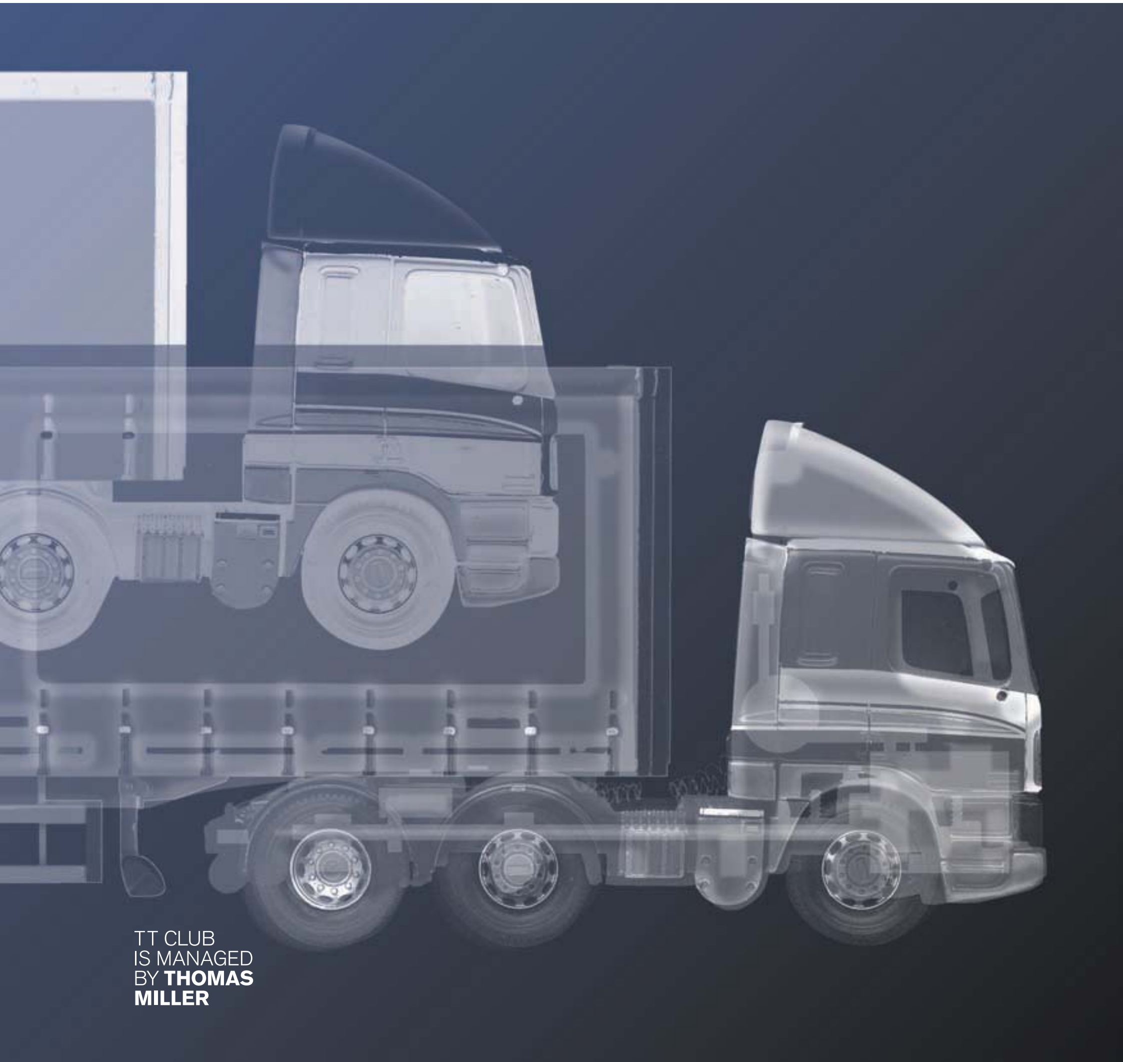
TT CLUB

Supply Chain Security
Management, initiatives & technologies

transport insurance plus



TT CLUB
IS MANAGED
BY **THOMAS**
MILLER

Supply Chain Security Management, initiatives & technologies

First Edition 2010

ISBN 978-1-85330-019-9 (Printed)
ISBN 978-1-85330-019-6 (PDF)

Disclaimer
The materials contained in this booklet have been prepared for information purposes only and must be considered in the context of any specific operational situation. Whilst every care has been taken to ensure the accuracy of the materials, the editor, any contributor or the TT Club accept no responsibility for loss or damage which may arise from reliance on information contained herein.

Designed by Evolution Digital Limited
Printed in England by Evolution Digital Limited

About the TT Club & ICHCA International

TT CLUB

The TT Club is the international transport and logistics industry's leading provider of insurance and related risk management services. Established in 1968, the Club's membership comprises ship operators, ports and terminals, road, rail and airfreight operators, logistics companies and container lessors.

As a mutual insurer, the Club exists to provide its policyholders with benefits that include specialist underwriting expertise, a world-wide office network providing claims management services, and first class risk management and loss prevention advice. This is one of a number of publications that seek to disseminate good practice through the supply chain.

For more information about TT Club and its services please visit www.ttclub.com.

ICHCA
International Ltd

ICHCA International is dedicated to the promotion of safety and efficiency in the handling and movement of goods by all modes and during all phases of both the national and international transport chains. Originally established in 1952 and incorporated in 2002, it operates through a series of Local, National and Regional Chapters, Panels, Working Groups and Correspondence Groups and represents the cargo handling world at various international organisations, including the International Maritime Organization (IMO), United Nations Conference on Trade and Development (UNCTAD), International Labour Organization (ILO) and the International Standards Organization (ISO).

ICHCA members include ports, terminals, transport companies and other groups associated with cargo handling and coordination. Members of ICHCA Panels represent a substantial cross-section of senior experts and professionals from all sectors of the cargo transport industry globally. Members benefit from consulting services and informative publications dealing with technical matters, ‘best practice’ advice, and cargo handling news.

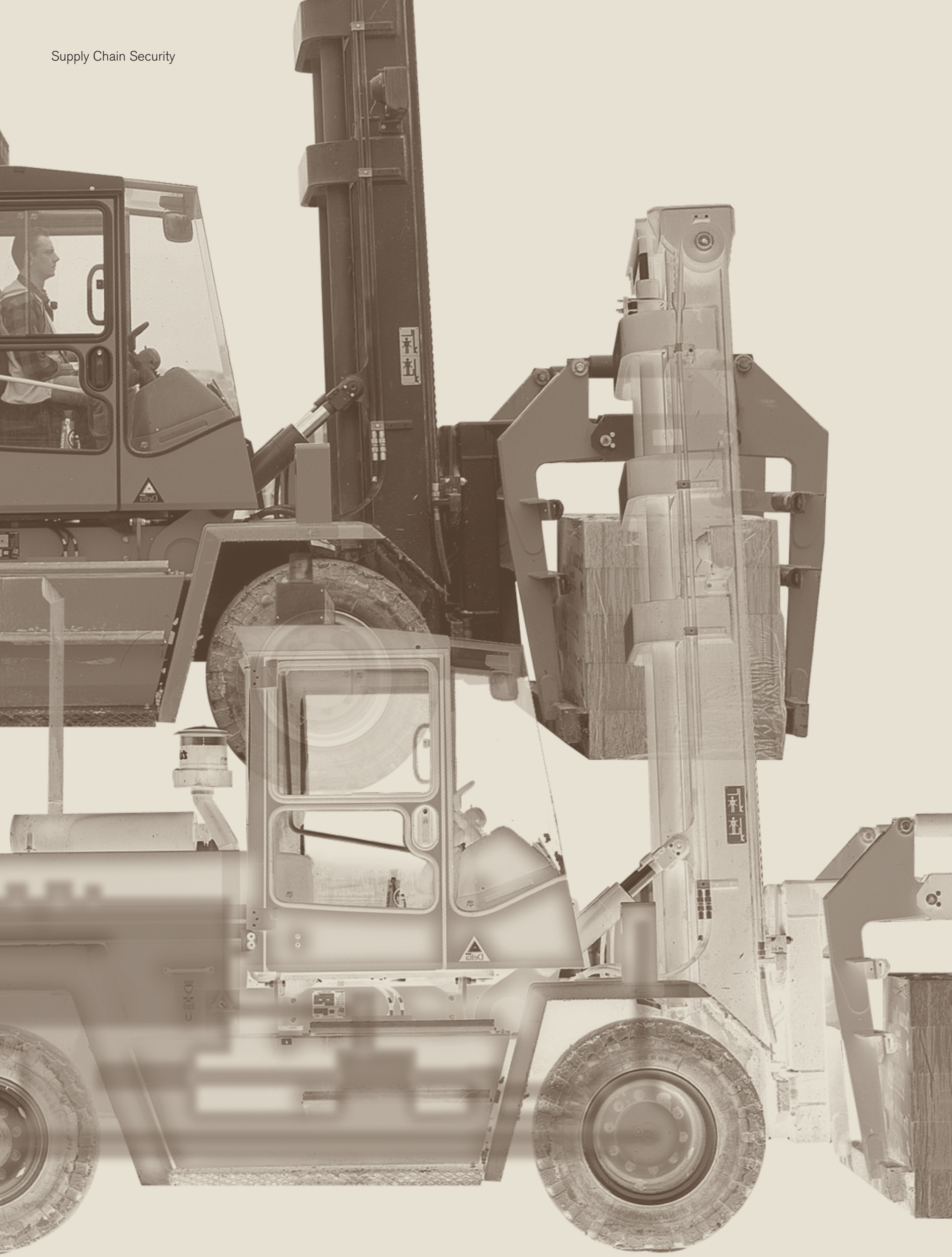
For more information on ICHCA and its services please visit www.ichca.com.

Preface & Acknowledgments

In the early 1990s the TT Club published a booklet entitled 'Terminal Security', prepared by Andre Ya Deau, of the US security management consultancy International Security Services Inc and Peter Westley of the London based investigation company Signum Services. The aim of that document was to outline a number of general principles of good physical security practice as well as to offer specific recommendations for terminal operators. In July 2004 the IMO's ISPS Code came into force, introducing a need for common security standards at the ship/port interface and the concept of the secure maritime supply chain. The aim of this booklet is to extend that concept to the entire end-to-end supply chain and to inform the reader of contemporary supply chain security methodology which should form part of good practice for operational management. This booklet takes into account contemporary terminal, or nodal, practice as well as supply chain initiatives and regulation. Similarly, while the original was more aimed at warehouses and terminals, this new loss prevention booklet seeks to encompass all operators in the supply chain.

A number of people have been involved in compiling this booklet, but particular thanks need to be expressed to Carina Dixon of NewMarket Partners, London, who chairs the International Security Panel of ICHCA International, Risto Talas, Research Fellow at University of Hull Logistics Institute, and Paul McCarthy of ONE Security, Sydney, Australia.

This 'StopLoss' booklet has been prepared in collaboration with the International Security Panel of ICHCA International, who publish this text as Security Series SS1.



Contents Page

Foreword

Since 2001 a plethora of International Maritime and Supply Chain Security Legislation, and associated security initiatives, have been introduced to protect the world's global supply chain. Terrorism has heightened the awareness of governments and industry to the vulnerability of the supply chain, accelerating the importance of supply chain security internationally. Government and industry initiatives are requiring business to take action to strengthen the security and resilience of their supply chains.

Supply chains are varied and complex, involving numerous parties, which make them vulnerable to exploitation by criminals and terrorists. Protection against such exploitation can only be achieved by considering the supply chain as a whole, rather than at individual nodes in isolation. Supply chain security requires each stakeholder to be involved themselves and engaged with their upstream and downstream partners to create a chain of responsibility that extends from the point of origin to the final destination.

The ISO 28000:2007 series of standards on supply chain security management systems was developed in response to demands from the international transportation industry for a common global standard that would be mutually acceptable and recognised, rather than being forced to adopt and comply with security measures that had no direct relevance to their business.

When your business adopts an approach aligned with ISO 28000:2007 standards, you will observe that security becomes an integral part of your business encompassing responsibility across all departments. This results in enhanced operations, safeguarding of employees and assets and provides customers with the required confidence to associate with your business knowing that their cargo will be protected.

This publication provides a cogent introduction to ISO28000:2007 standards and processes along with a review of a methodology used to measure its benefits by companies who look at security from the perspective of a higher level of management and actively incorporate it into the entire scope of their business operations. It also profiles current supply chain security initiatives and technologies evaluated for each part of the supply chain.

Foreword (continued)

Investment in supply chain security provides higher levels of security and therefore lowered risk. This also leads to significant increase in business value through improved and streamlined operational capabilities, increased customer confidence, reduced costs and thereby increased profitability.

Yuvraj Narayan,
Board Member , TT Club
Chief Financial Officer, DP World

Introduction

In the years immediately following the events of 11 September 2001 the transportation industry created and implemented several port and supply chain security measures to prepare and protect the industry such as the IMO's International Ship and Port Facility Security (ISPS) Code and the United States' Container Security Initiative (CSI) and Customs-Trade Partnership Against Terrorism (C-TPAT) initiative. As the depth and complexity of supply chain security has become apparent, the focus of many security initiatives has broadened past terrorism and it is these initiatives that this booklet aims to introduce in a practical manner.

Debate at this time is focused on securing supply chains from end to end. Research has shown that it typically takes 25 different parties and 30 different documents to get goods from one end of the supply chain to the other. With all these hands involved, the opportunities for tampering are plentiful. Against this background, the World Customs Organisation introduced the twin pillars of the customs-to-customs network arrangements and customs-to-business partnerships in the Safe Framework of Standards to Secure and Facilitate Global Trade (known as the 'SAFE Framework').

> *'Supply chain security is… only as strong as its weakest link,'*
>
> ***S Jayakumar, Singapore's Deputy Prime Minister and Coordinating Minister for National Security and Minister for Law***

The SAFE Framework introduced the concept of the 'Authorised Economic Operator' which has since been enshrined in various countries' legislation including the EU. Authorised economic operators include manufacturers, importers, exporters, brokers, carriers, consolidators, intermediaries, ports, airports, terminal operators, integrated operators, warehouses and distributors. This brings emphasis to the entire supply chain.

Supply chain security initiatives are not exclusively 21st century phenomena. The Business Alliance for Secure Commerce (BASC) began as an anti drug-smuggling programme introduced between Mexico and the United States in 1996. Similarly, The Transported Asset Protection Association (TAPA) was founded in the 1990s to counter the threats to increasingly high-valued shipments of technology products.

Furthermore, the current interest in supply chain security initiatives is only partly due to the events of 11 September 2001. The reality is that globalisation has resulted in companies' supply chains becoming extended across continents as never before and the need for the effective management of risk has resulted in the extension of supply chain risk management to include issues of security. However, as global trade increases, the danger of weapons or a terrorist entering a country in a cargo container is a very real threat. The incident at the Port of Ashdod in March 2004, involving the apprehension of a terrorist operative hiding in a container en-route to Canada, highlights the fact that 'the container is the Trojan Horse of the 21st century,' as described by Robert Bonner, US Commissioner for Customs and Border Protection.

A key focus of this booklet is ISO 28000, which fundamentally addresses the shift to supply chain security. One of the main purposes of ISO 28000 is to be a common value-adding, verifiable, internationally recognised standard that bridges governmental and industry-driven supply chain initiatives; it currently stands alone in being able to fulfill the requirements for reciprocity between them. It is based on all currently prevalent and relevant global security initiatives, including the World Customs Organisation's 'SAFE Framework', C-TPAT and EU AEO.

In addition, it represents a move away from mere compliance by applying a process approach and the 'Plan-Do-Check-Act' methodology to address potential risks. ISO 28000 offers a systematic approach to security management that can both improve operational capabilities and increase confidence on the part of customers and regulators. All businesses that are reliant on the supply chain for business continuity will benefit by adopting the sound management principles in ISO 28000.

'The implementation, by Governments, of a regulated agent system for maritime supply chain security, based upon the WCO Framework of Standards model, could have significant benefits for increasing safety and security while at the same time enhancing the facilitation of international trade. Procedural security measures, consistent with the approach of ISO, would enhance the effectiveness of such an approach, while at the same time building confidence in the integrity of the system.'

Chris Trelawny, Senior Technical Officer,
Maritime Security Section, International Maritime Organization

The Benefits of Investing in Supply Chain Security

It is the contention of this booklet that operators should invest enthusiastically in supply chain security. Whereas compliance has been the focus of supply chain security, the advice here promotes an approach which does not see supply chain security as an opportunity to meet static requirements. A better approach gives each individual company the latitude to institute security measures tailored to its unique needs and vulnerabilities. This is exactly the approach of the ISO 28000 Standard.

