Port Security

A Holistic Approach

Presidia Security Consulting

Stephen Moore

smoore@presidiasecurity.com

Presidia Security

- Founded in 2009 after leaving Defence
- Strategic security, investigations and intelligence
- Projects with Public Safety (Ports), CTA, CBSA (Air) & Major Investigation (Port Related)

Outline

- Threat
- Security Strategy & Common Findings
- Recommendations

Presidia Security Consulting

THREAT

General Threat Evolution

2012 Jeffrey Delisle charged with espionage

2014 Terror Attacks in Quebec and Ontario

2015 Cyber attacks reach unprecedented level

Port Security Threats

Revenue Generation

- Illegal Drugs
- Counterfeit Goods
- Illegal Immigrants
- Cargo Theft
  - 5 Billion dollar industry
  - High profit and low risk

Support Crimes

- Corruption intimidation of:
  - Industry insiders
  - Security
  - Law Enforcement Personnel

Threats to Port Security

- Three largest ports – Halifax, Montreal & Vancouver are the most vulnerable
- Sheer volume of traffic reduces likelihood of detection
- Countermeasures include intelligence, technology and expanded searches
- Despite best efforts resourcing is a challenge

Examples

- Vulnerability of Ports to Organized Crime
  - Theft and introduction of contraband into legitimate shipments
- Trucking cargo theft
  - Threats to family
- Major Canadian airports have 38 organized groups working out of them
  - Baggage handlers, ramp attendants, food caterers and refuelers

Presidia Security Consulting

ASK THE QUESTION

What is my Security Strategy?

What is My Security Strategy?

- What are the threats and risks to our operations?
- What security measures do we currently have in place?
- Are they sufficient to mitigate the threats and risks?
  - If not how do we close the gap?

Common Findings

Governance	Policy	Training	Response
• Security is decentralized • Information flow is poor	• Limited or non-existent	• No training plan	• Incidents not tracked • Lack of statistics • No formal lessons learned program

Presidia Security Consulting

RECOMMENDATIONS

Approach Security Holistically

Governance

- Security starts at your company
- Who is in charge of security at the strategic level?
- How are security concerns reported?
- What needs to be reported to the VP level?

Policy

- Security policies should be in one place and written for a non-security reader
- Security Governance should be recognized in the policy
- Security policy should recognize related programs

Training (Awareness)

- Who should be trained
- What do they need to know
- How will we communicate changes

Response

- Investigate incidents and track them internally (broader focus than criminal investigation)
- Keep meaningful statistics from year to year
- Implement a formal lessons learned program

Recommendations

- Technology should enable your strategy
- Move security above “gates and guards” level
- Consider opportunities for cooperation and trading value
  - Intelligence Hub
  - Pool security resources where feasible
- Security should enable operations. The goal is identify weak links and mitigate risk to enable your operations

Security Strategy

Asking the question is not expensive

- You may be able to do this internally
- Informed consent

Security enables operations

- Lower risk
- Trade value

Stephen Moore
smoore@presidiasecurity.com
613.883.7805
www.presidiasecurity.com