>$3.9 B</td>
<td>$8.3 B</td>
</tr>
<tr>
<td>Loss of Exports</td>
<td>$1.5 B</td>
<td>$3.2 B</td>
<td>$6.9 B</td>
</tr>
<tr>
<td>Reduced Economic Output</td>
<td>$9.4 B</td>
<td>$21.2 B</td>
<td>$49.9 B</td>
</tr>
<tr>
<td>Cost to Households</td>
<td>$81</td>
<td>$170</td>
<td>$366</td>
</tr>
<tr>
<td>Employment Disruption</td>
<td>73,000</td>
<td>169,000</td>
<td>405,000</td>
</tr>
</tbody>
</table>
Immediate Backlog Across Economy

- Automakers – More Expensive Parts / Reduced Production
  - Honda, Toyota & Subaru
- Wal-Mart Inc. – Reduced Inventory /Earnings Hit
  - Electronics
- U.S. Meat Exporters – millions of pounds in storage
  - $85 mil per week
- Farmers – Losses estimated in hundreds of millions
  - CA citrus exports cut by half
  - WA apple crops
Questions for Panel