> *'These risks are no longer the sole responsibility of specialists to manage in disconnected ways. Executives and boards of directors demand visibility into exposure and status so they can effectively manage the organisations' long-term strategies. We see more firms taking a critical step back to get a fix on the big picture. It's already beginning how they systematically identify, measure, prioritise, and respond to all types of risk in the business, and then manage any exposure accordingly.'*
>
> ***John Hagerty of AMR Research,***
> ***September 2005***

> *'Unfortunately, many organisations have found it difficult to justify the required levels of investment. The main reason has been the focus on direct expense related to security initiatives, and lack of awareness of collateral benefits that can be realised.'*
>
> ***Michael B. Crutch, Program Director,***
> ***Import Compliance and Supply Chain Security, IBM***
> ***November 2006***

In general the benefits of investing in supply chain security are multifaceted. A business becomes more efficient, visible, resilient, and inventory and customer relations are improved.

The US government estimated that trade in counterfeit items multiplied from US$5.5 billion in 1982 to US$600 billion in 2008, accounting for up to seven percent of world trade.

In particular, Supply Chain Security can do the following for a business:

- Reduce inspections (48% reduction★)
- Increase automated handling (43% increase★)
- Reduce process deviation (30% reduction★)
- Shorten transit time (29% reduction★)

- Improve asset visibility
- Provide more timely shipping information (30% increase in timeliness★)
- Provide more accurate shipping data

- Shorten problem resolution time (close to 30% quicker★)
- Quicken response to a problem (close to 30% quicker★)
- Reduce time to identify a problem (30% reduction★)

- Reduce theft / loss / pilferage (38% reduction★)
- Decrease tampering (37% reduction★)
- Reduce customer attrition (26% reduction★)
- Reduce excess inventory (14% reduction★)

★ according to an IBM survey of 11 manufacturers and 3 ‘innovator’ logistics service providers

It has been demonstrated that a security investment can reduce operational costs, increase efficiency and competitive advantage by demonstrating that a company (particularly a logistics provider) is committed to its customers’ best interests.

> *‘Security is a baseline service we offer our customers. This recognition (ISO 28000) underlines to them that we are committed to focussing strongly on maintaining or enhancing security in our terminals around the world.’*
>
> ***Mohammad Sharaf, CEO DP World***

Specifically embracing ISO 28000 has the following benefits:

Features	Benefits
Commercial & competitive advantage *Companies embracing ISO 28000, particularly during the early phases of its adoption, stand to benefit through increased market share and customer retention*	• *Unambiguous demonstration that an organisation takes not only its own security seriously but also the security of goods its customers expect it to protect* • *Enhanced brand equity through the clear demonstration of commitment to security*
Risk Management *Risk management is a fundamental corporate activity and essential for organisations operating within the international trading system. ISO 28000 enshrines risk management as a proactive means of protecting the organisation*	• *Pragmatic and business-centric approach to risk management key decision making, particularly in relation to the commitment of resources, based on a process of effective risk assessment*
Resilience & brand protection *ISO 28000 increases the resilience of the organisation in the face of increasing risk*	• *Reduced risk that the company will be irreparably damaged by incidents impacting its operations, financial health or reputation*
Improved resource management *Implementation of ISO 28000 has significant potential to enhance the effective management of security resources, resulting in cost savings*	• *Speedy identification of wasteful and inefficient resource management practices* • *Increased level of accountability at all levels leading to improved management of the security budget*
Benefits to corporate governance *Companies adopting ISO 28000 have made an organisational commitment not only to security but also effective management and continual improvement*	• *Adoption of ISO 28000 demonstrates effective corporate governance* • *Protecting company and clients' assets improves company value and shareholder protection*
Employee safety & security *ISO 28000 improves levels of safety and security for employees*	• *Impact on levels of staff satisfaction and retention* • *Reduction in injuries and lost time incidents*
Management process compatibility *Can be integrated with the existing internationally recognised management processes of ISO 14001, ISO 9001 and OHSAS 18001*	• *ISO 28000 adopts the same approach as existing management systems and processes, resulting in a reduction in the time required for implementation*

Features	Benefits
Scalability *ISO 28000 has been specifically designed to be flexible and applicable to all tiers of a business from the head office to remote warehouses*	• *Can be implemented equally effectively for smaller companies as it can for major international organisations*
Mutual recognition *In the future ISO 28000 is likely to be recognised globally by other trade security programs, and participants will receive benefits inherent with these programs*	• *Based on WCO SAFE Framework and other existing supply chain security initiatives*
Insurance premiums *Companies compliant with ISO 28000 may enjoy a reduction in insurance premiums*	• *Compliance with ISO 28000 should result in improved risk profile and claims experience, reflected in premiums* • *Potential positive impact on credit ratings at the group level, particularly if the organisation has exposure to higher risk locations*
Site collaborative approach *ISO 28000 encourages effective consultation and communication with all those affected by its operation*	• *Participation and staff 'buy in' rather than a disconnected third party approach encourages acceptance and cooperation of policies and objectives, and reduces the likelihood of a site culture of resistance to the system. Staff are more likely to support the system, openly reporting anomalies and site breaches*
Identifies expected outcomes *ISO 28000 takes a risk and systems based approach to security issues*	• *Having clearly expected outcomes makes for better use of resources and technology choices that are measureable and that truly address the issues rather than investing in technology that fails to deliver the overall expectations*

Universal compliance fosters a secure and vigilant industry, and the negative effects of noncompliance cannot be overlooked. Increasingly, businesses in the supply chain will be expected to comply with voluntary measures as a matter of routine.

Supply Chain Security Management – ISO 28000

The International Standards Organisation has developed security standards aimed at becoming the global supply chain security standard programme. It is intended to act in concert with and complement the World Customs Organisation's Framework and it does not attempt to cover specific Customs agency requirements. ISO 28000 was launched in November 2005 as a publicly available specification and is now a fully-fledged ISO standard.

For ISO 28000:
http://www.iso.org/iso/iso_catalogue/catalogue_ics/catalogue_detail_ics.htm?csnumber=44641

ISO 28000 is applicable to all sizes and types of organisations at any stage of production or anywhere in the supply chain. As long ago as 2005 an FM Global / Harris Interactive Research Survey found that, 69% of chief financial officers, treasurers and risk managers at Global 1000 companies in North America and Europe considered property-related hazards and supply-chain disruptions as major threats to top revenue sources.

It is a voluntary standard but, critically, may be certified by third party auditing companies to demonstrate that a company has taken a proactive and responsible approach to security by establishing a security management system that assures compliance with a documented security management policy.

ISO 28000 is based on the format adopted by ISO 14000 owing to its risk-based approach to management systems and is based on the methodology known as Plan-Do-Check-Act:

- **Plan**: establish the objectives and processes necessary to deliver results in accordance with the organisation's security policy
- **Do**: implement the processes
- **Check**: monitor and measure processes against security policy, objectives, targets, legal and other requirements, and report results
- **Act**: take actions to continually improve performance of the security management system

A study by Aberdeen Group shows that few companies can afford to ignore supply chain risks. Almost 99 percent of the 138 companies surveyed suffered a supply chain disruption and 58 percent suffered a financial loss.

ISO 28000 requires an organisation to assess the security environment in which it operates to determine if adequate security measures are in place and to identify and comply with relevant regulatory requirements. If security needs are identified by this process, the organisation should implement mechanisms and processes to meet these needs. Each risk can be evaluated as to criticality and a determination can be made as to what risks can be mitigated and what risks can't, either because of practicality or economic viability. In many cases this exercise will identify alternate business processes that not only reduce or remove the risk but may, in some cases, streamline the operation of the business, increasing bottom line profits. Where mitigation is not economically viable, the fact that a risk is identified allows a planned response to be made. Holistically, this process will identify potential threats that require mitigation and provide a mechanism for preparedness and recovery.

The security management system clearly defines the strategic security objectives of the organisation and puts into effect constant monitoring with a focus on continual improvement.

The following sections give a general overview of the security management system of ISO 28000 but should not be taken as representing the complete requirements of the Standard.

General Requirements

The purpose of the Standard is to provide a documented security management system which identifies security threats, assesses the risks and controls and mitigates their consequences.

This process is continual so that the system can be effectively maintained and improved.

The scope of the security management system needs to be defined by detailing the physical area covered by the system and the operations that are undertaken within this area. Any outsourced processes should be considered and controlled where necessary.

Security Management Policy

A security policy should be defined and authorised by top management which clearly states the overall security objectives of the organisation. The organisation should demonstrate, through this policy, its commitment to complying with relevant legislation or other requirements and its commitment to continually improve its security management system. The policy should be communicated and promoted as widely as possible.

An example Security Policy

ABC Ltd is committed to providing a secure workplace ensuring that our business activities are conducted in a manner that complies with national and international laws and regulations.

This policy has been established to demonstrate ABC's commitment to the security of our employees, customers and assets. This is essential to the successful conduct and future growth of our business, and is in the best interest of each of the Company's supply chain customers.

Senior Management will visibly uphold the principles of this policy and integrate them throughout the Company, while the executive management team will review security management performance and policy.

The management and security staff at ABC premises will be responsible for implementing and maintaining the security management systems necessary to comply with this policy and will be held accountable for compliance and performance. All areas of the business will support the operation of the security management system.

Every employee, whose work may have an impact on security, will be trained and held accountable for complying with the policy and related procedures, practices, instructions and rules.

Each employee has a duty to report any unusual observations, practices or persons that could pose a security risk to ABC and the community where we operate.

Through the active participation and commitment of all ABC employees, we will strive to meet and exceed these aims and demonstrate our commitment to security excellence.

Security Risk Assessment & Planning

Security Risk Assessment

A thorough and comprehensive security risk assessment is the key to a successful security management system. Without understanding the risks that the organisation may face and their consequences it will not be possible to ensure that the appropriate security is in place to mitigate the risks.

It is recommended that a recognised form of methodology is used for undertaking a risk assessment. ISO 28001 is one methodology that may be used and provides guidance on the process including suggested threat scenarios and consequence classification and scoring.

Risk assessments should be documented to provide for their continued review on a regular basis or following a change in threat, an incident at the organisation or a change in operations.

The following is general guidance on the basis of undertaking a risk assessment.

A review of the organisation's operations and current security procedures should be undertaken and key assets to protect identified.

Threats to the organisation should be assessed through a process of information gathering. This may include:

- *Past incidents*
- *Information from government and other agencies*
- *Information from surrounding organisations*
- *Information from industry*

Threat scenarios relevant to the organisation should be determined and for each one the consequence if it should happen and likelihood of it happening should be investigated.

For each threat scenario a scoring should be given determined by the level of consequence and likelihood.

For high scores (ie. the consequence would have a significant impact on the organisation and/or there is a significant likelihood of an incident occurring) the organisation should consider what measures it should put in place either to reduce the consequence or the likelihood and bring the score down to an acceptable level.

continued over...

Measures considered to reduce the risk fall into 4 categories:

- *Treat - may be organisational and/or physical measures*
- *Transfer - transfer of the risk by subcontracting, physical transfer to other locations or time*
- *Terminate - the organisation may decide not to continue the activities*
- *Tolerate - impracticality of measures required, lack of authority to impose them or other insurmountable factors*

Once measures have been decided they should be implemented and then assessed for their effectiveness in lowering the risk. As previously stated the risk assessment should be continually reviewed and actioned as required.

Case study – *Critical Infrastructure*

Through the process of undertaking a thorough threat and risk assessment critical infrastructure was identified which if damaged would lead to the total inoperability of the business for at least three months due to the lead time for replacement parts. This had not been identified in previous assessments and security requirements were therefore deemed inadequate. Mitigation was developed and implemented to provide better protection of this critical infrastructure.

Legal, Statutory & Other Security Regulatory Requirements

All requirements that the organisation is required to comply with should be identified and assessed with regard to its security threats and risks. This may, for example, be legislation, initiatives to which the organisation subscribes, requirements of customers or the organisation's corporate body. A method of ensuring that this information is up to date and its requirements are communicated to those who need to action them should be developed.

Security Management Objectives, Targets & Programmes

Management should identify security objectives and targets. Objectives may include such things as reduction in risk levels, introduction of additional features, improvements to existing facilities, elimination or reduction in frequency of undesired incidents. Targets should be set for each objective detailing the timeframe in which the objective should be achieved and suitable monitoring indicators.

For each objective a programme should be developed to show how the objective will be achieved on target. Responsibility for achieving the programme should be defined.

Implementation and operation

Structure, Authority & Responsibilities for Security Management

The organisational structure for security should be defined detailing the roles, responsibilities and authorities of persons with security duties. The structure should demonstrate the organisation's top management commitment to the system and its continued improvement. In order to achieve this, a member of top management should be designated as responsible for the overall management of the system. A team of senior management should also be appointed to periodically review the system.

Competence, Training & Awareness

The organisation should ensure that personnel with security responsibilities have the required competencies to carry out their duties; this may be through education, experience or training. Security awareness by all personnel and visitors to the organisation is essential to the effective running of any security system and a programme of education should be in place to ensure ongoing security awareness by all persons.

Case study – *Security awareness*

Security training had been received by those personnel with security duties but no security awareness training programme was in place for all staff and visitors. This led to a lack of understanding by staff of the requirements for security and generated conflict between the security guards and operational staff. Through a programme of short training courses, posters and a feedback system for security issues the security awareness of staff was greatly increased, thus providing co-operation with security personnel and, most importantly, providing the site with one of the best security resources available, the engagement of all staff to report security deficiencies or unusual circumstances.

Communication

The system should include procedures to ensure that relevant security information is communicated to those who require it. At all times the consideration of the sensitivity of the information should be taken into account.

Documentation Including Data Control

When implementing a security management system an organisation should put in place sufficient documentation to ensure that the policy and requirements of the system are demonstrated and that the system may be clearly followed by all involved in its implementation and operation.

All security information, including documentation and data should be controlled. Consideration should always be given to the level of sensitivity and access restricted accordingly. Procedures should be in place to ensure the availability of information to those who require it, including the effective backing-up of information.

Operational Control

The operations and activities necessary for the security management system should be identified. Controls should be put in place for situations where their absence could lead to a failure in the security management system. Upstream and downstream activities should be assessed and controls put in place to mitigate any threats identified.

Emergency Preparedness, Response & Security Recovery

Potential emergency situations should be identified and plans put in place both to respond to and recover from their effects. Consideration should be given to the resources and responses that would be required by security during other types of incident eg. environmental. Emergency Response Plans should be tested periodically.

Case study – *Emergency Preparedness, Response and Recovery*

Separate plans had been developed for emergency situations relating to health & safety or environmental issues and responses to security situations. Little consideration had been given to overall combined response from all departments for each situation and no consideration had been given to the ongoing requirements for securing the facility during and following an emergency. Comprehensive and fully co-ordinated plans were developed which addressed the security of the operations during and following an incident of any kind.

Checking and Corrective Action

Security Performance Measurement & Monitoring

Procedures should be established to monitor both the performance of the security management system and the performance of security. This should include both proactive measures, that monitor compliance with the system, and reactive measures, to monitor deteriorations, failures, incidents and non-conformances. Key performance indicators should be set.

System Evaluation

Evaluation of the system should be undertaken through such measures as testing, exercises, post incident reports and lessons learned.

Security Related Failures, Incidents, non-Conformances and Corrective & Preventive Action

Where a failure, or the potential for failure, is recognised the organisation should have in place a procedure to initiate corrective or preventive actions. The identification of the root cause is essential in ensuring appropriate action is put in place. Following any corrective or preventive action an evaluation should be undertaken into the effectiveness of the action.

Case study – *Corrective action following a security incident*

An unannounced breach test was undertaken resulting in the penetration of the perimeter by an individual. The failure was initially assumed to have been a lack of attentiveness by the guard. However, by following a robust format for investigation into the root cause it was found that there was a blind spot at the guard post. Corrective action was undertaken to remove this failure in security.

Control of Records

The organisation should maintain records sufficient to demonstrate conformity to the requirements of its security management system and ISO 28000. Procedures should be in place to control records and ensure they are available as required. Records may be in hard or soft copy. Consideration of the sensitivity of information should be considered at all times.

Audit

A programme of internal audits should be developed in order to determine whether the system conforms to planned arrangements, has been implemented and is maintained and effective in meeting the organisation's policy and objectives. The frequency of audits should be determined from previous audit results and non-conformances.

Management Review & Continual Improvement

Senior management should review the whole of the security management system periodically to ensure that it continues to be suitable and adequate and is effective in managing security within the organisation. The review should assess any changes that may be required to the system and identify opportunities for improvement.

Measuring the Value Created by Supply Chain Security

As has been demonstrated, the ISO 28000 standard provides the methodology for introducing and implementing the management of supply chain security measures. This section builds on this by evaluating the rationale for introducing these security measures, ie. how to measure and interpret the value created by supply chain security.

This question will be addressed while examining two different approaches which can be employed in conjunction with ISO 28000 combined with the results of recent academic study. Whilst the study was conducted in the port sector the findings can be applied across all operations within the supply chain. The first concept is Total Security Management or TSM. The second approach describes how the principles behind the Six Sigma quality management measurement tool can be bolted on to the principles behind ISO 28000 in order to measure the value created by supply chain security.

