

Supply Chain Security

Leszek Sitkowski LRQA Poland

Supply Chain Security Management Systems



LRQA
Measure the Difference

Presentation Outline

- HOW DID WE GET TO THIS
- INTERNATIONAL ACTION
- ISO 28000: 2007



Events That Changed World Thinking

- New York & Washington – September 2001
- Madrid – March 2004
- London – July 2005
- Germany – July 2006
- Glasgow – June 2007
- Algiers – December 2007



Examples - Supply Chain Security

- December 2003 an ABC television crew, tested and demonstrated the inconsistencies between documentation and contents in cargo movement by smuggled 15lb of depleted uranium from Jakarta to Port of Los Angeles by simply not declaring the contents.
- Jan – Apr 2005, US DHS reported 83 Chinese illegal immigrants in containers.
- November 2007, Slovakia. 3 persons arrested for attempting to smuggle 1kg enriched uranium.
- 2007. Russian authorities blocked more than 120 attempts to illegally move “highly radioactive” material out of the country.
- April 2008, Fifty-four illegal immigrants from Myanmar died inside one container truck in Thailand

Who is at Risk

- Manufacturers
 - Oil and Gas
 - Food and Beverage
 - Chemical and Pharmaceutical
 - Wholesale and Retail
 - Airports and Airlines
 - Logistics and Freight Forwarders
 - Transport Companies
 - Ships, Ports and Terminals
 - Service Industries and Government
 - Insurance
 - The supply chain itself
- Counterfeit
 - Insurgency
 - Bio-terrorism
 - Theft, counterfeit
 - Supply loss
 - Terrorism
 - Smuggling
 - Organized crime
 - Bomb in a box
 - Migratory impact
 - \$\$\$ Damages
 - All of us

Why Supply Chain Vulnerabilities Are Rising

- Just-in-time or lean approaches;
- Global sourcing; globalization of supply chains;
- Focused factories and centralized distribution;
- Outsourcing;
- Supply consolidation ; reduction of the supplier base;
- Volatility of demand; and
- Lack of visibility and control procedures.

Sources: Christopher, Martin and Wilding, Richard, (2002): "Supply chain vulnerability", Final Report, Cranfield School of Management, England. ; and (2003): "Supply Chains In a Vulnerable, Volatile World", AT Kearney, Executive Agenda, Volume VI Number 3 Third Quarter 2003, US.

Some figures

- Global transit loss estimates - \$30 to \$50 billion per year.
- Typically 2% to 8% income reduction for Fortune 500 companies due to poor security.
- Estimated, 80% of cargo thefts are “made to order thefts”
- Threat rated “severe” in Brazil, Russia, South Africa, Indonesia, Nigeria and Malaysia.’

What would be the cost of an effective terrorist attack using the supply chain – unknown.

An attack would probably cause major international disruptions and closure of some businesses in the chain.

*Sources: WCO (World customs Organization); WHO (World Health Organization); DOT (Department of Transportation US); DHS (Department of Homeland Security US) ; FBI (Federal Bureau of Investigations US); ICSC (International Cargo Security Council)

Potential risk to Individual Business

- What are the consequences of a major security incident?
 - Damage to tangibles? (*physical assets – property, products, infrastructure, personnel*)
 - Damage to intangibles? (*the non-physical assets – reputation, market position, goodwill*)
- The harm to business may include;
 - Business integrity
 - Reputation
 - Injury or serious harm to persons and property
 - Clients property
 - Standing in industry community – regulatory issues

International Action

- National Customs Department initiatives involving Industry and Trade
- Not specifically a National Security response, but calls for industry to contribute to the National efforts to combat crime and terrorism.
- The WCO Safe Framework of Standards and AEO specification is the largest industrial security initiative in history with 147 Nations heading in the same direction.

