Emergency Operations Centers
An Industry Partner’s Perspective for Port Security
by Hampton Dowling
L-3 Communications, Global Security & Engineering Solutions
23 July, 2009
Today’s Discussion
In the context of how we use EOCs

• The path taken to where port security is today

• Challenges that influence security

• Complexities facing today’s diverse port security management team

• Recommendations for approaching the future
Ports aren’t the same

But convenience and exposure are common

Is something that’s good or applicable for one port a good fit for the another….and the same for those hundreds in-between?
Port Security

It was perhaps “simpler” only ten years ago

- Acquiring traditional physical security capabilities, i.e., radios, cameras, fences etc. Budgets put security into different, often higher priority initiatives to meet requirements as feasible
- EOCs were typically meeting rooms with Internet connections, phone banks, large screens and white boards. Decoupled from routine operations
- There was little drama or information to suggest domestic ports were a target beyond local crime activity and illegal immigration. Legislation had limited specificity
- Standards weren’t always clear or enforced
- We weren’t attending “port security” forums.
Port Security

It’s now much more complex in 2009

The list expands all the time:

- Federal programs, initiatives that shape requirements and structure resources....
- MOUs between cities, major corporations and shipping companies.....
- Investment relationships, Public private partnerships...
- Managing sensitive intelligence data, real-time web-based collaboration.....
- GPS/GPR-enabled tools, biometrics, in-transit scanning, anomaly behavior applications, intelligent access control.....

The list grows in scope.
Canal expansion will drive exponential growth for ports in Latin America and Caribbean for transshipment thus more stress on Canadian & US ports.

Energy demand, off-shore drilling and coal production will drive increased traffic.

Ports typically less focused on container trade and traditionally linked to energy or tourism will become focal points of short shipping and small craft traffic.

Oil platforms will become high-risk critical infrastructure with dependences on port resources & regional authorities.

Coordination of rail & road traffic management and ERM will add increased complexity.

New legislation will create efficiencies and add burdens.

What’s 2019 look like?
Port Security Focus Areas

**Big picture can be a challenge to understand & manage**

---

**State Militias, Dept of Transportation, DHS**
- Information gathering, indication and warning queues
- Intelligence sharing, dissemination, planning collaboration
- Predictive analysis, interoperable communication, interdiction

**Overlapping Areas of Interest, Responsibility and Capabilities**

**Port Authorities**
- Port operations, safety of navigation and environment
- Landside & waterside security, active surveillance, and awareness
- Continuity of operation, government and authority

**Port Tenants**
- Terminal operations, supply-chain management, providing goods & services
- Supply-chain integrity, enforcement of trade, health & commerce regulations
- Property security, access control and surveillance
- Maintaining insurability and revenue generating requirements

---

**Area of Responsibility and Authority**

*What’s the justification for necessary trade-offs? Who decides?*
*How do we know what’s important?*
*By whom and how do we measure, attain and sustain success?*

---

*The drive for ports to meet increased capacity demands will stress all facets of operations, including ERM processes and security coordination*
2007-2008 saw a significant increase in federal-sponsored reports that included or were principally focused on both secure commerce and port security. In addition to GAO reports, federal strategy documents and congressional memos shape requirements that convey direct bearing on port planning, resource availability, security operations and advocacy for private sector services.

Now….Secure Filing Initiative (10+2) IFR on 26 January 09. For ports and entities charged with legislation compliance enforcement the dynamics of balancing requirements with revenue operations can be tough.
Example Mosaic of Equities

Each with unique needs influencing revenue & security

Group 1 Port Example
Complexity to Decisions
How we use EOCs is borne from this calculus

More Complex Threat Environment
- Large-scale threats are less likely but remain a possibility. Natural disasters will challenge both collaboration and emergency management across all jurisdictions.
- Threats may be less visible, be from within and leverage public access.
- Choice of weapons & delivery may be less predictable, unconventional.

More Complex Operating Environment
- Requirements to continue operations with increased security requirements driven by DHS, state, federal agencies and insurability.
- Requirements to restore public confidence in parallel with restoration of services.
- Myriad of public, private stakeholders all with highly visible equity, economic critical mass.
- Competing pressures: safety & security and requirement to sustain revenues.

Robust Security Capabilities
Economic Viability of Operations

Experience has shown the challenge is to design, develop effective security enhancements that are technically and operationally executable in public & private sectors.

- Drives efficiencies in solutions engineering and processes on large, complex scale.
- Offers unique understanding of O&M sensitivities, strategies, options for stakeholders.
- Traceability to cost & resources estimations.
oint Solutions for Port Security

Integrated Portal Systems

Fixed Systems
Rail Systems
Mobile Systems
Command Center Systems

How does this all fit together? Is it possible? Not practical?
Large organizations tend not to subordinate interests, actions or compromise characteristics. Compels other agencies to change or find their own solutions.

"Fusion centers" often gravitate data from top to upper levels versus "collaboration centers" that seek to serve entire vertical.

Situational awareness is often limited to display screens and not inclusive of available intelligent tools that reveal anomalies, truly integrate data artifacts.

Reliance upon proximity of staff versus tools, equal access, task visibility.

Scope of events are often slow to be revealed, ground truth can be shaded by lack of traceable credible data.
Optimizing EOC Resources

• Leverage business applications & rules such that more revenue generating services can be accurately monitored, services calculated and invoiced.

• Employ for improved administrative control of harbor maintenance & movements, pilots, traffic management and data statistics.

• Enable routine information for real time or historical support of emergency management.

• Enable transparency between security and port management.

EOC Software, Tools and Manpower

Typical Limited Port EOC Connectivity

- NCS
- HSIN
- GPRS
- CBP VPN
- WebEOC
- Focus Pages
- AMOC
- FPS Chat
- MARVIEW
- Blogs
- Blackberry
- FERN
- POTS
For Ports...
EOCs are a resource not just capability

• **Embrace a clear, fundamentally different philosophy**
  – Have the right mental model that drives data-sharing relationships
  – Get organized with energy to understand what we need to know, who has the information and put it together for ports who use it
  – Enforce transparent ethics and realize incentives

• **Simplify the “how” of it all**
  – Embrace a business model that employs EOCs as an asset versus a service (ports and maritime authorities are a business)
  – If solutions work elsewhere then apply & adapt
  – Apportion indemnification within partnership framework

• **Optimize resources**
  – EOCs need to be used as value proposition that support multiple purposes which directly influence revenue
  – Best value pays dividends shareholders can understand
Ports – big and small – cannot fail. Port security is a pillar of national security. It includes the supply chain, coastal surveillance, to law enforcement at a port’s rear area wharfs. There are many variables affecting all ports and their approach to security, and use of EOCs. Leveraging EOCs beyond crisis management increases its value and would provide a recognizable, tangible net return on the port’s investment.

- Ports’ growth & implications must be considered in making choices
- Focus on real requirements using proven guidelines
- Use industry partners wisely to build public confidence and develop reliability that drives increased revenue