ISO 28000 and Total Security Management (TSM)

Total Security Management (TSM) was modelled on the Total Quality Management (TQM) concept which seeks to improve customer satisfaction through an integrated effort from all areas of a business, towards continuous improvement of the quality of the services. A strategy based on TQM focuses on customer satisfaction by targeting improvement at all levels and encouraging employee involvement at all stages.

TSM is defined as 'a business practice of developing and implementing comprehensive risk management and security best practices for a firm's entire value chain.' TSM is a framework that manages security as a core business function and integrates security prerogatives across all activities of the enterprise. The four main areas where there are opportunities to create value are investigated below. This is all set against a background of turning security from a net cost to a net benefit.

TSM works with and through key internal and external stakeholders to ensure the use of a comprehensive approach to securing fixed assets, assets in transit, brand equity and human capital. There is an emphasis on business continuity planning with an evaluation of the firm's suppliers, distribution channels, facilities selection criteria and the internal policies and procedures that support preparedness for disruptive events.

The TSM approach to cost savings from improved business processes is reliant upon the automation of certain security practices in order to make labour savings; this is proposed in conjunction with enhanced brand recognition such as through championing the adoption of new supply chain security practices. The similarities between TSM and TQM are no coincidence. The Plan-Do-Check-Act cycle originally devised for TQM was adapted in the quality management standard ISO 9000, which also forms the framework of ISO 28000.

TSM consists of Five Strategic Pillars:

- Total Security practices must be based on creating value that can be measured
- Total Security involves everyone throughout the value chain
- Total Security implies continual improvement
- Total Security helps firms avoid, minimise or survive disruptive events
- Total Security requires resilience and business continuity planning as essential business functions.

The Five Strategic Pillars are supplemented by the Four Operational Enablers:

- Implementation of industry best practice
- Increased situational awareness
- Reliance upon training and exercises
- Outreach to all relevant parties.

Key sources of creating value in Total Security Management

1. Cost savings from improved business processes

There have been few studies in the field of trade facilitation resulting from the introduction of security measures, such as measuring the time factor (delay or speed-up) brought about by security measures. However, proponents of the introduction of measures such as the Container Security Initiative, the 24-hour rule and the Customs-Trade Partnership Against Terrorism 'fundamentally shift the focus from inspection to prevention, the benefits of which offset and ultimately outweigh the initial and recurrent costs of implementation.'

Furthermore, the detailed electronic data reporting to the US Customs and Border Protection's Automated Manifest System coupled with other procedural requirements allows for the accurate targeting of suspect containers which 'is proven as more cost-effective and less time-consuming than the traditional approach of random physical inspections.' Other benefits to compliant traders may include reduced insurance costs, penalties and risk exposure.

2. Reduced loss/theft from improved asset management

The value created from the reduction in losses or theft is directly related to the difference in the aggregate theft levels pre and post the introduction of security measures. The levels of pilferage in ports and theft from containers has fallen markedly, since the introduction of the ISPS Code, due to the requirement to introduce measures designed to prevent unauthorised access to the port facility.

3. Enhanced Brand Equity

What is the cost associated with losing the reputation for being able to provide safe and secure transportation services? A company would maintain brand equity following a security incident if it:

- maintained a security posture at or above a baseline level of security
- demonstrated an acceptable level of security commitment to the industry at large.

The ten measures for brand equity are:

1. Price premium
2. Satisfaction/loyalty
3. Perceived quality

4. Leadership
5. Perceived value
6. Brand personality
7. Organisational associations
8. Brand awareness
9. Market share
10. Price and distribution indices.

One major port operator's strategy of rolling out ISO 28000 across its terminals worldwide has increased its brand equity in terms of perceived quality, leadership, brand awareness and market share. By choosing to adopt ISO 28000, the perception of the quality of its security practices is enhanced; it has shown leadership by spearheading the drive towards ISO 28000 compliance among port companies; its brand awareness spreads as a result of the positive media coverage.

4. Improved preparedness for catastrophic loss.

The key to value creation through improved preparedness for catastrophic loss is the ability to resume normal or near normal trading conditions as quickly as possible. There is a need for building resilience into the organisation including crisis readiness and a documented recovery plan with defined steps for re-establishing critical operations following a disruptive event. Key to the resumption of operations is to run a back-up power supply and back-up IT systems which may be located outside the facility and can be activated following a disruptive event. After the Bishopsgate bomb in the City of London in 1994, many City firms located their back-up IT systems and back-up offices in London's Docklands. However, after the Docklands bomb in South Quay Plaza in 1996, this strategy had to be re-evaluated.

The measurement of value created through improved preparedness for catastrophic loss is a complex process. On the one hand there is expenditure associated with the construction of back-up systems, the running of crisis management drills and the introduction of operational redundancies. Furthermore, a facility such as a port terminal that suffers a catastrophic loss may be out of action for a considerable period before normal operations can resume and while the costs associated with business interruption and infrastructure reconstruction may be recoverable from insurers, the loss of business to rival operations may be harder to regain in the medium to long term.

There are two ways of modeling losses attributable to a terrorist attack in a port terminal; at the micro (port) level and at the macro (national economic) level. The OECD (2003) report states that a terrorist attack on a 30 hectare container terminal would result in a loss of US$32 billion. It has modeled (at the macro level) the costs associated with a 15-day and a 120-day closure of the ports of Los Angeles and Long Beach following a terrorist attack using a radiological dispersal device, each containing 5lbs of high explosive, including the destruction of three key bridges/overpasses using conventional bombs. It was concluded that in the case of a 15-day closure of both ports, the total economic loss would be US$4,284 billion resulting in a total of 26,521 job losses within and outside the Los Angeles region. The corresponding figures for the 120-day closure of both ports is a total economic loss of US$34,189 billion including 212,165 job losses both within and outside the Los Angeles region. The expenditure on any preparation for catastrophic loss would be significantly outweighed by the scale of the overall economic loss to the local economy.

ISO 28000 and Six Sigma

Six Sigma is a rigorous, focused and highly effective implementation of proven quality principles and techniques. Six Sigma was developed by a Motorola engineer as a method of approaching business problems with a statistical toolset. He called it ‘organised common sense.’ Some particular features of Motorola’s programme were:

- Goal-deployment of business objectives to process objectives
- Strong project management of process-improvement activities
- Emphasis on visibility of financial benefits of improvement.

The phrase ‘Six Sigma’ implies a goal of reducing the number of defects to less than 3.4 defects per million occurrences (assuming that the quality of the selected measure has a normal distribution). Processes that produce more than 3.4 defects per million occurrences have lower levels of Sigma, thus:

- 2 Sigma = 308,537 defects per million occurrences
- 3 Sigma = 66,807 defects per million occurrences
- 4 Sigma = 6,210 defects per million occurrences
- 5 Sigma = 233 defects per million occurrences
- 6 Sigma = 3.4 defects per million occurrences.

Five Steps of the Six Sigma Project (DMAIC)

The fundamental objective of the Six Sigma methodology is the implementation of a measurement-based process improvement through variation reduction. DMAIC is an acronym for the five interconnected steps of a process improvement project:

- Define
- Measure
- Analyse
- Improve
- Control.

Define

The first step in any Six Sigma project is to clarify the problem and narrow its scope in such a way that the project team can achieve measurable goals within a few months. These are typically the steps in the define stage:

- Define the customer, their critical-to-quality (CTQ) issues and the core business process involved
- Define who the customers are, what their requirements are for products and services and what their expectations are
- Define project boundaries – the stop and start of the process
- Define the process to be improved by mapping the process flow.

Measure

In the second step of the Six Sigma project, the team maps the process, gathers data, verifies the quality of the data and prepares it for analysis:

- Measure the performance of the core business process involved
- Develop a data collection plan for the process
- Collect data from many sources to determine types of defects and metrics
- Compare to customer survey results to determine shortfall.

Analyse

Once a process has been mapped and documented and the quality of the data supporting it has been verified, the Six Sigma team can begin the analysis. The team members usually start by meeting to identify ways in which people fail to act as needed or fail to assert effective control at each stage:

- Analyse the data collected and process map to determine the root cause effects and opportunities for improvement
- Identify gaps between current performance and goal performance
- Prioritise opportunities to improve
- Identify sources of variation.

Improve

The team identifies improvements based on the analysis undertaken. In other words, the suggested improvements must be backed by hard data and analysis:

- Improve the target process by designing creative solutions to fix and prevent problems
- Create innovative solutions using technology and discipline
- Develop and deploy the implementation plan.

Control

In the final stage of the Six Sigma project, the team creates controls to enable the company to sustain and extend the improvements:

- Control the improvements to keep the process on the new course
- Prevent reverting back to the 'old way'
- Require the development, documentation, and implementation of an ongoing monitoring plan
- Institutionalise the improvements through the modification of systems and structures (staffing, training, incentives).

Applying Six Sigma to Supply Chain Security

The application of Six Sigma to supply chain security is a relatively new phenomenon and only one theoretical study[1] currently exists. There is enormous scope to develop Six Sigma projects in order to measure, analyse and improve the different processes involved. These processes could include access control, monitoring of facilities and/or operations and detection of illicit and/or unauthorised cargoes. The aim of Six Sigma within supply chain security would be to reduce the number of defects

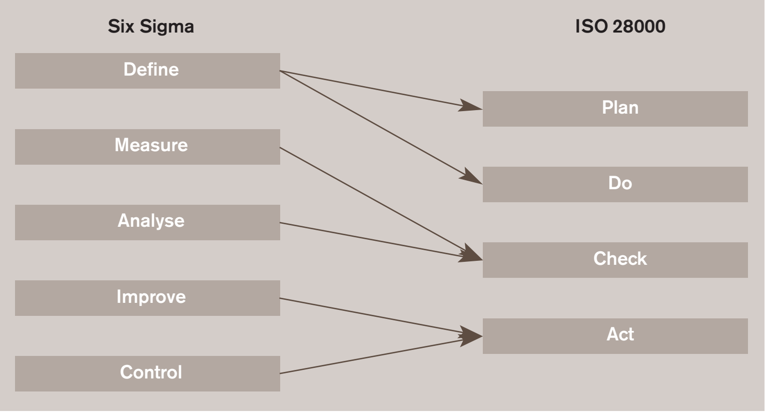
[1] *Ung, S.-T., Bonsall, S., Williams, V., Wall, A. & Wang, J. (2007) "The application of the Six Sigma Concept to Port Security Process Quality Control", Journal of Quality and Reliability Engineering International, 23: 631-639*

in any of these processes. Furthermore, a Six Sigma programme implemented operationally would complement any existing ISO 28000 programme as there is significant overlap between the two vis-à-vis the documentation of procedures, security performance measurement and monitoring and corrective actions. The methodology behind ISO 28000 is based on the cycle of Plan-Do-Check-Act:

- Plan: establish the objectives and processes necessary to deliver results in accordance with the organisation's security policy
- Do: implement the processes
- Check: monitor and measure the processes against security policy, objective, targets, legal and other requirements
- Act: take actions to continually improve performance of the security management system.

As set out above, the methodology behind Six Sigma is based on Define-Analyse-Measure-Improve-Control. The figure below describes the relationship between the methodology behind Six Sigma and the Plan-Do-Check-Act methodology of ISO 28000.

The relationship between Six Sigma and ISO 28000 (Courtesy Risto Talas)



The table below provides a closer analysis of the relationship between Six Sigma and ISO 28000 with specific reference to sections within ISO 28000.

Six Sigma Steps	ISO 28000 section	Description
Define Critical-to-Quality	*4.2. (e) 4.3.4. (a) 4.4.1. (c)*	*Security management policy Security management targets Identify, monitor requirements & expectations of organisation's stakeholders*
Measure	*4.3.4. (b) 4.4.4. 4.5.1.*	*Security management targets Documentation Security performance measurement*
Analyse	*4.3.4. (d) 4.4.1. (h) 4.5.2.*	*Security management targets Ensure security related threats are evaluated etc System evaluation*
Improve	*4.2. (f) 4.6.*	*Security management policy (continual improvement) Management review & continual improvement*
Control	*4.4.5. 4.4.6. 4.5.3. 4.5.4.*	*Document and data control Operational control Security related failures, non-conformities etc Control of records*

Other Six Sigma Steps	ISO 28000 section	Description
Processes	*4.3.3. 4.3.5. 4.4.1.*	*Security management objectives Security management programmes Structure, authority, responsibilities for security management*
Six Sigma Champion	*4.2. (h) 4.4.1 (a)*	*Security management policy visibly endorsed by senior management Appointment of a member of senior management responsible for design, maintenance, documentation & improvement*
Six Sigma Black Belts	*4.4.1. (b)*	*Appointment of members of management with necessary authority to ensure the objectives and targets are implemented*

Performance of a port terminal's detection systems.

The following example shows how Six Sigma can practically be applied in a port terminal which is ISO 28000 compliant or is seeking ISO 28000 compliance. The example is concerned with the port terminal's detection systems. However, first it is necessary to introduce the concept of key performance indicators (KPI's). KPIs are a measure of a security system's performance against certain pre-set benchmarks. The KPIs themselves can be represented as either a positive or negative score, as long as it can be interpreted consistently.

Define

The processes in our example are concerned with the port terminal's CCTV systems, which includes 20 cameras, over a 12 week period.

Measure

The KPIs record the number of hours that any of the cameras are non-operational and record this information on a weekly basis.

Analyse

The KPI of the performance of the security measures for detection allows for one non-operational hour for each camera in any given week but not exceeding 3 non-operational hours every 12 weeks. Furthermore, the total number of cameras being out of action for at least one hour may not exceed 3 in any given week. Any level above either of these measures is deemed to be a non-conformity which requires immediate attention.

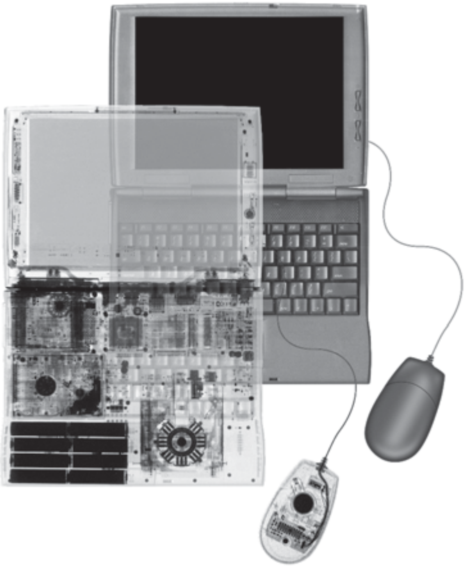
An analysis of the performance of the cameras is shown to be as follows:

camera	week 1	week 2	week 3	week 4	week 5	week 6	week 7	week 8	week 9	week 10	week 11	week 12	Totals
1	0	0	0	0	0	0	1	0	0	0	0	0	1
2	0	0	0	0	1	1	0	0	1	0	0	0	3
3	0	0	1	1	0	0	0	1	0	0	0	0	3
4	1	0	0	0	0	1	1	0	0	0	0	0	3
5	0	1	0	0	0	0	0	0	0	0	0	0	1
6	0	0	0	0	0	0	0	0	0	0	0	1	1
7	0	0	0	0	0	0	0	0	0	0	0	0	0
8	1	0	0	2	0	0	2	0	0	0	0	0	5
9	1	0	0	0	0	0	0	0	0	0	0	0	1
10	0	0	0	0	0	0	0	0	0	1	0	0	1
11	0	0	0	1	0	0	0	0	0	0	0	0	1
12	0	1	0	0	0	0	0	1	0	0	0	0	2
13	0	0	0	0	0	1	0	0	0	0	0	0	1
14	0	0	0	0	0	0	0	0	1	0	0	0	1
15	1	0	0	0	0	0	0	0	0	0	0	0	1
16	0	0	1	0	0	0	0	0	0	0	1	0	2
17	0	0	0	0	1	0	0	0	0	0	0	0	1
18	1	0	0	0	0	0	1	0	0	0	0	0	2
19	0	0	0	0	0	0	0	0	0	0	1	0	1
20	1	0	0	0	0	1	0	0	0	0	1	1	4
Totals	6	2	2	4	2	4	5	2	2	1	3	2	35

The best performing camera was # 7 with zero hours of non-operation. However, both cameras # 8 and # 20 were non-operational for more than 3 hours in the 12 week period. Furthermore, in weeks 1, 4, 6 and 7 there were more than 3 hours of non-operational cameras. Therefore, having recorded the security non-conformities and measuring them against the KPIs, we can conclude that two cameras need attention and that by the second half of the period under study, the number of camera-hours of non-operation had come down to acceptable levels. To translate this into Six Sigma language, each camera had the potential to operate for a total of 2016 hours over the 12 weeks and given that there were 20 cameras, this yields a total of 40320 camera hours. The total number of camera hours of non-operation was 35 across all the cameras over the 12 weeks which is a failure rate of 0.08681% or equivalent to a level between 4 Sigma and 5 Sigma. In order to reach a level of 5 Sigma, the number of camera hours of non-operation across all cameras over the 12 week period must be reduced to less than 9.4 hours.