International Initiatives on Supply Chain Security

- International Maritime Organisation 2004
 - ISPS (International Ship and Port Security) Code
 - Ports and Ship Security
- World Customs Organisation 2005
 - SAFE Framework of Standards (AEO)
 - 147 Countries
 - Establishes minimum standards for Customs/Customs and Customs/Business cooperation on security for the facilitation of trade.
 - Seeks Mutual Recognition between States



International Initiatives on Supply Chain Security

US – Homeland Security

- C-TPAT (Customs and Trade Partnership Against Terrorism)
- CSI (Container Security Initiative)
- Food and Drug Administration Bio-Terrorism Act
(Secure - food supply chain)
- others



International Initiatives on Supply Chain Security

European Commission – AEO Program

- EC regulation 648/2005 – ‘Authorised Economic Operator’
- With effect from 1 January 2008
- Customs Security Programme
- Pre arrival/departure information
- Risk related information
- Criteria:
 - An appropriate record of compliance with customs requirements,
 - A satisfactory system of managing commercial and, where appropriate, transport records, which allows appropriate customs controls,
 - Where appropriate, proven financial solvency, and
 - Applicable, appropriate security and safety standards.



Sharing Best Known Methods
(Quarterly meetings / Websites / Newsletters)

FSR
(Warehouses)

TSR
(Trucks)

PSR
(Parking)

TACS
(Air cargo)

Set of Standards

Incidents Reporting & Alerts (IIS)

©2007 Transported Asset Protection Association, All Rights Reserved

Sharing Best Known Methods
(Quarterly meetings / Websites / Newsletters)

One Standard

FSR

TSR

PSR

TACS

Incidents Reporting & Alerts (IIS)

©2007 Transported Asset Protection Association, All Rights Reserved

Other International Initiatives

- **BASC** (Business Alliance for Secure Commerce) driven by private industry; supported by CBP and linked with C-TPAT South America
- **AMS** (Automated Manifest System); driven by Transportation Security Administration (TSA) US
- **PIP** (Partnership In Protection), **ACI** (Advanced Commercial Information); driven by Canadian Customs and Canada Service Border Agency (CSBA)
- **EU Regulations 2320/2002 , 622/2003 & 831/2006** (Airfreight security regulations)
- **Chapter 1.4 for DG**: security provisions of the UN Model Regulations on transporting in Dangerous Goods
- **TAPA** (Technology Asset Protection Association); driven by major high-tech manufacturers

WCO - Authorised Economic Operator (AEO)

Customs/Business partnership

Application of the AEO program by National Customs Departments may vary however globally these shall include a number of common elements.

These elements include:

- Demonstrated compliance with Customs requirements;
- Financial viability;
- Consultation, cooperation and communication;
- Information exchange, access and confidentiality;



WCO - Authorised Economic Operator

cont.

Management and security requirements. Including;

- Satisfactory system for management of commercial records;
- Education, training and awareness;
- Cargo security;
- Conveyance security;
- Premises security;
- Personnel security;
- Trading partner security;
- Crisis management and incident recovery;
- Measurement, analyses and improvement.



The Objective - A Secure Supply Chain

All participants, business and trading partners

- Establish and maintains appropriate security measures for safeguarding people, goods, infrastructure, equipment and information within their particular area of responsibility.
- Where all of the participants ensure that there is continuity of security throughout the entire chain, this will be considered a Secure Supply Chain



Security/Trade Facilitation Objectives

The intent is that secure supply chain will result in reductions of costs, both to business and government, due to streamlining/fast tracking the throughput of product at international points of entry.

