

RISK MANAGEMENT

Border Crossing Points and Customs

OSCE 18th Economic and Environment Forum
First Preparatory Conference Astana
Tuesday 13 October 2009

Jan Tomczyk, FCILT
Independent Expert on Border and Customs Issues
UNECE Euro-Asian Transport Links Expert
EU Motorways of The Sea Black Sea & Caspian Sea Border Expert

Risk Management

- Also described as managing risk at border crossings, inland clearance depots with participation of exporters, importers and other trade user intermediaries
- Traditional view RM is a Customs issue
- Sole Customs role is a narrow perception
- Customs must stop being part of the problem and be part of the solution

Risk Management Definition

“Risk management gives Customs Administrations a solution enabling them to balance their control functions with trade facilitation by selective inspection of traded goods using risk management criteria, information, intelligence and trader process auditing and auditing the trader’s logistics service providers i.e., auditing the international supply chain”

Why Use Risk Management

- Traditional Customs procedures use document and physical border controls aiming to “capture” illegal trade
- Modern Customs Administrations use a disciplined and structured method to manage goods crossing borders: RM
- RM helps Customs increase operating efficiency and lowering interventions

Risk Management Objectives

- Getting the balance between trade facilitation and control while managing two risks:
 - managing risk to trade by not helping trade
 - managing non compliance risk
- Customs Administrations need to achieve a balanced risk management approach at the border crossing points
- See UK Customs “Striking the Right Balance”
- Scanning each import container is not managing risk

World Wide Risk Management

- Many countries now have Customs trader compliance programmes: Jordan, USA, Canada, Sweden, Australia, Holland, Singapore, the EU and other countries
- International organizations have supply chain security programmes: WCO, APEC
- Risk management often described for traders as managing compliance with the Customs Codes and Rules and Bilateral Agreements and with International Conventions

Getting Risk Management 1

- Systematic collection and analysis of Customs information and intelligence which identifies high risk from low risk
- Structured risk management includes timely assessment of information and updating risk profiles; before the goods arrive and before goods leave
- Using information and intelligence is the key part in risk management

Getting Risk Management 2

- IT helps risk management become effective
- IT risk assessment helps Customs and other border officials analyze each shipment using risk profiling method
- IT risk management needs feedback from traders, other Customs Administrations and organizations increasing effectiveness of the risk management system

Getting Risk Management 3

- Risk management includes risk profiling criteria for importer, transporter, freight forwarder, Customs broker, exporter, bank, insurance and other international supply chain intermediaries
- Not enough to profile the importer, risk management must profile the trade transaction and the international supply chain intermediaries

Getting Risk Management 4

- Risk management method is not a method carried out by Customs in isolation from the trading and logistics community
- Getting an effective and respected risk management method means changing how Customs Administration carry out their mandate
- Getting risk management needs partnering with traders and logistics service providers

Getting Risk Management 5

- Customs Administrations need to get commercial knowledge about trade transactions and international supply chain
- Customs need to start a trader low risk due diligence compliance programme where traders use proven written self compliance methods audited by Customs
- Customs must know each traders processes; how traders exercise reasonable care and how traders document that reasonable care

Getting Risk Management 6

- Customs decide each “baseline” trader compliance after auditing traders written processes measuring non compliance and setting a risk profile
- As a result trader and Customs understand what needs doing to get improved compliance
- Customs trader audit verifies how traders check they comply with laws and conventions
- Customs and traders become part of the international supply chain security solution

Getting Risk Management 7

- Risk based compliance management select goods for further control
- Using selectivity Customs recognise that some traders have different risk levels
- Risk based compliance management gives low risk traders less controls and high trade facilitation
- Low risk traders might get incentives such as fast track clearance and other incentives

Risk Management Good Practice at Border Crossing Points

Current Practice

- Control focus
- High levels of physical inspection
- Focus identifying non compliance
- One size fits all
- Limited use of IT
- Adversarial relationship with traders
- Competition between agencies
- Limited incentives for compliance
- Limited cooperation with neighbours
- Limited operational statistics