Calculation:
Five Sigma = 233 per million non-conformities
*Five Sigma camera hours non-operation = (20 cameras * 24 hours * 7 days * 12 weeks) * 233 / 1,000,000 = 9.395 hours*

(Courtesy Risto Talas)



Measuring the Value Created by the Six Sigma process

The key to measuring the value created by the Six Sigma process is in the realisation that the emphasis is no longer on the random inspection of whether security equipment is functioning to its normal specification but in the hands-on reporting of security non-conformities which can be used to build up a picture, over time, of how effectively a security system, such as the CCTV cameras used for detection, are functioning. The Six Sigma process provides the statistical tools for an experienced security officer to be able to measure the performance of any security system against his/her preset levels of acceptable performance. Deviation from these preset levels of acceptable performance in a negative sense will result in an increase in the port terminal's residual security risk.

Case study – *Guard force*

The company were unhappy with the performance of the guard force. A review of their duties and conditions was undertaken which highlighted shortfalls in their knowledge and understanding of their tasks as they had no documented procedures and had not received specific on the job training and issues in maintaining awareness during their shift as they were posted each day for long periods at the same post. Clearly understandable procedures were documented for each post and training given to all guards in their duties. A rota was developed to enable guards to be moved to different positions during their shift in order to maintain their performance.

Overview of Contemporary Supply Chain Security Initiatives

Mandatory Supply Chain Security Initiatives

IMO ISPS Code

The objective of the ISPS Code is to establish an international framework involving co-operation between Governments, Government Agencies, local administrations and the port and shipping industries to protect ships and ports engaged in international trade.

Name	*International Ship and Port Facility Security Code*
Originator	*International Maritime Organisation*
Who Can Apply	• *Ships engaged on international voyages:* • *Passenger ships including high-speed passenger craft* • *Cargo ships including high-speed craft of 500 gross tonnage and upwards* • *Mobile offshore drilling units* • *Port facilities serving such ships engaged on international voyages*
Voluntary / Mandatory	*Mandatory*
Mission	*The protection of ships and ports facilities from unlawful acts.*
Requirements	*For ships:* • *On-scene Security Survey* • *Ship Security Assessment* • *Preparation of Ship Security Plan* • *Implementation of Ship Security Plan* • *Training of Company & Ship Security Officers* • *Verification Procedure* • *International Ship Security Certificate* *For ports:* • *Port Facility Security Assessment* • *Preparation of Port Facility Security Plan* • *Approval of Port Facility Security Plan* • *Implementation of Port Facility Security Plan* • *Training of Port Facility Security Officers* • *Statement of Compliance of a Port Facility*
Benefits	*The full benefits of protected ships and port facilities will only come about once all Contracting Governments put in place and maintain the necessary arrangements for compliance with the ISPS Code*
Website	*http://www.imo.org/*

It is important that all terminals and port facilities that are not currently compliant with the ISPS Code are encouraged to make the necessary changes as soon as possible. In addition to the benefits detailed above, compliance with the ISPS Code is a requirement for many voluntary initiatives.

EU Port Security Directive 65 (2005)

The main objective of the Directive is to introduce a security system in all port areas, establishing a Community framework to guarantee a high and comparable level of security in all European ports. The Directive complements the measures behind the ISPS Code. Taken together, they provide the necessary framework for protecting the whole chain of maritime transport logistics (from the ship to the port via the ship/port interface and the whole port area) against the risk of attacks on European Community territory.

Name	*EU Port Security Directive 65 (2005) of 26 October 2005*
Originator	*European Commission*
Who Can Apply	*All EU Member States' ports in which one or more port facilities are required to comply with the ISPS Code*
Voluntary / Mandatory	*Mandatory*
Mission	*Introduce a security system in all European ports*
Requirements	*EU Member States should rely upon detailed security assessments to identify the exact boundaries of the security-relevant port area, as well as the different measures required to ensure appropriate port security* *Such measures should differ according to the security level in place and reflect differences in the risk profile of different sub-areas in the port* *EU Member States should approve port security plans which incorporate the findings of the port security assessment. The effectiveness of security measures also requires the clear division of tasks between all parties involved as well as regular exercises. This clear division of tasks and the recording of exercise procedures in the format of the port security plan is considered to contribute strongly to the effectiveness of both preventive and remedial port security measures*
Benefits	*The principles and benefits from enhanced security of the ISPS Code are extended beyond the port facility to the whole port area*
Website	*http://europa.eu/legislation_summaries/transport/waterborne_transport/l24162_en.htm*

Advanced Cargo Information

The first advanced cargo information (ACI) requirement introduced in the wake of 11 September 2001 was the US CBP 24 Hour Rule. Since then, additional ACIs have been introduced by the United States, Mexico, Canada, the European Union, China and Japan. They are outlined below and the section concludes with a brief description of the United States' intention to scan 100% of inbound containers by 2012.

24 Hour Rule

The 24-hour rule requires sea carriers and NVOCCs (Non-Vessel Operating Common Carriers) to provide US Customs with detailed descriptions of the contents of sea containers bound for the United States 24 hours before the container is loaded on board a vessel. The rule allows US Customs officers to analyse the container content information and identify potential terrorist threats before the US-bound container is loaded at the foreign seaport, not after it arrives in a US port. The use of such vague cargo descriptions as 'Freight-All-Kinds', 'Said-To-Contain' or 'General Merchandise,' is no longer tolerated. Sea carriers and NVOCCs that violate the 24-hour rule receive 'Do-Not-Load' messages. The 'Do-Not Load' message instructs these parties not to load a specific container that has been found in violation of the 24-hour rule. Carriers and NVOCCs that disregard these 'Do Not Load' messages (and load the cited container) are denied permission to unload this container at any US port.

The tightened reporting requirements for containerised cargo entering the United States as prescribed by the 24 hour rule has forced companies' supply chains towards greater functionality. To meet the 24 hour rule requirements, shipowners and other NVOCCs have extended their electronic commerce technologies by developing e-commerce portals through which their customers can communicate more easily their shipping information and giving customers the ability to manage their shipments by increasing visibility in their supply chains.

Importer Security Filing '10+2 Rule'

The Importer Security Filing (ISF), commonly known as the '10+2' initiative, is a Customs and Border Protection (CBP) regulation that requires importers and vessel operating carriers to provide additional advance trade data to the US CBP pursuant to Section 203 of the SAFE Port Act of 2006. See:

http://www.cbp.gov/linkhandler/cgov/trade/cargo_security/carriers/security_filing/ra.ctt/ra.pdf

‘10+2’ is designed to build on the capability of the CBP’s automated targeting system (ATS) by helping to identify the entities involved in the supply chain and their locations as well as providing more detailed descriptions of the goods to be imported into the United States. The ten items to be transmitted to the CBP by the importer, or their authorised agents no later than 24 hours before loading at the non-US port are:

- Manufacturer (or Supplier)
- Seller
- Buyer
- Ship-to Party
- Container Stuffing Location
- Consolidator (Stuffer)
- Importer of Record/Foreign Trade Zone (FTZ) Applicant Identification Number
- Consignee Number(s)
- Country of Origin
- Commodity Harmonized Tariff Schedule of the United States (HTSUS) Number.

The additional two items that must be submitted by the carrier, electronically to the CBP, within 48 hours of the vessel departing from the last port, inbound US are:

- Vessel Stow Plan
- Container Status Messages.

However, in the event of foreign cargoes remaining on-board or other transit cargoes, only the following five items need to be transmitted 24 hours before loading in the non-US port:

- Booking Party name/address
- Ship-to Party
- Commodity HTS-6
- Foreign Port of Unlading
- Place of Delivery.

Mexico 24 hour rule

On 1 September 2007, Mexican Customs implemented a similar ACI system to the United States. The information which must be transmitted to Mexican Customs at least 24 hours before loading in the non-Mexican port is designed to be similar to that required by the CBP and is as follows:

- Name and complete address of the shipper, consignee and the person who shall be notified of the arrival, as stated in the bill of lading (When the consignee is 'TO THE ORDER OF' the name of the Notify party must be declared)
- Amount of the merchandise and measurement unit, if the merchandise is carried in containers, the amount and measurement unit shall also be specified for each container.
- Gross weight or volume of the merchandise. If the merchandise is carried in containers, the gross weight or volume shall be specified also for each container
- Merchandise description, avoiding general descriptions that do not allow proper identification of the nature of the merchandise; such as 'general cargo', 'dry cargo', 'chemicals', 'perishable items', 'bulk merchandise', 'bulk minerals' or 'FAK'
- Number, quantity and dimensions of containers
- Seal number(s) for each container
- Type of service contracted
- In the case of dangerous merchandise, state class, division and United Nations number, as well as a telephone number for emergencies. See: http://www.hamburgsud.com/WWW/EN/Services_and_Offices/Regional_Information/Asia/Regional_Content/Microsoft_Word_-_NEW_24_HRS_REGULATION_FOR_MEXICO_sep_1_RAS.pdf

Canadian Advance Commercial Information

On 19 April 2004, the Canadian Border Services Agency introduced the advance commercial information programme, which is similar to the US CBP 24 hour rule, requiring marine carriers to electronically transmit marine cargo data to the Canada Border Services Agency (CBSA) 24 hours prior to loading cargo at a foreign port. See: http://www.cbsa-asfc.gc.ca/prog/aci-ipec/menu-eng.html#a1

European Union Pre-Arrival and Pre-Departure

As of 1 July 2009, EU authorities required importers and exporters to lodge pre-arrival and pre-departure summary customs declarations up to 24 hours prior to exportation or importation, depending on the method of transportation. Thus, the EU has become one of the few customs territories in the world requiring not only pre-arrival declarations but also pre-departure customs declarations. The new EU customs rules require the declarations to be stored in electronic format for at least three years. Since many multinational companies will choose to centralise their electronic storage of these documents, they will have to evaluate carefully the applicable EU Member State's national legislation relating to data protection and retention. The AEO Security and Safety Certificate and AEO Customs and Security Certificate are aimed at lessening this burden by providing significant benefits with regard to pre-arrival and pre-departure declarations. Non-AEO entities have to provide pre-departure and pre-arrival declarations consisting of additional security-related information. See: http://www.mwe.com/index.cfm/fuseaction/publications.nldetail/object_id/61581f82-7f64-4c88-b797-c2e63964ed1a.cfm

Japan Advance Cargo Information

On 1 June 2007, Japan Customs introduced their advance cargo information for both marine and air cargoes. The required items include:

- Shipping location and destination of cargo
- Marks, numbers, name and quantity of goods
- Address or place of residence, name or appellation and telephone number of consigner and consignee.

See:http://www.customs.go.jp/english/procedures/advance2_e/index_e.htm

China Advance Cargo Information

From 1 January 2009, Decree No 172 of the General Administration of Customs of the People's Republic of China came into force 'for the purposes of regulating the customs administration of manifests of inbound and outbound means of transport, facilitating international trade and ensuring international trade security'. Under the measures, operators of inbound and outbound means of transport, non-vessel operating common carriers, freight forwarders and shipping agency companies are obliged to submit cargo manifests to Chinese Customs 24 hours prior to the loading of cargo. See: http://english.customs.gov.cn/publish/portal191/tab3972/info162113.htm

United States 100% Container Scanning 2012

The United States legislation 'Implementing Recommendations of the 9/11 Commission Act of 2007' unilaterally introduced 100% scanning requirement for US-bound maritime cargo at the point of export, to be implemented by 1 July 2012. See: http://www.gao.gov/new.items/d08126t.pdf Pilot programmes for 100% scanning have been conducted in Southampton Container Terminal, UK; Qasim International Container Terminal in Karachi, Pakistan; and Cortes in Honduras under the auspices of the Secure Freight Initiative which derived from the Security and Accountability For Every (SAFE) Port Act of 2006. While commentators disagree about the financial and security viability of 100% container scanning, ports should be aware that failure to comply with the legislation may put them at risk of being unable to export to the United States from 2012, though the legislation does allow for a period of up to two years in which the mandatory introduction may be delayed. Nevertheless, there is much opposition to the introduction of the legislation, particularly from the EU, which is considering introducing a requirement for US ports to scan 100% of all containers bound for Europe.

Voluntary Supply Chain Security Initiatives

WCO Framework of Security standards to secure and facilitate global trade

This is a framework of security standards developed by the World Customs Organisation. It intends to provide a new and consolidated platform which will enhance world trade, ensure better security against terrorism, and increase the contribution of Customs and trade partners to the economic and social well-being of nations. It aims to improve the ability of customs to detect and deal with high-risk consignments and increase efficiency in the administration of goods, thereby expediting the clearance and release of goods.

The SAFE Framework sets forth the principles and the standards and presents them for adoption as a minimal threshold of what must be done by WCO Members.

Name	*WCO SAFE Framework of Standards*
Originator	*World Customs Organisation*
Who Can Apply	*Member States (159 countries have indicated their intention to implement the WCO Framework at Jan 2010)*
Voluntary / Mandatory	*Voluntary*
Mission	• *Establish standards that provide supply chain security and facilitation at a global level to promote certainty and predictability* • *Enable integrated supply chain management for all modes of transport* • *Enhance the role, functions and capabilities of Customs to meet the challenges and opportunities of the 21st Century* • *Strengthen co-operation between Customs administrations to improve their capability to detect high-risk consignments* • *Strengthen Customs/Business co-operation* • *Promote the seamless movement of goods through secure international trade supply chains*
Requirements	*For the Customs to Business Partnerships Pillar* • *An appropriate record of compliance with Customs requirements* • *A demonstrated commitment to supply chain security by being a participant in a Customs-Business partnership programme* • *A satisfactory system for managing commercial records*
Benefits	*Obtaining enhanced competitiveness in national and international markets due to reduction in delays and costs which are achieved with predictable and efficient movement of goods across borders*
Website	*http://www.wcoomd.org/home.htm*

For those Customs administrations expressing a need, assistance in the form of a programme for sustainable capacity building (Columbus Programme) is being implemented by the WCO Secretariat, with the committed support of other WCO Members. The programme has been in existence since 1 January 2006 and is conducted in three phases. The first phase (needs assessment) is a comprehensive diagnostic assessment of the current situation in the Customs Administration. The second phase (implementation) is support for action planning, donor matchmaking, planning of pilot activities and implementation. The third phase (monitoring) involves the monitoring of progress. Further information on the Columbus Programme, is available on the WCO website.

http://www.wcoomd.org/home_wco_topics_cboverviewboxes_programmes_cbcolumbusprogrammeoverview.htm

For the customs-to-business partnerships pillar each Customs administration will establish a partnership with the private sector in order to involve it in ensuring the safety and security of the international trade supply chain. The main focus of this pillar is the creation of an international system for identifying private businesses that offer a high degree of security guarantees in respect of their role in the supply chain. These business partners should receive tangible benefits in such partnerships in the form of expedited processing and other measures.

Below are some examples of the initiatives either derived from or aligned with the WCO SAFE Framework.

EU AEO, European Union Authorised Economic Operator

The EU has entered into legislation 'The Security Amendment to the Community Customs Code' which promotes a co-ordinated approach to securing the international supply chain for all EU businesses. The Amendment entered into force on 1 January 2008 across the EU allowing Customs authorities to grant the status of Authorised Economic Operator ('AEO') to any business that satisfies EU criteria which, in turn, will be recognised across all Member States.

AEOs will be able to benefit from facilitations for customs controls or simplifications for customs rules or both, depending on the type of AEO certificate. There are three certificate types:

- **Customs Simplifications.** AEOs will be entitled to benefit from simplifications provided for under the customs rules.
- **Security and Safety.** AEOs will be entitled to benefit from facilitations of customs controls relating to security and safety upon entry of the goods into the customs territory of the Community, or when the goods leave the customs territory of the Community.
- **Customs Simplifications/Security and Safety.** AEOs will be entitled to benefit from both simplifications provided for under the customs rules and from facilitations of customs controls relating to security and safety (a combination of 1 and 2).