LAND, AIR & SEA

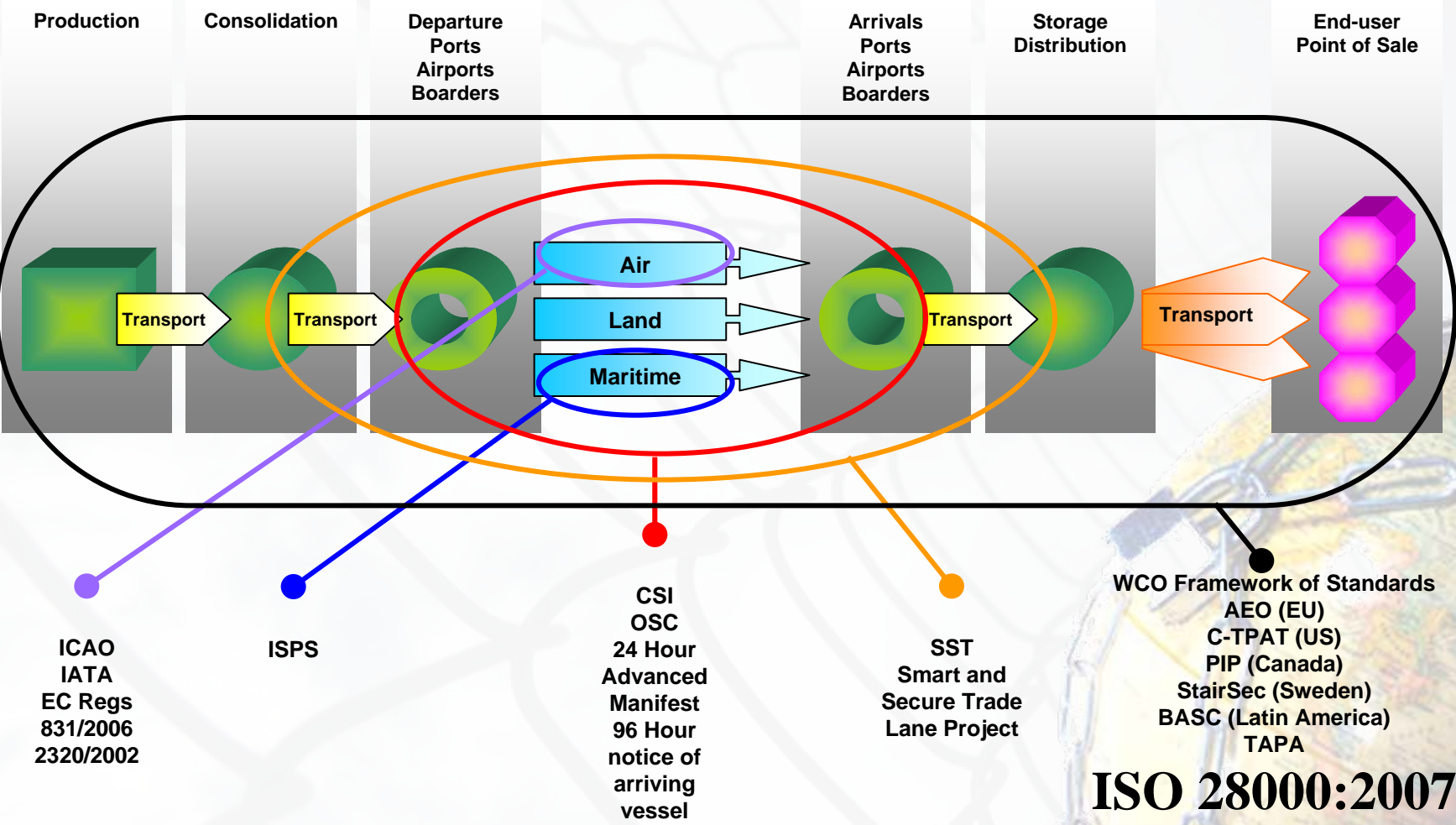
GREEN Lane

(Fast-tracked Customs)

RED Lane

(Additional attention by Customs)

Supply Chain Movement



The ISO 28000 series of Standards

- Developed in response to demand from industry against a background of varying international security regimes.
- Generic management specification to improve the security in supply chains.
- A high-level management standard designed for all sizes of organisations.



The ISO 28000 Series

Standards and codes of practice for supply chain security

These standards have been developed to compliment the various international initiatives to facilitate uniform implementation worldwide.

