Cyber Risk in the Marine Transportation System

Cubic Global Defense

Cubic.com/Global-Defense/National-Security
Cubic Global Defense
Global Security Team Capabilities

• Program Management
  • Integration of Effort

• Technical Support
  • Science and Technology Solutions
  • Plan Development
  • Instructional Design
  • Systems Analysis
  • Civilian and Military Coordination
  • Threat / Hazard Assessment
  • Business & Government Continuity

• Training, Exercises, Workshops, etc. to include virtual training: Firepump_coupling_Maintenance.mp4
What is Cybersecurity?
Cybersecurity Defined

Cybersecurity can be defined as:

“the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user’s assets.”
Impacts of Exploiting Cyber in MTS

- Financial loss
- Terminal and / or port shutdowns
- Economic disaster
- Environmental catastrophes
- Loss of life
Maersk Attacked June 2017

- A.P. Moeller-Maersk is the world’s largest shipping company, handing ~15% containers globally
- NotPetya ransomware demands $300 (US) Bitcoin payment, but not effectively
- Started in Ukraine
- Affected all business units at Maersk
  - Container shipping, port and tug boat operations, oil and gas production, drilling services and oil tankers
- Global impact: 15 ports
Hackers Used Cyber to Facilitate Drug Smuggling

By breaking into the offices of a harbor company, the criminals could install key-loggers to take control of computers.

Computers of container terminal were hacked so the containers that contained drugs could be monitored.

By means of false papers and a hacked pin code, the drivers were able to pick up the container at a location and time of their choosing.

1044 kilos cocaine/1099 kilos heroin
Targets of Cyber Attacks

Data
- Change data
- Steal data

Cyber Infrastructure
- Launch attacks against you or others

Physical Infrastructure
- Manipulate physical security controls
- Physical destroy systems
Starting the Conversation

- Levels of interest vary
- Cyber should be a topic in all security discussions
  - Physical and cybersecurity convergence
- Not just an issue for information technology staff
- Several frameworks and industry best practices available
- Most organizations struggle to adapt these best practices due to time and expertise restraints
Authority & Jurisdiction

• Identify legal and regulatory requirements
• Approach cyber issues with a risk management approach
  • Cyber is another operational domain.
Strategy for Improvement

**Assessment**
- Assess for vulnerabilities
- Compare to industry best practices

**Develop Policy**
- Develop policies and procedures that fit organizational needs
- Create strategies for future projects, training, etc.

**Exercise**
- Put your new policies to the test
- Learn the hard lessons in an exercise vs. a real event

**Upkeep**
- Periodically re-evaluate your security program against latest threats and standards
- Continue exercising and maintaining your plans, plus ongoing training for employees
Cybersecurity Assessment

• Clearly identify your assets
  • Hardware
  • Software
  • Network configurations
  • Sensitive data
• Gauge your current cybersecurity policy (if any)
• Gauge your employee training program
• Compare against industry standards
National Institute of Standards & Technology

Identify
- Asset Management
- Business Environment
- Governance
- Risk Assessment
- Risk Management Strategy

Protect
- Access Control
- Awareness and Training
- Data Security
- Info Protection: Policies and Procedures
- Maintenance
- Protective Technology

Detect
- Anomalies and Events
- Security Monitoring
- Detection Processes

Respond
- Response Planning
- Communications
- Analysis
- Mitigation
- Improvements

Recover
- Recovery Planning
- Improvements
- Communications
Cybersecurity Policy

• Cybersecurity policy will:
  – Address the issues identified in the assessment
  – Address human and technological assets
  – Be *customized* to build upon the existing port facility security plan (PFSP)
  – Allow for periodic review and update to address emerging threats and new standards
Upkeep

• In August, the National Institute of Standards and Technology (NIST) changed the best practice for passwords.

P@ssSw0rd45*

Strongpasswordsarethebest!😊
Cybersecurity Training

• General awareness training
• Need for initial and periodic cybersecurity training
• Culture
Exercise

• Put policies to the test
• Identify weaknesses
• Establish a positive culture
• Practice makes perfect
Solutions

• Seek help!
• Assess the current state of systems
• Build a cybersecurity plan that is consistent with best practices
• Create realistic steps to remedy the vulnerabilities found in the assessment
  – Adding technology, manpower, training
• Enforce the plan, update regularly
• Empower all employees as defenders
• Repeat
Questions or Comments

Contact Information:
Katey Groves & Cece Garcia
Katey.Groves@cubic.com
Cubic Proprietary