Future Practice

- Facilitation / control balance
- Intervention by exception
- Focus on information
- Compliance / non compliance balance
- Flexible solutions for different clients
- Extensive use of IT
- Constructive trade partnership
- Single Window System
- Strong compliance incentives
- Extensive cooperation
- Clear performance measuring

Risk Management and Supply Chain Security

- Border crossing point part of international supply chain
- Preventative due diligence reduces risk at borders
- Routine checks immediately identifying deviations and shortcomings
- Preventative checks preferred to extra inspections along the supply chain
- Better to have procedures preventing containers getting manipulated before and during transport: 100% scanning does not prevent international supply chain abuse
- Supply chain delay might result in less business for the exporting company i.e., each day delay corresponds to a 0.8 % add on tariff for a countries exports (Hummels, D., “Time as a

trade barrier”, 2001, p.17)

Supply Chain Risk Management

- Threat to supply chain might include:
 - Hijacked container
 - Trojan horse container
- Supply chain risk management must be designed to identify each threat type
- OECD reports parts of risk analysis not fully implemented
- Customs and trader partnership needed to help identify illegal containers

Supply Chain Risk Analysis 1

- Threat assessment: identifies adverse events that might have an impact
- Vulnerability assessment: identifies infrastructure weaknesses or process and personnel policies that might get exploited
- Critical assessment: identifies, assesses and prioritises action strategies
- Risk assessment: qualitative and quantitative determining event likelihood

Supply Chain Risk Analysis 2

- Risk characteristics: seek to assign risk using low, medium or high scale and helps develop effective response
- Risk mitigation: implementing counter measures using risk, cost etc
- Systems approach: procedures, actors, technology, infrastructure, policy and governance
- Monitoring and evaluation: continuous assessment process ensuring current security measures and strategy; external peer review, testing and validation

Assessing Container Risk After 9/11

“Hijacked” container

- Modus operandi

Container intercepted along logistics supply chain and illegal goods, persons, weapons, drugs inserted

- Precedent

Not very common use in contraband and drug smuggling. More likely scenario for theft where container tampering common

- Discovery risk

Possible to discover because of multiple handling and visual inspections along the chain

“Trojan horse” container

- Modus operandi

Terrorist creates “legitimate” export business, builds track record and trust using legitimate operations over a period of time. Implements and receives vetting for on-site security practices

- Precedent

Fairly common practice to pack container with drug and or contraband at source. Less common for a trader to build a reputation before going bad.

- Discovery risk

Very low discovery risk when traders get a “legitimate” trading record

“Hijacked” Container Security Measures Effectiveness

- Scanning and inspection: effective
- Physical integrity: effective
- Container environment: effective
- Tracking: effective
- Trade documents, data and intelligence: partially effective

“Security measures and the hijacked/Trojan horse scenarios” by OECD in Container Transport Security Across Nodes, 2005, OECD/ECMT

“Trojan horse” Container Security Measures Effectiveness

- Scanning and inspection: effective
- Physical integrity: not effective
- Container environment: not effective
- Tracking: partially effective
- Trade documents, data and intelligence: effective

Supply Chain Security Weaknesses 1

- Supplier country of origin risks: western terrorism threat level, cargo tampering rates and the host government's ability to suppress and control these exposures
- Lack of contractually mandating that business partners are certified by Government security criteria
- Lack of a global supplier base risk assessment process which might identify high risk business partners

Supply Chain

Security Weaknesses 2

- Security and cargo “chain of custody gaps” within the supply chain, including un-vetted container stuffing, consolidation or 3rd Party Logistics and in-transit warehouse locations
- Consolidation of Government Customs security programme member company materials with non Government security company materials: consolidated shipments including unscreened cargo

Improving Supply Chain and Cross Border Security 1

Five goals (Cross Border Research Association, 2006, Lausanne):

1. Facility management: securing premises
2. Cargo management: protecting goods
3. Human resources management: ensuring personnel background checks
4. Information and communication management: protecting data, tracing illegal activities and security gaps
5. Business network and company management methods: internal and external security of the companies business systems

Supply Chain Security Initiatives 1

World Customs Organization Framework of Standards to Secure and Facilitate Global Trade (SAFE) elements:

