Managing Cyber Risk

Captain Andrew E. Tucci
U.S. Coast Guard
Ships Then
Ships Now
Cargo Operations Then
Cargo Operations Now

- Cargo handling equipment at the port/railway interface
- Commercial Long-Haul Trucks
- Port Security and Access Controls (physical, CCTV, gates, TWIC, ID cards)
- Container Cranes (or liquid cargo handling systems at oil, chemical and LNG terminals) at vessel/port interface
- Automated cargo handling equipment, vehicles and similar conveyances
- Automated Cargo Container Tracking Systems
- Terminal Operating Center (financial, communications, customs, security and other back office functions)
- Shore-based systems that directly support safe vessel operation and navigation:
  - GPS
  - Lock operation
  - Communications
  - Maintenance and management
  - Systems aboard USCG vessels, tugs, fire boats, port police
  - Pollution response systems
What is at risk?

• Navigation Systems (GPS, AIS, ECDIS)
• Industrial Control/SCADIA
• Communications, Sensors/monitoring
• Engine Management Systems
• Fire detection, fire suppression, WT doors
• Ballast/stability
• Cargo control
Who?

- Cyber Espionage by Foreign Intelligence Services
- Lone hackers & Hacktivists Groups
- Criminal Networks
- Insider Threats
- Simple technical failure
How?

- Hidden, powerful Wi-Fi devices on ships
- Easily available GPS jamming devices
- Cyber Crime as a service
- Crew/employee conduct
- Technical error/failure
What Makes Cyber Risk Special?

Vulnerability increases with every new device

Threat is unlimited

Likelihood of an incident is near certain

Detection is a factor

rapidly growing portion of our total risk exposure
Identify Your Risk

- Assemble a team: IT personnel, operators, emergency management
- Why not just IT personnel?
- Inventory your systems and map your network
- Be honest about what is “connected”
- Think hackers, insiders, and tech error.
- What could go wrong?
- Murphy Rules!
Reduce Your Vulnerability

- Engineering Solutions
- Training and company policies
- Physical Access control
- Technical solutions
Reduce Consequences

- Continuity of Business Operations Planning
- Manual Backups
- Response and Recovery Plans
- Employee procedures
- Who will you call for help?
- How about an exercise?

A plan can keep you in business!
Use the resources that are available

- ICS Alerts
- ICS Advisories
- ICS-CERT Monitor Newsletters
Cyber Security Risk Model

Various Attack Types
- APT/Organized Crime
- Hacktivists
- Insiders
- Technical Error

Prevention/Protection Measures
- Technical controls
- Policy controls
- Physical controls
- Defense in depth

System Failure

Mitigation Measures
- Recovery & Continuity of Business Planning
- Manual Back ups
- Notifications & Communications
- Exercises & Contingency Plans

Impacts
- MTS Disruption
- Environmental
- Property Damage
- Human life, safety, health

All activities must take place systematically and against a backdrop of the training, education, and policies needed to promote a culture of cyber security.
Questions?