- ISO 28000 - Supply chain security management
 - Published Sept. 2007
 - Risked based model
 - Plan, Do, Check, Act principles
 - Designed for 1st, 2nd & 3rd party auditing
- This is the Certification Standard, similar to
 - ISO 14001, OHSAS 18001,

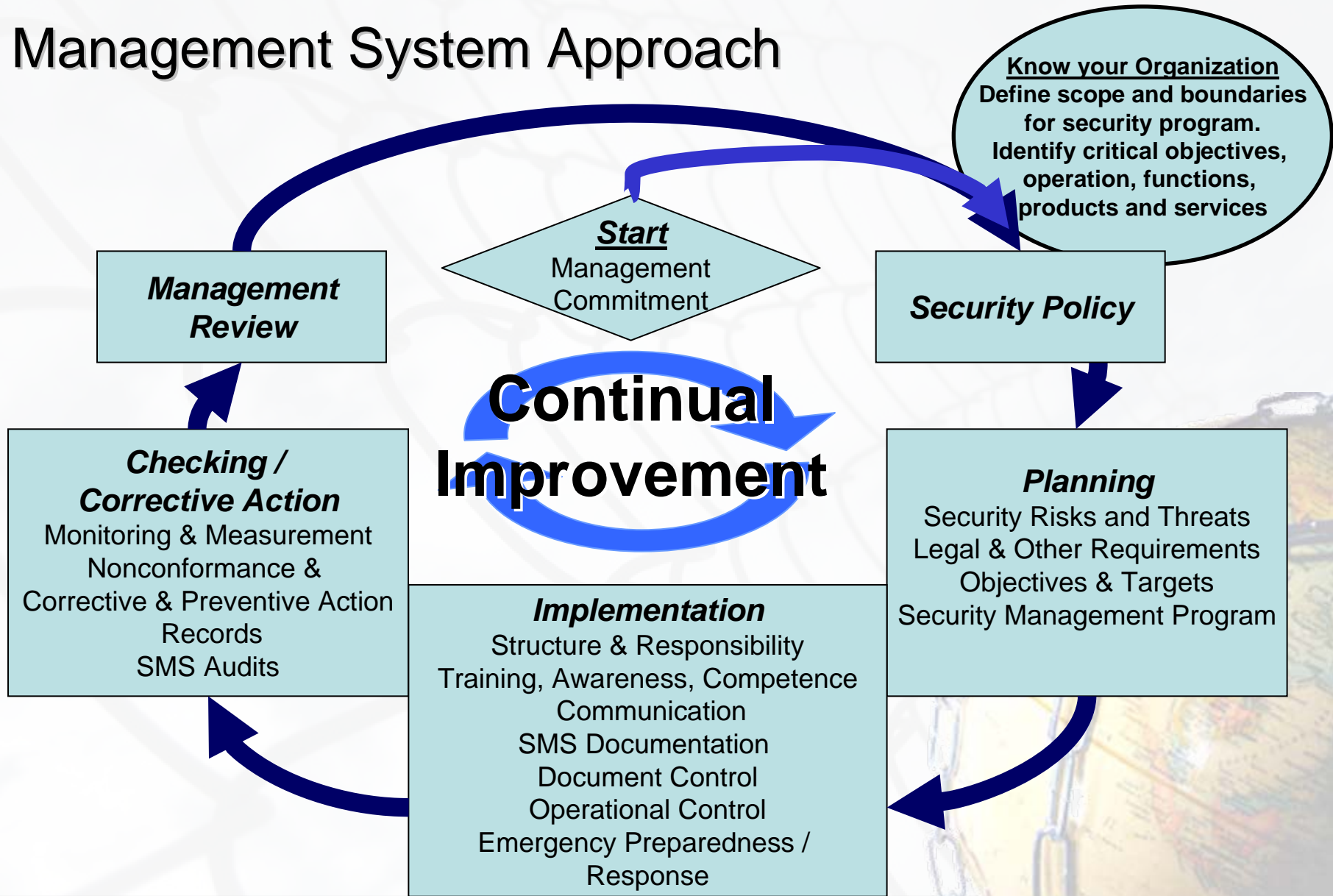
The ISO 28000 Series

- ISO 28001 - Best practice guideline for implementing Supply Chain Security, assessments and plans
 - Aligned with WCO Framework of Standards
 - This is a guideline only and not a mandatory requirement.
- ISO 28003 – Requirements for bodies providing audit and certification.
- ISO 28004 - Guidance for ISO 28000

