Marine Terminal Management Training Program

INSURANCE TRENDS AND LOSS MITIGATION STRATEGIES

AAPA Port Administration and Legal Issues Seminar

Hyatt Regency Philadelphia
201 S. Columbus Blvd.
Philadelphia, PA
October 8, 2014, 2:00 pm-3:00 pm

ROBERT M. HORKOVICH, ESQ.
Chair, Insurance Recovery Group
(212) 278-1322
rhorkovich@andersonkill.com
DISCLAIMER

The views expressed by the participants in this program are not those of the participants’ employers, their clients, or any other organization. The opinions expressed do not constitute legal advice, or risk management advice. The views discussed are for educational purposes only, and provided only for use during this session.
INSURANCE TRENDS

- Cyber Risk/Insurance
- Terrorism
- Infectious Diseases/Ebola
- Climate Change
DATA SECURITY BREACHES
WHAT ARE THE CAUSES?

- Negligence – 35%
- Malicious or Criminal Attack – 37%
- System Error – 29%\(^1\)

WHAT ARE THE EFFECTS?

- Information Loss – 44%
- Business Disruption – 30%
- Revenue Loss – 19%
- Equipment Damages – 5%
- Other Miscellaneous Costs – 2%²

²2013 Cost of Data Breach Study: Global Analysis, Ponemon Institute, May 2013.
WHAT'S THE COST?

AVERAGE RESOLUTION TIME: 24 days

AVERAGE COST: $5.4 Million

---

THIRD-PARTY DATA MANAGEMENT & RISKS

• Cloud is the Trend
• Cost Savings
• Data Security Risks
• Lack of Control
• Can delegate the data management but not the responsibility
• What are the risks; Amazon/Sony Breach
BEST PRACTICE

- SEC Guidance
- FFIEC Guidance
- Due Diligence on Vendors
- Negotiate Strong Terms in Vendor/Cloud Contracts
- Risk Transfer Indemnity/Insurance
- Security Assessment of Vendor: Tricky in a Multi-Tenant Cloud Platform
- Make Sure There is Adequate Notice/Disclosure of Use of Cloud to Stakeholders
• Notice of Incident (even if your data is not disclosed)
• Cooperation with regulation authorities and law enforcement
• Periodic audit rights
• Notification costs responsibility
• Costs of computer forensic experts
• Use of sub-contractors
• Cloud Services Termination: How does hosted data get disposed of? / Who pays?
• Representations and Warranties about firm protecting data
SECURITY & INSURANCE

- Encryption
  - Automatic red flag for AGs/FTC if data disclosed and not encrypted
- Contractual Indemnity/Hold Harmless
- Mandate insurance purchase by vendor
- Require additional insured status
POLICIES COVERING LOSS

- Take Inventory of Policies
- 1\textsuperscript{st} Party, 3\textsuperscript{rd} Party, Hybrid Coverage Issues
TYPES OF INSURANCE POLICIES

- Errors & Omissions Liability
- Directors & Officers Liability
- General Liability
- Umbrella Liability
- Broad Form Property
- Cyber Extensions on FIB/Fidelity
- Specialized Cyber (other panel)
COVERAGE UNDER CGL?

- IP Exposure
- Data Loss
- Business Interruption
- Third Party Losses
- Privacy
WHEN CONVENTIONAL COVERAGE IS NOT ENOUGH

CYBER POLICIES!
CURRENTLY AVAILABLE CYBER INSURANCE

- Privacy Injury Liability
- Privacy Regulatory Proceedings and PCI Fines
- Network and Content Liability
- Crisis Management Fund
- Network Loss or Damage
- Business Interruption
- Electronic Theft
- Network Extortion
THINGS TO DO

• Understand your exposure.
• Review your insurance policies and request extensions of cyber/data/electronic coverage on existing policies.
• Avoid new exclusions.
• Avoid gaps.
• Enlist an expert consultant or broker.
• Consider panel on cyber policies.
• DO NOT TAKE “NO” FOR AN ANSWER!

Look for Conference Updates at #PHA14
TERRORISM RISK INSURANCE ACT (TRIA)

- Enacted in 2002.
- Extended but set to expire on 12/31/2014.
- Bill to extend TRIA is in committee.
TRIA

- Creates a federal “backstop” for insurance claims related to terrorist acts.
- Requires insurance companies to offer terrorism coverage.
- Created a U.S. government reinsurance facility to provide reinsurance coverage to insurance companies in the event of a terrorist act.
- $100 billion per year cap.
TERRORISM INSURANCE

- Fire exclusion following terrorist act precluded by at least 9 states including New York, California, and Illinois.
- Insurance companies that offer workers’ compensation coverage are required to offer terrorism coverage to their clients.
RECOMMENDATIONS

- Negotiate full term terrorism insurance from your insurance companies.
- Review language imposing candidates in which terrorist act losses would be excluded.
- Consider stand alone terrorism insurance to cover gaps in insurance program should TRIA expire.
- Expect severe supply line disruptions in case of a terrorist act.
INFECTIONOUS DISEASES

Look for Conference Updates at #PHA14
• Deadliest virus in history (55% fatalities after infection).
• Company exposures: Personal/Business Interruption.
• Potential global supply chain interruptions.
• Potential port closure or curtailments.
ANALOGY

Coverage for clean-up and removal of property due to the hantavirus in tents in National ports.
RECOMMENDATION

• Protect health and safety of employees.
• Consider supply chain alternatives.
• Maintain general liability insurance coverage for claims of negligence. Watch for exclusions for infectious diseases/bacteria.
• Maintain D&O coverage for claims by investors that you inadequately prepared or acted.
• Maintain property/business interruption insurance.
• Maintain records of any physical impact (closure for clean-up of contamination).

Look for Conference Updates at #PHA14
Look for Conference Updates at #PHA14
RISING WATER LEVELS

Look for Conference Updates at #PHA14
MORE FREQUENT AND INTENSE STORMS

2012
Superstorm Sandy
86th Street Subway NYC

2005
Hurricane Rita
Coastal Texas

2005
Hurricane Katrina
I-10/I-610/West, Louisiana

Look for Conference Updates at #PHA14
LOSS MITIGATION

- Emergency response plan.
- Identify operations and assets most at risk.
- Pre-loss checklists.
- Update valuations.

Look for Conference Updates at #PHA14
ANALYSIS
IDENTIFY THE TYPES OF RISKS A TERMINAL OPERATOR IS EXPOSED TO:

- Partial or total loss of, or damage to, your property.
- Loss of income through business interruption or reduction of it as a result of property.
- Loss of, or damage to, third parties and/or their property.
- Loss of, or damage to, employees and/or their property.
REDUCING RISKS

REDUCE THE FREQUENCY AS WELL AS THE SEVERITY OF PURE RISKS:

- Avoidance
- Loss Control
- Self-retention
- Insurance