1. Advance electronic information
2. Risk management: each country participating in SAFE uses a consistent risk management approach to security threats
3. Outbound inspection: using risk targeting method
4. Business partnership: SAFE defines benefits that Customs shall offer companies that meet minimal supply chain security as well as standards and best practice

Supply Chain Security Initiatives 2

WCO standards for cooperation between Customs 1:

- Integrated supply chain management: data submission, authorised supply chain
- Cargo inspection authority
- Modern inspection equipment technology
- Risk management methods: automated selectivity methods, WCO SAFE, references
- High risk cargo or high risk containers
- Performance measures
- Security assessments
- Employee integrity: WCO Revised Arusha Declaration

Supply Chain Security Initiatives 3

WCO standards for cooperation between Customs 2:

- Advance electronic information: need for IT, Revised Kyoto Convention ICT Guidelines, use of electronic operators' systems, electronic data exchange standards, WCO data model, ICT security, digital signatures, training, data privacy and data protection
- Targeting and communication: WCO Global Information and Intelligence Strategy, WCO Standardized Risk Assessment document, WCO General High Risk Indicator document, WCO Handbook for Customs Officers on Risk Indicators
- Outbound security inspection: examining on request

Supply Chain Security Initiatives 4

WCO Authorized Economic Operators (AEO) 1:

- Demonstrated compliance with Customs requirements
- Satisfactory method managing commercial records
- Financial viability
- Consultation, cooperation and communication
- Education, training and awareness
- Information exchange, access and confidentiality
- Cargo security

Supply Chain Security Initiatives 5

WCO Authorized Economic Operators (AEO) 2:

- Transportation security
- Premises security
- Personnel security
- Trading partner security
- Crisis management and incident recovery
- Measurement, analyses and improvement

Supply Chain Security Initiatives 6

Transport Asset Protection Association (TAPA) Freight Suppliers Minimum Security Requirements (FSR):

- Perimeter security: CCTV etc
- Access control to company offices: entrances issue
- Facility dock and warehouse: access control and CCTV
- Security methods
- Security procedures
- Standard truck security requirements
- Pre –Alerts
- Enhanced security requirements: driver training, escort

Supply Chain Security Initiatives 7

Transport Asset Protection Association (TAPA) Freight Suppliers Minimum Trucking Security Requirements (TSR):

- Physical security: truck and trailer
- Security methods: tracking, alarm, truck immobilization
- Security procedures: collection of information, delivery, pre-alerts, scheduled routing, event reporting, stops, secure parking, key management, etc
- Personnel security: vetting, checking and hiring
- Training: security
- Enhanced security needs: drivers, truck escorts

Conclusions 1

- Risk management and supply chain security at border crossings not only a Customs Administration role
- Risk management and supply chain security role includes all participants in a logistics supply chain from origin to destination
- If, Customs Administrations only carry out border crossing point truck and container X-Ray scanning it is not a Risk Management method
- If, Customs Administrations rely on high levels of physical inspection without a risk management method using information and intelligence the border crossing points are at risk
- Using Risk Management with information and intelligence border crossing points get layered security

Conclusions 2

- Preventative security measures described in this short presentation preferred to inspections
- Having routines might identify deviations and security shortcomings
- Procedures preventing a container from being manipulated before and during transport should be used
- Customs Administrations need to identify and record which traders part of a Risk Management, Customs compliance programme and or supply chain security initiative in other countries: less risk
- Most Customs Administrations do not know which trucks entering border crossing might belong to some type of supply chain security programme so all get treated the same: “one size fits all”

Some information sources

- OECD: “Terrorist modus operandi: hijacked versus Trojan horse containers”, Container Transport Security Across Modes, 2005, OECD/ECMT
- “Customs Modernization Handbook”, The World Bank, 2004
- “Supply Chain Security Initiatives: A Trade Facilitation Perspective”, Swedish Board of Trade Kommerskollegium, 2008
- TAPA www.tapaemea.com

Rahmiet, Spasiba, Thank You

Jan Tomczyk, FCILT

Fellow of the Chartered Institute of Logistics and Transport, UK

Member European Customs and International Trade Forum

Member Central Eurasian Studies Society, Harvard University

EU MOS Black Sea and Caspian Sea Customs Expert

UNECE Euro-Asian Transport Linkages Expert