28000 Family - Summary

- Requires organisations to: –
 - assess the security environment in which it operates
 - determine if adequate security measures are in place
 - Improve performance .
- Designed to be a sound foundation for complying efficiently with other international, national and sector based security requirements and schemes.

Management System Approach



ISO 28000 and Global Security Initiatives



Customs Trade
Partnership
Against
Terrorism
(C-TPAT)



World
Customs
Organization
(WCO)

SAFE
Framework



European
Commission
Authorized
Economic
Operator



Singapore
Secure
Trade
Partnership
(STP)



Transported
Assets
Protection
Association
(TAPA)



ISO 28000

ISO 28000 requires us to Understand the risks

Security risk assessments rely on a thorough and accurate understanding of five crucial elements

- **Assets** – anything of value to the organisation
- **Threat** - any possible intentional action or series of actions with a damaging potential to any of the stakeholders, the facilities, operations, the supply chain, society, economy or business continuity and integrity (ISO 28004)
- **Vulnerability** - intrinsic properties of something that create susceptibility to a source of risk that can lead to a consequence (ISO/IEC Guide 73)
- **Consequence** - outcome of an event affecting objectives (ISO/IEC Guide 73)
- **Likelihood** - chance of something happening (ISO/IEC Guide 73)

Assets, Threats, Vulnerability and Risks

Assets

Which assets do you want to protect?

Threats

What could threaten your assets?

Vulnerability

Are your assets vulnerable to these threats?

Risks

What are likelihood & impact of the threats?

Measures

What are you going to do about the risks?

Procedures

How do you manage the selected measures?

Implementation

How do you make the measures work?

Control

How do you know it is effective?

ISO 28000 and Business Improvement

Establishes mechanisms for the systematic

- Identification of legislation, regulations and standards that apply to the security operations on site.
- Identification and development of security procedures.
- Application of appropriate security tools
 - Fit for purpose (CCTV, Access Control, Fencing, etc.)
- Development of emergency plans for managing identified risks.
- Management commitment and review
- Performance management, and
- Continual improvement



Security Management System

ISO 28000 – 4.3.3 Security management objectives

The organization shall

- establish,
- implement and
- maintain

documented security management objectives at relevant functions and levels within the organization.



What Security Management Objectives?

- **Provide for the protective security of persons, property and information**
- Ensure client cargo and property integrity is maintained?
- Meet a national or regional Customs Department requirement?
 - EC, AEO
 - US, C-TPAT
 - Other requirements - TAPA

A study conducted by Massachusetts Institute of Technology in June 2006 quantified the collateral benefits companies could receive from investment in supply chain security. BASC trade

The study showed that those who invest enjoy a

- 48% reduction in inspections, **GREEN LANE**
- 50% improvement in asset visibility,
- 31% shorter problem resolution time, and
- 38% reduction in theft, loss and pilferage.

Business oriented security risk management

Risk Management Standard

Company policies

Sector-specific risks

Activity-related risks

Company-specific solutions



Summary

- Proper Supply Chain security is achieved with risk based management
- Current best practices (company-own, TAPA etc.) can be used for definition of risk treatment measures (solutions)
- Current information sources (TAPA, Eurowatch, Police, Company-own) can be used for threat analysis
- Certification / verification should not be based on auditing of presence of countermeasures, but on use of integral risk management.
- External & periodic review (audit) of risk management and operational control, through internal audits as well as 1st, 2nd or 3rd Parties is a necessity

LRQA Contact details

Lloyd's Register Quality Assurance, Poland

- **Leszek Sitkowski**

Thank You