Name	*European Union Authorised Economic Operator*
Originator	*European Commission*
Who Can Apply	• *Manufacturers, importers, exporters, brokers, carriers, consolidators, intermediaries, ports, airports, terminal operators, integrated operators, warehouses and distributors who are legal entities within the EU* • *Shipping lines and airlines that do not have a legal entity in the EU but have a regional office may also apply for a Safety & Security Certificate*
Voluntary / Mandatory	*Voluntary*
Mission	*Enhance security through granting recognition to reliable traders and encouraging best practice at all levels in the international supply chain*
Requirements	• *Customs compliance* • *Appropriate record keeping* • *Financial solvency* • *Security and safety standards*
Benefits	• *AEOs will be recognised worldwide as safe, secure and compliant business partners in international trade* • *AEOs will be given a lower risk score in risk analysis systems when profiling* • *If physical controls are to be conducted AEOs will be given priority treatment* • *Mutual recognition of AEO programmes under Joint Customs Co-operation Agreements could result in faster movement of their goods through third country borders* • *Reduced data sets for entry and exit summary declarations – only for AEO safety and security* • *AEOs will be in a stronger position to benefit from simplified procedures*
Website	*http://ec.europa.eu/taxation_customs/resources/documents/customs/policy_issues/customs_security/AEO_guidelines_en.pdf*

The main benefits of AEO status in the EU started to be realised with the introduction, in July 2009, of the requirements for pre-arrival and pre-departure and the changes linked to the Modernised Customs Code. The main changes are:

- rationalisation of the legal framework and the definition of customs rules and procedures

- greater standardisation of customs rules and their implementation, through increased ‘communitisation’ of economic operators' rights and obligations, in particular as regards decisions, simplifications and guarantees
- simplification of customs procedures - especially through computerisation and the possibility of managing them at EU level (‘centralised customs clearance’)
- computerisation of all declarations and data exchange
- interoperability of national customs computer systems - facilitating trade while ensuring tight control through common management of risks and easier co-operation between customs authorities
- the basis is laid for new facilities such as self-assessment by operators and single interfaces or one-stop services.

The deadline for the implementation of the Modernised Community Customs Code is 24 June 2013. For further information see:

http://ec.europa.eu/taxation_customs/customs/procedural_aspects/general/community_code/index_en.htm

C-TPAT, Customs-Trade Partnership Against Terrorism

C-TPAT is a joint government-business initiative to build co-operative relationships that strengthen overall supply chain and border security. Central to the security vision of C-TPAT is the core principle of increased facilitation for legitimate business entities that are compliant traders. Only importers and carriers based in the US are eligible to participate in this program and one of its main motivations is to protect US borders from terrorist attacks occasioned by goods entering the country.

Under C-TPAT, non-US based marine port authority and terminal operators (MPTO) may be eligible for membership of the C-TPAT scheme but only following an invitation from US Customs and Border Protection (CBP) to join. The terminal must handle cargo vessels departing to the US and have a designated company officer that will be the primary cargo security officer responsible for C-TPAT.

Name	*Customs-Trade Partnership Against Terrorism (C-TPAT)*
Originator	*US Customs & Border Protection*
Who Can Apply	• *US Importers of record* • *US/Canada Highway Carriers* • *US/Mexico Highway Carriers* • *Rail Carriers* • *Sea Carriers* • *Air Carriers* • *US Marine Port Authority/Terminal Operators* • *US Air Freight Consolidators, Ocean Transportation Intermediaries and Non-Vessel Operating Common Carriers (NVOCC)* • *Mexican and Canadian Manufacturers* • *Certain Invited Foreign Manufacturers* • *Licensed US Customs Brokers* • *Non-US marine port authority and terminal operators*
Voluntary / Mandatory	*Voluntary*
Mission	*To build co-operative relationships that strengthen and improve overall international supply chain and US border security*
Requirements (continued)	*Participants will sign an agreement that commits them to the following actions:* *1. Conduct a comprehensive self-assessment of supply chain security using the C-TPAT security guidelines (available via the website) encompassing the following areas:* • *Procedural security* • *Physical security* • *Personnel security* • *Education and training* • *Access controls* • *Manifest procedures* • *Conveyance security* *2. Develop and implement a program to enhance security throughout the supply chain* *3. Communicate C-TPAT guidelines to other companies in the supply chain and work in relationships with these companies* *ISPS Code and MTSA compliance are a prerequisite for C-TPAT MPTO membership, and only terminals in compliance with the applicable ISPS code requirements may be utilised by C-TPAT members. The Physical Access Controls and Physical Security provisions of these criteria*

continued over…

Requirements (continued)	*are satisfied for ISPS regulated vessels and port facilities by those vessels' or facilities' compliance with the ISPS Code and Coast Guard regulations*
Benefits	• *Reduced number of inspections on entering the USA* • *The incorporation of good sound security practices and procedures into existing logistical management methods and processes* • *Greater supply chain integrity* • *Reduced risk mitigation* • *Reduced cargo theft and pilferage* • *Stronger brand equity* • *Improved asset utilisation* • *Greater efficiency between internal and external functions* • *Improved security for their workforce* • *Improved marketability* • *Understanding the end to end process, including knowing each entity along the supply chain*
Website	*http://www.cbp.gov/xp/cgov/trade/cargo_security/ctpat/*

PIP, Partners in Protection

PIP is the Canada Border Services Agency (CBSA) programme that enlists the co-operation of private industry to enhance border and trade chain security, combat organised crime and terrorism and help detect and prevent contraband smuggling.

In June 2008 PIP achieved mutual recognition and compatibility with the US C-TPAT programme and a strengthened programme was introduced.

Name	*Partners in Protection*
Originator	*Canadian Border Services Agency*
Who Can Apply	*1. Eligible business categories: importer, exporter, highway carrier, marine carrier, air carrier, rail carrier, customs broker, courier, warehouse operator, freight forwarder, shipping agent* *2. Owners or operators of facilities in Canada that are directly involved in the importation and exportation of commercial goods*
Voluntary / Mandatory	*Voluntary*

continued over…

Mission	*Enlist the co-operation of private industry in efforts to enhance border and trade chain security, combat organised crime and terrorism, and help detect and prevent contraband smuggling*
Requirements	• *Completion of a Security Profile demonstrating all minimum security requirements have been met* • *Application review and onsite validation visit* • *Revalidation including updated Security Profile and site visit every 3 years* • *Exchange of information* • *Awareness sessions*
Benefits	• *Participants in Customs Self Assessment programme are eligible to apply to the FAST programme to be able to use designated FAST lanes to cross the border into Canada* • *Improve security levels* • *Access to CBSA expertise* • *Enhance reputation by being a secure, low-risk company* • *Gain a competitive advantage* • *Contribute to the protection of Canadian society*
Website	*http://www.cbsa-asfc.gc.ca/security-securite/pip-pep/menu-eng.html*

Secure Exports Scheme

It is designed to protect cargo against tampering, sabotage, smuggling of terrorists or terrorist-related goods, and other transnational crime, from the point of packing to delivery. Exporters from New Zealand are eligible and encouraged to participate: especially those moving goods to the US. The programme emphasises that security measures are customisable depending on the applicant's situation.

A Mutual Recognition Arrangement has been signed between NZ Customs Service and United Stated Customs and Border Protection. This acknowledgement by both administrations of their respective customs-to-business supply chain security programmes will benefit their members by enhancing border clearance privileges where both parties are partners in their respective countries' schemes.

Name	*Secure Exports Scheme*
Originator	*New Zealand Customs Service*
Who Can Apply	*All exporters, by all modes of transport, to all destinations*
Voluntary / Mandatory	*Voluntary*
Mission	*Keeping trade flowing and secure*
Requirements	• *Accurate advanced export information* • *Maintaining an agreed level of security* • *Working in partnership with customs*
Benefits	• *Secure supply chain from point of packing to time of loading for export* • *'Green lane' status means cargo can be moved to port/airport facilities knowing the potential for Customs intervention for security is low* • *Ability to demonstrate compliance with security standards when contracting to supply overseas importers that are committed to supply chain security* • *Joining the scheme will enhance your border clearance privileges in the United States provided your client is a member of C-TPAT (Customs Trade Partnership Against Terrorism) initiated by US Customs and Border Protection* • *In the event of trade disruption caused by security alerts, partners' exports are likely to experience minimal disruption as their security can be assured* • *The World Customs Organisation's Framework of Standards to Secure and Facilitate Global Trade is being adopted and implemented by a large number of international Customs administrations. By joining this scheme, partners will already have in place security measures that comply with these standards* • *Reduced fees for the lodgement of all export entries.* • *Customs can provide advice and assistance if you strike unexpected issues with your export goods at overseas borders*
Website	*http://www.customs.govt.nz/exporters/Secure+Exports+Scheme.htm#howitworks*

Voluntary Business - Other Security Initiatives driven by Customs or Industry

CSI – Container Security Initiative

The Container Security Initiative was launched in 2002 by the US Customs and Border Protection agency with 20 of the world's largest container terminals. By March 2008 there were 58 CSI ports worldwide representing approx 86% of US imports.

CSI addresses the threat to border security and global trade posed by the potential for terrorist use of a maritime container to deliver a weapon. CSI uses a security regime to ensure all containers that pose a potential risk for terrorism are identified and inspected at foreign ports before they are placed on vessels destined for the United States. The US Customs and Border Protection (CBP) has stationed teams of US officers to work together with host customs administrations to establish security criteria for identifying high-risk containers. Those administrations use non-intrusive inspection (NII) and radiation detection technology to screen high-risk containers before they are shipped to US ports.

Name	*Container Security Initiative (CSI)*
Originator	*US Customs & Border Protection*
Who Can Apply	*All Customs Administrations*
Voluntary / Mandatory	*Voluntary*
Mission	*Target and pre-screen containers and develop additional investigative leads related to the terrorist threat to cargo destined for the United States*
Requirements	*The Customs Administration must be able to inspect cargo originating, transiting, exiting, or being transshipped through a country. NII equipment (including equipment with gamma or X-ray imaging capabilities) and radiation detection equipment must be available and utilised for conducting such inspections. This equipment is necessary in order to meet the objective of quickly screening containers without disrupting the flow of legitimate trade* • *The seaport must have regular, direct, and substantial container traffic to ports in the United States* • *Commit to establishing a risk management system to identify potentially high-risk containers, and automating that system. This system should include a mechanism for validating threat assessments, targeting decisions and identifying best practices*

continued over…

Requirements (continued)	• *Commit to sharing critical data, intelligence, and risk management information with the US CBP in order to do collaborative targeting, and developing an automated mechanism for these exchanges* • *Conduct a thorough port assessment to ascertain vulnerable links in a port's infrastructure and commit to resolving those vulnerabilities* • *Commit to maintaining integrity programmes to prevent lapses in employee integrity and to identify and combat breaches in integrity*
Benefits	• *A significant measure of security for the participating port as well as the United States* • *Better security for the global trading system as a whole.*
Website	*http://www.cbp.gov/xp/cgov/trade/cargo_security/csi/*

CSI, a reciprocal program, offers its participant countries the opportunity of sending their customs officers to major US ports to target ocean-going containerised cargo to be exported to their countries. Likewise, CBP shares information on a bilateral basis with its CSI partners. Japan and Canada currently station their customs personnel in some US ports as part of the CSI program.

BASC, Business Alliance for Secure Commerce (formerly: Business Anti-Smuggling Coalition)

BASC was created in 1996 when a North American company, importing through the port of San Diego, California, submitted a proposal to the US Customs Service that would implement supply chain security procedures to reduce the risk of legitimate cargo being used by illegal organisations for narcotics trade, cargo theft and contaminated cargo. The proposal also sought to complement and strengthen the US Customs Service's Carrier Initiative Program (CIP) and Land Border Carrier Initiative Program (LBCIP), in order to modify the thinking of production companies towards implementing preventive measures in place of repressive measures.

BASC is a co-operation programme between the private sector and national and international organisations, created to promote a secure global supply chain. The main goal is to encourage, within its membership, the development and implementation of voluntary steps to address the risks of narcotics and merchandise smuggling through legitimate trade, as well as the threat of a disruption in the global economy brought about by terrorism.

BASC procedures require a security program which consists of a number of operating measures adopted to protect an organisation, its assets, properties, employees and customers.

Name	*BASC, World BASC Organisation*
Originator	*A US importer with the US Customs in 1996. Since then grown by Business, supported by US CBP, International Chamber of Commerce, World Customs Organisation*
Who Can Apply	*Member Countries* *Customs Administrations* *International Organisations* *Associations* *Businesses*
Voluntary / Mandatory	*Voluntary*
Mission	*Secure and facilitate international trade by the establishment and administration of global security standards and procedures applied to the supply chain in association with customs administrations and government authorities*
Requirements	*A security program which consists of a number of operating measures adopted to protect an organisation, its assets, properties, employees and customers* *The factors to consider in preparing a security program include:* • *Organisational security requirements* • *Potential of the organisation to meet those requirements* • *The organisation's vulnerability to current and future security risks* • *Available options to the organisation to cover its security needs* *Other important aspects that should be included in a Security Plan are:* • *Clear definition of security requirements* • *Written procedures for internal/external notification of security* • *Mechanisms to establish accountability in case of theft or robbery* • *Handling of documents and files* • *Procedures when checking lighting and perimeter fencing* • *Procedures when closing facilities (doors, gates, windows, etc)* • *Security systems to check entry and exit of people and/or vehicles*

continued over…

Requirements (continued)	• *Procedures for handling cargo* • *Definition of policies for external monitoring* • *Control and management of keys and conducting periodic inventory* • *Policies and procedures for personnel hiring* • *Policies to be applied in criminal background checks* • *Procedures for obtaining photographs and fingerprints of all employees* • *Assignment of responsibilities for contract security personnel* *To maintain the security programme it is important to:* • *Update the safety and security programme at least once a year* • *Update the security methods included in the plan* • *Assessment of contract services* • *Personnel training*
Benefits	• *Improved competitiveness and image of the companies* • *Expanded opportunities for businesses in international markets* • *Reduced risks related to international trade* • *Diminished economic losses due to inefficiency* • *A developed atmosphere of safe work* • *Improved control and traceability of the supply chain*
Website	*http://wbasco.org/index-eng.htm*

TAPA (Transported Asset Protection Association)

This is an association of security professionals and related business partners from hi-tech companies, who have been working together to address emerging security threats common to the technology industry and hi-tech businesses.

The goals of TAPA include:

- Security of goods from theft
  - – in transit
  - – during in-transit storage
  - – while in warehousing
- Specifies minimum standards for security throughout the supply chain
- Describes methods for maintaining standards
- Includes a process for TAPA certification.

Name	*Transported Asset Protection Association*
Originator	*Hi-tech companies*
Who Can Apply	*Hi-tech companies*
Voluntary / Mandatory	*Voluntary*
Mission	*To address cargo theft problems facing the hi-tech industry on a collective level*
Requirements	• *Have a security policy, procedures and plan* • *Submit to periodic audits and certification*
Benefits	• *Reduced losses associated with transportation related thefts* • *Economic benefits derived from more attractive freight carrier contract terms* • *Reduced customer inconvenience and disruption* • *A reduction in the incidence of lost sales* • *The combined leverage of over 50 of the world's largest technology companies at work to negotiate more favourable terms with insurance companies and freight carriers*
Website	*http://www.tapaonline.org/*

Supply Chain Security Technologies & Their Applications

This section will provide an overview of some of the different technologies that may be used to provide security protection in the supply chain. It does not aim to be exhaustive or to provide detailed technical information, but rather may act as a starting point for the process by which companies may evaluate the value and suitability of technologies to their needs.

Technology today is evolving faster than ever and many of the types of equipment discussed are continually being improved to provide more suitable and effective solutions to security problems. This evolving landscape is also reflected in the cost of many technologies where advances have enabled costs to be reduced and, with higher adoption, economies of scale may begin to be seen.

The technologies have been divided into three sections

- **Supply chain links** – technologies that may be deployed to monitor the security of goods throughout the supply chain.
- **Supply chain nodes** – technologies that may be deployed to provide security at individual nodes along the supply chain.
- **Data Exchange Protection** – the protection of information sent electronically.

The development or upgrading of any security system should be based on a thorough threat and risk assessment. Only by understanding the risks to the business can a company research and determine the most appropriate mitigation strategies.

Solutions may be found by implementing processes, or deploying people or technology. When reviewing possible mitigation for identified risks a company should consider all three of these solutions and choose mitigation in proportion to the perceived exposure. In choosing the most appropriate mitigation companies will need to consider such things as their risk tolerance, impact on or assistance it may provide to operations, resources that may be required, cost and return on investment.

Technology supports and reinforces security processes and provides tools for personnel but it can’t stand alone in providing effective security.

Security should co-ordinate with key operational departments in the design of its technology platforms. It should complement existing work flows and not have a negative impact on throughput or productivity.

Compatibility with existing systems and infrastructure and the ability to allow the integration of future applications should be a primary factor in determining technology investment.

Full technical and operational specifications and service delivery should be documented to ensure that expectations are met and that the company has full legal and financial redress for any shortfalls in service by providers.

The company should consider the ease of use of any technologies and ensure the provision of comprehensive training to all users, including knowledge transfer, as a key element of any contracted service.

It would be impossible for anyone to have a full understanding of all the technologies available and it is recommended that companies participate in industry groups and seek references from other users, where possible, to understand issues such as climatic ranges that may impact the effectiveness of technologies.

Supply Chain Links

Container seals

Container seals are either mechanical or electronic and each has a unique identification number. They are fixed to the container doors to act both as a deterrent to illegal access to the container for the purpose of removal or damage to the goods, or the inserting of something illegitimate within the container and to provide easily observed evidence of tampering.

A missing or broken seal, or a seal with a different number to the cargo documents, indicates that the container may have been accessed by an unauthorised person during transit.

Seals should be placed on the container by the party responsible for stuffing the container and should include procedures for ensuring the verification of the contents prior to sealing. Should these procedures be inadequate, illegitimate cargo may easily be placed in the container prior to sealing and the seal will then imply a false legitimacy to the goods.

Seals themselves also need to be managed in a secure way to ensure that they are not obtained and used by other parties which again may imply false legitimacy to goods. Seals should be kept in a secure cabinet or area where they can only be accessed by authorised persons. Records should be kept of seals issued which are regularly audited to ensure that none are missing.

The usefulness of seals is dependent on the adherence to checking of the integrity of the seal at each change of custody within the supply chain and procedures being in place detailing the action to be taken when a missing, broken or changed seal is found. This relies on seal documentation being provided at each node in the supply chain and the correct checking of the seal by each participant which, as a manual process, can be time-consuming. It is in the best interest of each party involved in a change of custody to ensure the verification of seal integrity to ensure that any tampering can be traced to its source in the supply chain.

The International Organisation for Standardisation has issued ISO/PAS 17712 Freight containers – mechanical seals. This details various types of mechanical seals including high security seals which are a requirement for all containers in transit to the United States and have been endorsed by the World Customs Organisation. A source of suppliers whose products conform to this ISO standard can be found on the International Seal Manufacturers Association website: http://www.ismasecurity.com/.

In reality, mechanical seals are a deterrence that it is easy to overcome and are therefore in effect a means of noticing that a container may have been tampered with. They may be broken easily and some may be replicated with little difficulty. In addition, experienced thieves have devised ways to gain entry to a container by bypassing the sealed container doors, or removing and replacing the original seal without damage.

Electronic seals

Often known as e-seals, these are electronic devices that use batteries or electrical power to detect tampering. Electronic seals are usually more expensive than mechanical seals, but may be reusable, depending on the precise design functionality. Transponder seals are not electrified but are briefly powered up by the seal reader to check if tampering has occurred.

There are several different types of e-seal, with the most common being RFID (Radio Frequency Identification, see below). All are capable of reporting sensor information and data that go beyond the seal status and ID.

As with any security system, the level of risk to the supply chain, the desired outcome from deploying a particular technology, the advantages and disadvantages of the deployment and the cost/benefit ratio should all be considered.

There are many different solutions within this field and the compatibility of these systems is a major factor in choice for deployment. It is of no benefit for the shipper to apply RFID to a container if there are no compatible readers en-route.

RFID is constantly evolving to provide different abilities, suitability and costs. One topical example is from the ZigBee Alliance which is focusing on retail services including supply chain management. Whilst this may prove to be a highly effective development which may reduce the cost of seals, it will introduce yet another system.

Bar Codes & RFID tags

A barcode is an optical, machine-readable, representation of data that can be read by optical scanners (barcode readers), or scanned from an image by special software.

Bar codes are widely used by manufacturers and retailers for the easy identification of goods and are increasingly used on pallets for the accurate tracking of cargo through the supply chain.

Bar code systems usually require a person to scan a label or tag to capture the data. RFID is designed to enable readers to capture tag data and transmit it to a computer system–without user intervention and can, therefore, be used to reduce the amount of time and labour needed to input data manually and to improve data accuracy.

RFID is a generic term that is used to describe a system that transmits the identity (in the form of a unique serial number) of an object or person wirelessly, using radio waves.

There are many different types of RFID systems and it is important to choose the right type of system for the particular application.

There are two main categories of RFID systems, Passive and Active. Both use radio frequency energy to communicate but the method of powering the tags is different.

- **Passive** – relies upon RF energy transferred from the reader to the tag
- **Active** – has its own internal power source (battery).

Passive tags can be packaged in many different ways, cost from 20-40 cents, are commonly disposable and require no maintenance. They have a short read range of a few cm to a couple of metres.

Active tags are used more on large assets such as cargo containers which need to be tracked over longer distances. They may have a read range of up to100 metres.

There are two main types of active tags:

- **Transponder** – activated when it receives a signal from a reader and broadcast information.This system conserves battery life
- **Beacon** – emits a signal, at pre-set intervals, which is picked up by readers, normally in a fixed location. Several readers may be positioned around a perimeter where the precise location of an asset needs to be tracked.

Active tags may cost as much as US$50 depending on the amount of memory, battery life and any additional sensors required, although the constant development of technologies within this field is reducing the costs.

Tags can operate at low, high and ultra-high frequency (UHF). It is not necessary to understand the communication methods but end users do need to understand the basic characteristics of the different systems and what affects their performance.

Low and high frequency systems have a smaller reader field which can be more easily controlled. Ultra-high frequency systems are harder to control because energy is sent over long distances. The radio waves can bounce off other surfaces and reach untargeted tags.

Low and high frequency systems also work better than UHF systems around metal and water as the radio waves do not bounce off metal and cause false reads and are better able to penetrate water.

The goal of using RFID in supply chains is to gain 'visibility'. The information from tags attached to individual items or pallets, as they are loaded into a container, can be written onto a tag on the container. As the container travels through the supply chain its tag can be read at different nodes to confirm its location. However, each of the nodes along the supply chain would need to have compatible readers installed. The possible interception of information held on an RFID tag does need to be considered and, where it is not necessary to hold the information locally, it would be recommended that it is not. Ideally, a tag which just identifies the item (eg. container) though a unique ID would be recommended with any further information held within other systems that can be accessed by those that need to. Where electronic seals are used the RFID would also need to hold information on the status of the seal integrity.

The other alternative is to use mobile or satellite technology together with a GPS system to enable direct communication between the tag and computer system which would include its position at any given time. These systems rely on the availability of the services and may be compromised where line of sight to satellites is not easy, for example in a stack of containers.

Whilst the advantages of being able to track goods throughout their transit of the supply chain are obvious, RFID has as yet to become a widely used technology for security purposes. The integration of systems throughout the supply chain where many parties may be involved requires co-operation and agreement on who bears the cost of the infrastructure and what type to use. The nature of supply chains also means that the company who initially attaches the RFID tag is unlikely to recover it and, therefore, they must be disposable and, hence, the cost minimal. The cost of RFID tags has not reached a level where there will be large scale adoption of the technology, however, the reduction in cost of production relies on economies of scale. At present the use of RFID is generally confined to high-value or highly-sensitive goods where the cost/benefit ratio is acceptable.

RFID tags that form part of a container seal are known as electronic seals. If the container is opened without authorisation, that information is communicated to a computer the next time the RFID tag in the seal is read. Depending on the RFID capability the tag may also be able to record the time the seal was tampered with or send a 'mayday' message at the actual time of tampering.

Active RFID tags can also be used to provide other functions for security purposes eg. they could be combined with motion sensors so that when objects are moved without authorisation, an alarm is sounded.

	Active RFID	Passive RFID
Tag power source	*Yes*	*No – energy transferred from the reader via RF*
Availability of tag power	*Continuous*	*Only within field of reader*
Required signal strength from reader	*Low*	*High – must power the tag*
Available signal strength from tag	*High*	*Low*
Communication range	*100m*	*10m or less*
Fast multiple Tag collection by reader	*Yes*	*No – limited speed*
Sensor capability	*Continuously monitor and record sensor input and time-stamp events*	*Can only read sensor values when tag is powered by reader. No time-stamp*
Data storage	*Large data storage and can have data search and access capabilities*	*Small read/write data storage*
Area monitoring	*Yes*	*No*

Smart Containers

A smart container is one which has sensors installed and a means of communicating the information from them.

Sensors which may be located within the container can detect changes in light levels, temperature, humidity, as well as chemical, nuclear, radiological and biological agents and materials. GPS may also be used to give real time location or RFID for specific tracing at nodes along the supply chain. Communications in some form are essential for distributing the information to the relevant parties and may be via GPS or satellite depending on the coverage required.

Smart containers may provide information to support some or all of the following:

- Tracking/tracing
- Integrity and condition monitoring

- Inventory monitoring
- Container identity verification.

The information provided by a smart container may benefit all parties in the supply chain.

Such sensors were successfully trialled as part of Operation Safe Commerce, the pilot studies for secure containerised trade lanes initiated by US Customs. Research studies and trials continue within the supply chain but to date this technology has not been generally adopted.

Tracking systems

Real time locations of containers, vessels or vehicles in the supply chain can be provided by tracking systems.

A GPS tracking unit is a device that uses a Global Positioning System to determine the precise location of a vehicle, person, or other asset to which it is attached and to record the position of the asset at regular intervals.The recorded location data can be stored within the tracking unit or it may be transmitted to a central location data base, or internet-connected computer, using a cellular (GPRS) radio, or satellite modem embedded in the unit.This allows the asset's location to be displayed against a map backdrop either in real time or when analysing the track later. Additional functions may include such things as alerts for deviations from defined routes and engine cut-outs.

This is a high-end solution and, therefore, has a much higher cost, however it can supply full visibility for the transit of goods through the supply chain enabling immediate identification of deviations or problems en-route and aid optimisation of the supply chain.

Supply Chain Nodes

The nature of companies operating in the supply chain is to facilitate the movement of goods for other parties. Every organisation also owns assets in the form of buildings, yards, vehicles, computers etc, which all require access, from time to time, by staff, contractors, visitors and authorities. Physical Access Control is the controlling of who and when access to these assets or goods is granted.

Physical Access control can be achieved by such means as fencing, guards, gates, locks or with assistance from computers and software.

Fencing

In order for a fence to have any protective value it must be in a good state of repair. This means it should be intact, the fabric taut and well secured to its upright supports and the supports well anchored in the ground. It should not, for example, be possible simply to unbolt the upright.

There are many types of fencing but, as guidance, a fence should, ideally, be constructed of welded mesh to a height of over two metres. It should be topped with outward facing angle irons or 'V' irons which support barbed wire and/or topped with razor wire. Where the fence meets an area such as the waterfront, there should be some overhang, if possible with coiled razor wire hung from the end.

Access under the fence line should be considered and the fence secured either to the ground or a barrier such as K-blocks or a cross rail installed between the uprights. Cross rails are also useful to have at the top and, ideally, in the middle of the fence to help keep the fabric taut and to increase the strength of the fence line.

Consideration may also be given to reinforcing the fence line to prevent vehicles being driven through it (either with or without cutting the fence) either to gain access or to remove goods.The topography of the facility may, itself, be sufficient to fulfil this goal ie. a ditch, steep hill, trees, pipe or rail line. In areas where the topography provides no natural obstacles a barrier such as K-blocks may be installed.

An incidental benefit of installing a physical barrier is the reduction in accidental damage to the fence, from operations, which leads to a reduction in maintenance costs. This may, quite quickly, compensate for the extra installation cost.

Intrusion Detection Sensors

Traditionally, perimeter security has been provided by fences, often complemented by security guards. Using security guards for this purpose can often be expensive and inadequate, and detection systems are available to enhance this capability.

Intrusion detection sensors must reliably detect intruders attempting to cut, climb or lift the perimeter fence and, at the same time, reject environmental 'noise' such as that caused by adverse weather.

Fence detection systems can be as simple as a disturbance-sensitive cable attached to an existing fence, or they can take the form of a fence themselves. Performance of the detection system is largely dependent upon the quality of the fence and its installation. A properly installed fence sensor, associated with a high-quality fence, should provide a good system. The type and construction of the fence will determine what type of sensor can be used.

There are several different types of fence sensors eg.

- **Taut wire** – high tension wires with sensors that detect displacement. They can be mounted on existing structures or can be stand alone. They look almost like a traditional fence
- **Electrostatic field** – can be set to detect intruders up to 1 metre from the fence line
- **Fence disturbance sensor** – wire sensors installed in a fence (eg. chain link), which are sensitive to vibrations
- **Infrared beam** - trips an alarm when the beam is interrupted.

Many sensor systems can be integrated with other technologies such as CCTV. Whilst these systems may provide good security monitoring they incur the additional expense of installation and maintenance. Other pitfalls are that they can be accidentally tripped or even knocked out by a facility vehicle backing into the fence or may be too sensitive and susceptible to trip in weather conditions such as high winds.

The monitoring of such systems has to be undertaken in a consistant manner with a response to every alarm no matter how many times it happens. A common tactic used against alarm systems is to repeatedly trip them so that, eventually, the monitoring becomes ineffective or the system is turned off.

Case study – *Intrusion detection sensors*

Intrusion detection sensors had been fitted to a fence line to provide alarms on movement. The fence in place was not suitable for the sensors as it had too much movement during windy conditions and so frequently false alarmed. This led initially to the alarms being ignored and finally to the system being disabled. The functionality of this equipment for the conditions was not fully evaluated and the contract entered into did not provide for any recompense for its unsuitability.

Access Points

From a security perspective, the fewer access points a facility has the better.

Access points should be designed to ensure that they provide similar protection to the fence line when closed and/or unattended eg. the top of a gate should have similar barbed or razor wire and it should not be possible for someone to gain entry underneath, in particular this should be considered with rail gates where rails may be raised leaving a gap under the gate.

The design of gates should be such that it is not possible to unbolt a gate or remove it from its hinges.

The choice of the means of security for access points should reflect the volume and type of traffic, and the security level required.

Manual Gates & Locks

Manual gates which are locked using mechanical locks or padlocks are an effective form of access control and are generally inexpensive, easy to use and will not stop functioning during a power failure. They are mainly suited to access points which are used infrequently, although can be effective for main access points controlled by security guards. The main problem that arises is the management of keys for the lock or padlock. Strict control needs to be maintained with a limited number of persons having access to the keys and effective procedures in place for lost keys.

Manual gates and locks do not identify who, when and how many times a room, building or site has been accessed. Where manual gates are used, manned by security guards, a suitable system for identifying authorised persons and vehicles will need to be in place eg. photo ID card.

Automated Gates and Barriers

Automated gates and barriers are used to control access by vehicles and pedestrians.

Consideration should be given to the ability to integrate automated access control into any pre-existing identity management system, the ability to manually operate during power failure and the ability to provide unimpeded exit during an emergency situation.

There are many different types of automated access point controls available including barrier/boom gates, swing/sliding gates, rising bollards, turnstiles, revolving doors and pedestrian barriers.

Electric gates can provide automated access:

- at scheduled times
- upon an authorised access card transaction
- using a manual button or wireless key.

Barrier/Boom gates

These provide both visual and physical deterrence to vehicles trying to enter a facility. They are ideally suited to low security areas such as staff car parks or high frequency access points where fast throughput is required. Barrier/boom gates allow fast access to an area. However, they provide no barrier to a pedestrian and can easily be breached by a vehicle with little damage, if any, to the vehicle.

Swing and sliding gates

These are heavier and more robust and are suited for use in higher security areas and after-hours vehicle access points as they physically block pedestrian and vehicle access. In contrast to boom gates, they are slower moving, more expensive, require more maintenance and may cause disruption during a break down due to their restrictive nature.

In cases where a vehicle access point is manned during business hours and unmanned out-of-hours, a combination of boom gate and swing/sliding gate is often used. During business hours, the heavier gate is left open whilst the boom gate is down, rising for authorised access only. After hours, the boom arm is constantly raised whilst the swing/sliding gate is closed, only opening for authorised access.

Rising bollards

As their name implies, these are bollards that are fitted into the ground and can be raised and lowered as quickly as boom gates and provide a higher level of security. However, unlike boom gates, they can cause considerable damaged to a vehicle attempting to breach the perimeter. Like boom gates though, rising bollards are easily breached by pedestrians.

Road blockers/rising kerbs

These higher-security variations have a substantial solid frame that rises out of the ground to provide a formidable barrier against vehicle attack. They are not a low-cost option and are intended for use where high-level security is required and where it is imperative to stop unauthorised vehicles entering.

Where space and traffic flow allow, the configuration of the roadway leading to a vehicle access/exit gate can provide an excellent preventive security measure, forcing vehicles to slow down and, thus, deterring the likelihood of a vehicle attempting forced entry or exit.

Pedestrian access

Where possible, separate pedestrian access points should be provided. The type of control required should be based on the level of security and the throughput needed. Separate consideration should be given to the need for any other security controls such as personal or baggage searching.

Turnstiles and pedestrian barriers control people using an access point. They are useful in areas of heavy traffic to ensure an orderly use of the entrance. However, they may reduce the speed of entry/exit at peak times such as shift changes to such an extent that time is wasted.

Technologies such as electronic access control systems may be used in combination with turnstiles and, if programmed suitably, can prevent

- **tailgating** – an individual following another through an access controlled point without authorisation
- **anti-passback** – the prevention of an individual passing the access card back to another to allow them access into a site.

Quality, reliable turnstiles can be costly as can pedestrian barriers. It is recommended that only full-height turnstiles are used to guard against breaches.

Although turnstiles are effective in the prevention of tailgating and management of anti-passback, an individual may still accidentally 'fool' an electronic access control system by badging the turnstile reader but not passing through the turnstile. The access control system will think the individual has entered another area when, in fact, they have not.

Where precise knowledge of individuals' locations is required reader or 'man-trap' turnstiles can prevent this. After badging their access card, the individual enters the turnstile but, instead of making a full turn and guiding the individual to the other side, it only makes a partial turn, 'trapping' the individual in the turnstile. Here another reader must be badged to proceed to the other side and only then will the system update their location. If the reader is not badged, the turnstile returns to its original position and the system recognises and records the individual as remaining in the original area.

Case study – *Pedestrian turnstiles*

A full height turnstile was installed with access control via an electronic identity card so that a security guard was not considered necessary. An assessment highlighted that whilst the full height of the turnstile ensured that nobody could jump over the barrier, the construction of the turnstile provided a 'ladder' that someone could climb to gain access over the top. Fencing and barbed wire was affixed to the top of the turnstile to provide protection to the same standard as the fence line.

Lighting

For obvious reasons, security issues are more likely to occur at night when darkness provides cover and there may be less activity at the facility. Adequate lighting not only acts as a deterrent but allows security patrols to view areas fully. Any lighting used for security purposes must be of sufficient coverage and illumination to allow adequate visibility of the area either to security patrols or CCTV cameras.

Light pollution may be an annoyance to neighbours and the position and angle of lighting towers should ensure that adequate lighting is provided to the required areas but that it does not cast illumination into the sky or onto other areas. Consideration should also be given to the shielding of the light source where its direct view may cause problems to adjacent working areas or traffic.

Motion detection may be suitable for use where lighting is not required for other operations, however, adequate response to the lighting being triggered must be in place but due to the nature of the sensor this may include numerous false triggers eg. animals. Sensors for dust-to-dawn operation to reduce unnecessary electricity useage may be fitted.

Identity management systems (IDMS)

Identity management systems range from a set of simple registers to computer-based software systems that integrate with other systems used by the business giving tools to restrict, record and control activities that are susceptible to fraud or negligence. Additionally, where required by legislation, these systems can provide links to organisations that engage background checks and security clearances.

IDMS may be used for two purposes:

- **Authentication –** confirming that the person is who they say they are
- **Authorisation –** confirming locations, vehicles, systems etc that the person is allowed to access.

For all IDMS consideration must be given to the procedures for both entry and exit and in particular how exits will be operated during an evacuation.

Documented Registers

A simple register system can be adopted whereby details such as name, contact details, access authorities and reference checks can be recorded. In most instances this type of register would be linked to some form of ID card that can be shown to gain access to the facility or restricted area.

Whilst this may be effective in smaller operations where a good level of recognition of employees will be found, for larger organisations this system could easily be abused. This type of system relies totally on the persons operating it and clear procedures and policies need to be in place and followed at all times. Monitoring of the performance of these duties should be carried out to ensure that personnel do not become indifferent or deficient in pass checking or respond to pressure from persons to allow unauthorised access.

For contractors or visitors a register can be used to record their details including name, company, vehicle registration and ID (eg. driver's licence.) Good practice is to ensure advance notice of visitors or contractors is given to the entry personnel to confirm access authority.

Software-based Identity Management Systems (IDMS)

Businesses that experience high traffic of staff, contractors and/or visitors, can streamline identity management processes with a software based IDMS.

An IDMS system should be able to generate a card that can be used as proof of identity to gain access to the facility or restricted areas. This should ideally include a means of physical identity (ie. photo) and enable clear definition of access authorisations/restrictions (eg. colour coding).

Consideration will need to be given to if and how this system will be used for contractors and visitors. Where contractors will be onsite for some time is would usually be appropriate to include them within the IDMS. However, for one-off visitors, it may be more practical and less time consuming to have available specific visitor passes which are issued once details have been taken and identity confirmed (eg. passport, driving licence).

Other features of IDMS that may be useful to an organisation are:

1. The ability to access, cross-reference, and propagate all data records providing a 'single record' among disparate systems referencing employees, contractors, and visitors such as:
   - Payroll
   - Access control
   - Customer Management System
   - Enterprise Resource Planning
     - Vendor Management
     - Human Resources
   - Safety management (inductions, certifications and training)
2. The ability to provide distributed management of records to each supervisor or contract manager
3. The ability to integrate with a visitor management system enabling all visitor history and activity to be linked to the person being visited
4. When compliance to legislation is required, the ability to define workflows that incorporate the required background and police checks into the approval process of personnel

5. Linking to vehicle access control to record such things as use, speed, carbon emissions
6. Linking the physical access control to the safety system can be used to ensure that inductions and competencies are in place before granting access.

Thus, the key advantages of IDMS can be summarised as:

- Single point for data entry and data access for personnel
- Consistency of information on personnel, across the business
- Assurance as to the credentials of staff, contractors and visitors reducing the risk of identity fraud
- Creation of a security aware workplace and culture
- Streamlined processes such as termination whereby a single action can notify payroll and revoke network access, physical access, access to vehicles as well as to other business systems
- A single point of access for personnel information is of great benefit should an emergency occur.

Electronic Access Control System (EACS)

The most effective ways to restrict and monitor access to and around a facility is to install an EACS to electronically lock and unlock portals such as doors, gates, turnstiles or even access to vehicles and computers. EACS provides a variety of options on managing these processes. Each person requiring access may be provided with a unique identifier such as a PIN, a card with encoded-on unique number, a combination of both or alternatively they may be able to use a biometric signature such as their fingerprint or retina scan as the unique identifier. Each unique identifier is programmed into the EACS along with the access restrictions (time, dates & locations of approved access) determined for the person. Every time a person presents the unique identifier at an electronic reader (scanner) the information is sent to the EACS and a determination is made against the assigned access restrictions and the portal is either unlocked granting access or remains locked preventing access.

Basic stand-alone EACS

A basic stand-alone EACS is an improvement to mechanical keys in that unique identifiers can be programmed and de-programmed easily. This is effective when a unique identifier is lost or stolen or a user is no longer employed by the organisation but hasn't returned their non-biometric unique identifier.

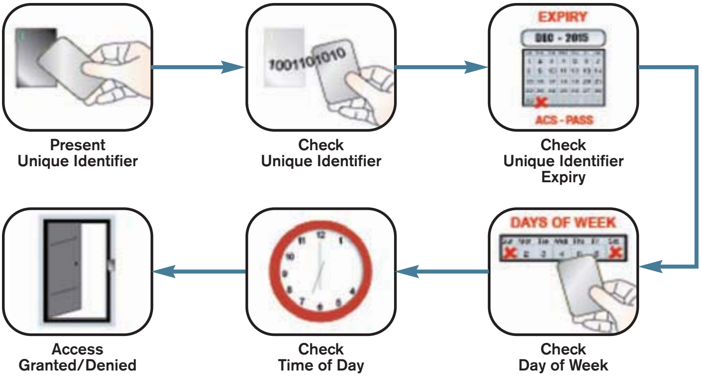
A basic stand-alone EACS, generally, does not allow time restrictions or provide reporting functions. The cost for a basic stand-alone EACS is between US$250 and US$600.

Networked EACS

The next step beyond a basic stand-alone EACS is a networked EACS. A networked EACS links all portals controlled via communications cable back to a central management system software package installed on a computer. A good EACS allows easy administration of cardholder access restrictions for each portal in the system. From the software, reports of system activity can be generated such as who went where and at what time, who is programmed in the system and what restrictions people have.

Networked access control systems cost in the region of US$3,000-4,000 per door plus, approximately, US$1,500-4,000 for entry level software.

Typical EACS workflow (Courtesy ONE Security, Sydney, Australia)



Integrated EACS

An integrated EACS will offer a degree of integration with other systems, such as CCTV, allowing you to link cameras to portals. Each access attempt is recorded to the database along with video of the event. An integrated EACS allows search of stored video by a search key such as the cardholder who entered, the portal, or the camera. Depending on the size of the system, integrated EACS software packages cost US$3,000 - 40,000.

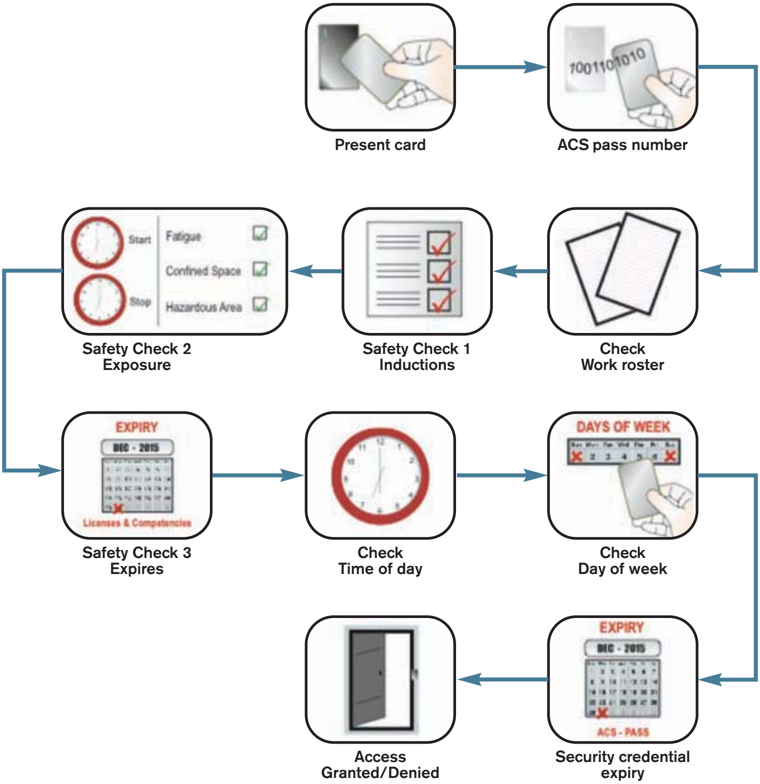
Multi-site integrated EACS

Many organisations have multiple business locations. Rather than installing different systems for each site there are advantages to standardising on a single system. Many of the benefits are the same as for standardising on systems such as Microsoft Word and PowerPoint. The system becomes known by everyone, only one card need be carried, training is reduced, support is standardised and management understands the capabilities of the system. Enterprise-wide access control systems allow security managers to centralise management and reporting functions, providing a useful tool in the monitoring and control of company security policies.

Enterprise Safety & EACS

Enterprise Safety & EACS take access control management to a whole new level. Enterprise Safety & EACS provide managers with tools to define access control parameters around both the site security policy and the safety policy. Managers can define access restrictions around multiple expiries such as competencies, licences, inductions, insurances, contracts, etc. Contractors can even be restricted to site access depending on whether they have received a purchase order from the Finance Department. Enterprise Safety & EACS offer organisations automated compliance with safety rules and regulations by using a gatekeeper system.

Typical Enterprise Safety & EACS automated workflow (Courtesy ONE Security, Sydney, Australia)



Additional benefits and features of Enterprise Safety & EACS

(a) Exposure

Exposure is a very useful feature that allows a pre-determined time limit to be imposed on a person after entering an area. Examples of this feature in use are:

1. Impose a time limit on a person's exposure to hazardous materials. If this time limit is exceeded, text messages or emails can be sent as a warning and if the breach continues the alarms could escalate for investigation
2. Impose a time limit on access to a ship in the harbour. Again, if the time limit is breached alarms can be escalated
3. Impose a time limit on transport drivers between locations

4. Impose a time limit for on site exposure and then impose a set time of rest before site access is permitted again.

(b) Inductions

The inductions feature allows entry of expiry dates for inductions. Some systems give the tools for creating inductions, linking the pass, or fail, to a persons access privilege. Automatic emails and text messages can be sent warning a person and their supervisor that access will be suspended pending a successful outcome of the induction.

(c) Check work roster

This feature allows you to restrict a persons access to a site between roster times allocated. If a person is not rostered on, their access is suspended.

(d) Expiries

The Expiries feature allows linking a person's access permissions to the expiry of their competencies and licences. For example, if an electrician's licence expires his access to the sub-stations and electrical switch rooms can be suspended until the licence is renewed, or if a driver's license is expired his access to the site vehicles is automatically suspended until the licence is renewed. Whilst this functionality may provide a useful tool in ensuring all personnel have the correct licences to carry out their work, policies should be carefully considered to ensure that operations are not impacted

(e) Distributed Management

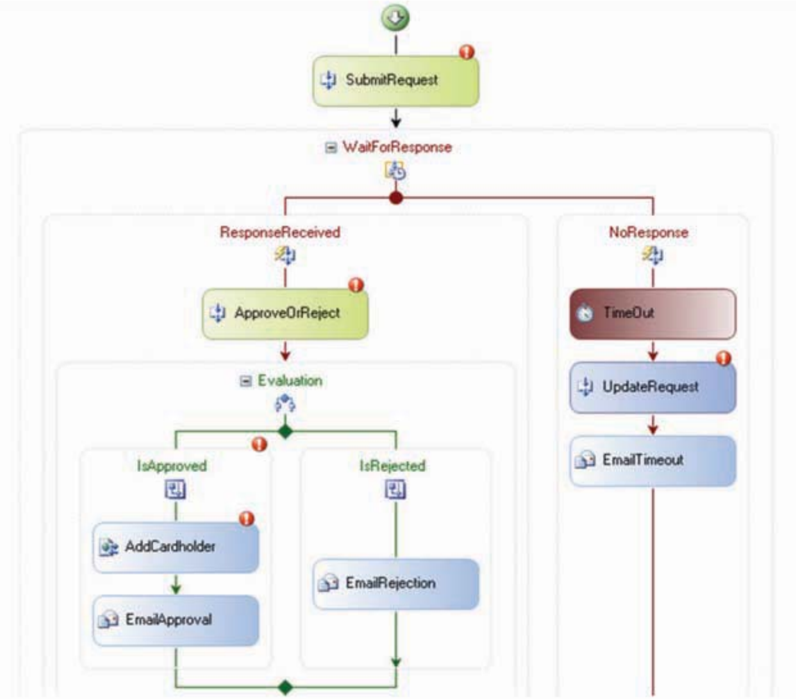
An effective feature set of an EACS is distributed management of administrative duties, via a web page interface, normally assigned to security officers or to a wider range of people, while at the same time protecting information from unauthorised access. Using this method, access can be viewed anywhere on the corporate network, or on the internet if the business chooses to, rather than depending on locally installed software.

Local area managers and supervisors know best when access is required to their area and may be allowed to view and update their own department's information, request access and pre-register visitors. Moreover, external contracting companies may be given access to manage their own contractors, allowing them to register themselves when requesting access to the facility.

(f) Automated Authorisation Workflow

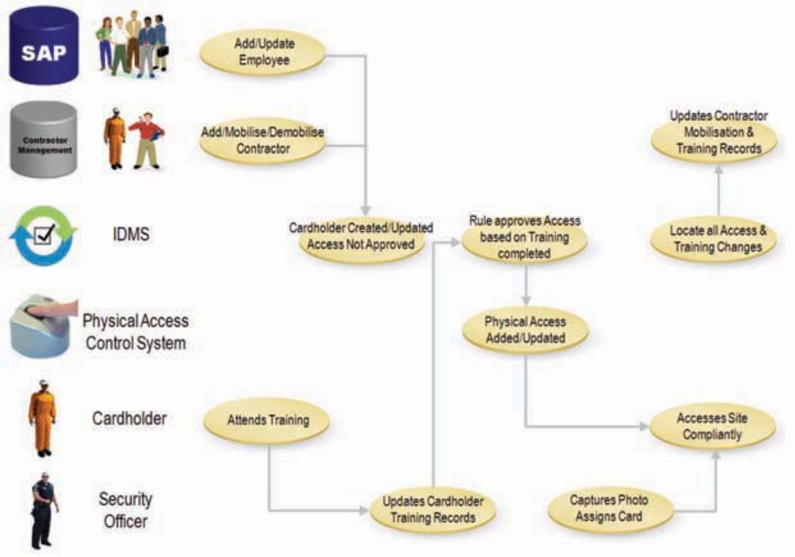
It has been previously suggested to allow local management, employees and contractors to manage and/or request their own access. This can be managed by an authorisation workflow. Although an employee or contractor could request access within the actual EACS, their access would need to be authorised via a workflow process.

Typical automated authorisation workflow
(Courtesy ONE Security, Sydney, Australia)



This could be as simple as an access-level 'owner' clicking on a tick box or a sophisticated chain of events requiring several managers clicking on email links to accept or deny the request along with a criteria of induction processes and compliances to be satisfied. The diagram below demonstrates an automated workflow of a new cardholder obtaining access to their new workplace.

Typical Identity management workflow
(Courtesy ONE Security, Sydney, Australia)


SAP
Contractor Management
IDMS
Physical Access Control System
Cardholder
Security Officer
Add/Update Employee
Add/Mobilise/Demobilise Contractor
Cardholder Created/Updated Access Not Approved
Rule approves Access based on Training completed
Physical Access Added/Updated
Updates Contractor Mobilisation & Training Records
Locate all Access & Training Changes
Attends Training
Updates Cardholder Training Records
Captures Photo Assigns Card
Accesses Site Compliantly

Vehicle Electronic Access Control System (VEACS)

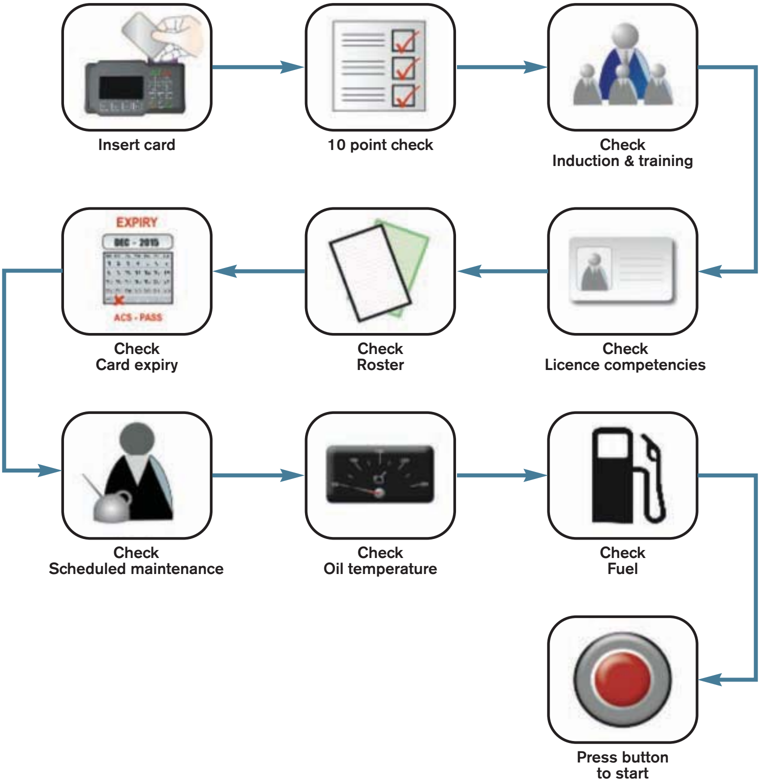
Vehicles such as cars, trucks, forklifts and cranes are valuable assets to an organisation. Maintenance of these assets can be a costly exercise, particularly repairs needed due to damage caused by negligence of the drivers. The driving of these vehicles is generally shared amongst common drivers making accountability for damage difficult. VEACS is a system that can be installed in any vehicle and requires a driver's identity card to be inserted before the vehicle will start and continue to operate. This operation identifies the driver at any given time and which vehicle they were driving. All knocks and crashes are recorded in real time by G-Force shock sensors, identifying the driver and the date/time of the incident, creating accountability for any damage done to the vehicles.

VEACS can also have speed limiters that can be set to record any speeding breaches. Serial offenders can be automatically 'locked out' from having access to a vehicle, forcing them to report to management.

Many countries require a pre-start safety check to be completed before a vehicle can be driven. A VEACS incorporates the procedure during startup, automating the process and saving time. VEACS may also alert the driver of any over temperature or oil pressure alarms, or when maintenance is due.

VEACS can be incorporated into Enterprise Safety and EACS to provide integrated security and safety systems for a site.

Typical vehicle EACS automated workflow
(Courtesy ONE Security, Sydney, Australia)



Key advantages from VEACS

(a) Security

When using VEACS, only licensed authorised drivers can operate the vehicles. If the driver is not licensed, inducted, or has not completed safety checks etc, the vehicle will not start. Due to the driver accountability created, vehicle and asset damage can be minimised and negligence can be identified making it possible to initiate the appropriate action.

(b) Environmental

When using VEACS, a vehicle will only run when the identity card of the driver is inserted in the system. This means that vehicles are not left running for extended periods of time wasting fuel as the identity cards are also required to access buildings on a site. This feature significantly reduces running costs.

Maintenance can be scheduled accurately as the system records the number of actual running hours between services rather than the guesswork that normally occurs with maintaining fork lifts and heavy machinery. This regular maintenance keeps the vehicles operating efficiently.

Automating the pre-start safety checks and scheduled maintenance reduces paperwork.

(c) Safety

VEACS creates driver accountability thus encouraging them to drive responsibly and within the speed limits. Data shows that where VEACS systems are installed a reduction in accidents is seen.

Biometrics

Within the supply chain process biometrics may be used to identify and verify access to specific locations and computer systems as well as confirming the identity of persons delivering or collecting goods.

Biometrics automatically identify or verify an individual, based on either physical or behavioural characteristics, by using computer technology, in a non-invasive way, to match details of individuals, in real time, against stored records.

The most common systems use an individual's physical features such as fingerprint, iris and hand geometry, however other systems exist, such as:

- **Physical:** face, retinal, voice and
- **Behavioural:** characteristics of signing, unique way of walking (gait).

The accuracy of confirming an individual's identity by biometrics is significantly greater than methods such as swipecards, passwords or PINs as it links the event to a specific individual, whereas a password or swipecard may be used by someone other than the authorised user. Unlike swipecards or passwords, biometric identifiers are inextricably linked to a person and, therefore, cannot be forgotten which also proves more convenient for the individual as there is nothing to carry or remember. The counterfeit risk to a biometric identity is also extremely reduced.

Like other electronic access control systems biometrics can provide an audit trail of when and where a person was located and what systems they accessed.

As biometrics are electronic identity verification systems, this removes the human element of access control and eliminates issues such as indifferent or deficient pass checking, pressure to allow entry to persons without the correct pass because of cultural, or hierarchical conflicts.

Since biometrics can accurately identify individuals, companies also gain benefits by relieving security personnel, network managers, and customer service representatives of the tedious and often intrusive task of identity verification and password/PIN administration.

There is no single biometric system that is best for all circumstances. The effectiveness of a system is dependent on how and where it is to be used. An evaluation of the different types of biometric technology should be undertaken in respect to its operational requirements. Consideration should be given to areas such as location and climatic conditions, type of user, expected user traffic, interoperability with existing systems, known maturity and performance of the technology.

Whilst biometric technology has improved considerably and is generally reliable, factors that may affect the end result should be considered in determining which system to use. These may include the user type eg. where work may result in heavily soiled hands fingerprint recognition may be less reliable. The quality of the sensor used for the initial recording of a person's data will correlate to the recognition results.

Like any electronic system used for access control, back-up procedures need to be in place to deal with any denied-access issues and also to manage any system down times.

The following are some advantages and disadvantages of the most common biometric technologies.

Fingerprint - Advantages	Fingerprint - Disadvantages
Fingerprints are unique to each finger and remain permanent during one's lifetime	*Some occupations may cause difficulty wih sensors capturing accurate image ie. dirt*
Easy to use with some training	*Health concerns from touching a sensor used by numerous individuals*
Require little space	*Not easily verified by a human*
Users have multiple fingers	
Have proven effective over many years of use.	

Iris - Advantages	Iris - Disadvantages
No contact required	*More difficult to capture initial data requiring more training*
Iris remains stable over lifetime	*Easily obscured by eyelashes, eyelids etc*
Iris is a protected internal organ which is less prone to injury	*Can't be verified by a human*
	Public fears related to 'scanning' the eye with a light source

Hand Geometry - Advantages	Hand Geometry - Disadvantages
Easy to capture data	*Requires a large amount of space*
Believed to be a highly stable pattern during adult life	*Requires some training*
Not affected by occupations where dirt or similar may be an issue	*Not easily verified by a human*

Monitoring

CCTV is a well-established monitoring technology that is going through rapid technological changes as mainstream consumer cameras are starting to appear that can handle security-specific scenarios using off-the-shelf technology in novel ways. Continuous technological changes drive down the costs of CCTV components and increase the range of new functionality. There are some useful guiding principles to consider in this market:

- Ensure that you do not commit to a technology that will be superseded before its full economic life has expired. Try to ensure that systems conform to standards set by independent standards bodies, rather than individual vendors, otherwise you may find that you have separate security and non-security infrastructures where only one is needed
- Carefully evaluate technical features for practical use - just because a feature is available does not necessarily make it of use in practice
- Understand the objectives of your CCTV installation.

Many countries have laws governing surveillance and recording and a review of the applicable laws should be undertaken prior to installing any monitoring system.

At its simplest, CCTV provides a means of viewing a large area from a single location and recording it for later review. There are two primary objectives of CCTV:

- Spotting intrusion or suspicious behaviour as it happens – Active monitoring
- Providing post-facto supporting evidence to detection, root cause and law enforcement – Passive recording.

Active Monitoring

Active monitoring enhances the observation range of your guard force. Its output is interpreted by the guards who may be a single guard in a lobby watching entrances and exits (Intrusion Point Surveillance) or a team overseeing a large site and access ways using cameras with functionality such as PTZ (Pan/Tilt/Zoom) to steer what the cameras are looking at (Overview Surveillance).

Computer enhancement may enable various types of recognition, from simple scene changes to identifying specific object types in the scene, such as faces. As noted above, careful evaluation of such features is required. It is common for 'scene change alerting' to be turned off by operational staff if there are too many false alarms.

Active monitoring enhances other security measures and policies that are in place ie. active monitoring of an entrance can be used to curtail tailgating, or verify identity in conjunction with access control and identity management; monitoring of hallways and thoroughfares can be used to oversee contractors such as couriers and maintenance crew; intercom augmented portals provide the impression of physical presence regardless of the proximity of the monitoring centre.

Most importantly, Active monitoring is pro-active security. Personnel are constantly scanning for risks and reacting to them.

Passive Recording

Passive recording (or just recording) provides an historical record of all areas under surveillance. While passive recording fails to offer pro-active security it provides valuable information for reconstructing the timeline leading up to events and immediately following them. It can be used to help resolve the root cause of any event and to establish indicators of potential risks that may need to be addressed. It may also be used to provide evidence for detection and law enforcement agencies.

Recording should be retained in as high a quality as possible for a defined period of time.

Key issues relating to monitoring are as follows.

(a) Intrusion Point Surveillance

Intrusion point surveillance covers entries and exits – doors, gates, driveways – as well as closed and open perimeters – jetties and wharfs. Intrusion points may be monitored to detect unauthorised or forced entries, to provide confirmation of an individual/vehicle with its access permissions and to detect any damage to perimeters.

Intrusion surveillance can also be used to monitor areas where access control may not be in place but intrusion could still be an issue ie. loading docks where closed transport containers, truck trailers, and truck cabins come to rest thus allowing concealed intruders an opportunity to alight.

(b) Overview Surveillance

Overview cameras are useful in tracking movement and activity of foot traffic, vehicles and goods. Following an incident, overview surveillance may help to identify the conditions which led up to the event and the subsequent results, thus enabling appropriate corrective action to be taken to reduce the risk in the future.

Case study – *CCTV*

An appropriate CCTV system was installed at a site with dedicated personnel assigned to monitor the images on a 24 hour basis. Whilst the personnel were dedicated to the work and suitable procedures had been put in place for the response to any incident or suspicious circumstances no specific site training had been given. This meant that the monitoring personnel had not been trained to understand 'normal practices' and therefore found it difficult to identify unusual circumstances. Little co-ordination was found between the monitoring staff and security guards. A training package was designed and delivered to provide the CCTV monitoring staff with a full understanding of the operations of the site, active monitoring techniques and co-ordinated operations and drills with the security guards.

Overview surveillance may also be beneficial for business operations when complemented with protocols that provide accountability.

(c) Video Surveillance Technologies

At the core ofVideo Surveillance are cameras, recording devices and displays. In addition, advances in computer systems have created a wealth of analysis tools that can run in real time with live video as well as provide quick access to recorded video.

(i) Cameras

Although the simplest device, inVideo Surveillance, to operate, there is a large variety of cameras, all of which come with numerous options so that selecting the best compilation of features is critical to effective monitoring. For most sites a combination of different types of camera for different monitoring functions would be recommended.

Some examples of the more specialised camera types that may be suitable for use in a supply chain node are:

Pan/Tilt/Zoom (PTZ) allows security personnel to turn a camera to a point of interest and zoom in. They can be programmed to follow pre-determined routes or manually operated. PTZ cameras are also used to provide surveillance over a wide area where multiple static cameras are not cost effective.

PTZs provide key benefits in a supply chain - they can:

1. Follow objects as they move around docks/yards
2. Zoom in to see details such as licence plates, faces or transactions
3. Be triggered by an intrusion detection sensor to track to the alarm location.

PTZ cameras potential shortfalls:

1. High elevation can mask detail or make it easier for items such as hats to obscure faces
2. During or in the lead up to an incident they may be monitoring a different area and no useful recordings will be made
3. Active monitoring is needed to provide more than casual touring of an area.

Wide Dynamic Range is one of the most critical innovations in video surveillance as it allows different parts of a scene to have different light levels and still resolve critical detail.

In practical terms Wide Dynamic Range offers some of the following visibility enhancements:

1. Regions under flood light allow for detailed visibility in directly lit and indirectly lit areas
2. Licence plates are visible at night despite strong headlamps
3. Faces can be made out against bright backgrounds such as portals and windows.

In spite of these great benefits Wide Dynamic Range has some limitations:

1. Low light scenes are not improved
2. Directed intense light sources such as lasers still destroy the image/display
3. Configuration is required to establish the thresholds for the scene.

Day/Night and Infrared Illuminators and Thermal – A substantial portion of criminal activity occurs under cover of darkness and Day/Night or Infrared-Illuminated cameras provide visibility in unlit or poorly lit areas. True Day/Night requires a physical filter that moves in and out of the focal path to compensate for the difference between visible light (day) and infrared (night).

Benefits are:

1. Enhancd visibility in areas with little or no natural light, works well for both indoor and outdoor terrain
2. Spaces can be monitored continuously without the need to use expensive lighting.

Day/Night is not a perfect solution:

1. Infrared illumination is only effective for a few hundred metres
2. Night visibility is limited to black and white
3. Resolving details such as faces is more difficult, if not impossible.

DSS Night Vision has more advanced light sensitivity which requires very minimal light levels and can give a clear, crisp colour picture.

Thermal cameras register differences in heat output from different elements in the scene and display them at different levels of brightness.

Practical benefits include:

1. People, animals and vehicles stand out as bright objects against a neutral background making detection easier
2. Visual impairments such as smoke, fog, sand storms, brush and leaves do not block thermal detection
3. Previously undetectable conditions such as people hiding in containers or undisclosed heat sources stand out clearly
4. Site safety can be improved by detecting the presence of people or vehicles in unauthorised areas.

Thermal cameras are not ideal for all applications:

1. Camera resolution is very low, usually a quarter or half that of standard definition video
2. Backgrounds are indistinct due to low differences in heat level

3. Details such as faces are indistinguishable as heat radiates uniformly from them.

(ii) Video transporting

There are three primary modes for transporting video:

- Analogue – the mainstay of current CCTV systems
- HDcctv – a new entrant that offers high-definition video in an infrastructure similar to Analogue
- IP (Internet Protocol) – network cameras with an origin in consumer webcams.

Analogue cameras represent the bulk of installed cameras worldwide and still enjoy over 90% market share. The benefits outweigh most of the limitations and, as the predominant product, they are available in the widest range of options at the lowest cost.

Benefits include:

1. Connections are point-to-point, making failure identification easy and decreasing the risk of being tapped externally
2. Cameras are plug-and-play, no configuration needs to be performed to transmit video or for a display or recorder to receive it
3. Negligible latency, the delay between what the camera 'sees' and when it can be shown on a display is small enough that PTZ tracking of objects can be easily performed
4. Standards based on NTSC or PAL video, no compatibility issues as the standards come from the broadcast industry.

Limitations include:

1. Uni-directional, cameras are primarily one way, limiting control and configuration to being performed either at the camera or over a separate communication network such as RS-485
2. Fixed resolution, regardless of manufacturer claims NTSC cameras are limited to 480 lines of visible video (with a maximum horizontal width of 720 columns) while PAL cameras are limited to 576 lines of visible video (with only 704 columns)
3. Interlaced, every frame of video is actually made up of two time-shifted fields. Each field covers half of the video frame (alternating odd and even rows). Each field is also time-offset from the previous alternating field by half a frame.

HDcctv is a new technology designed to behave in the same way as an Analogue camera while providing innovations previously limited to IP cameras

Benefits include:

1. Connections are point-to-point, making failure identification easy and decreasing the risk of being tapped externally
2. Plug-and-play, no configuration is required, and interoperability between vendors cameras, displays and recorders is guaranteed by compliance to the HDcctv Alliance specification
3. Negligible latency, the delay between what the camera 'sees' and when it can be shown on a display is small enough that PTZ tracking of objects can be easily performed
4. High definition, video can be captured at 30 frames per second for NTSC, 25 frames per second for PAL at broadcast industry standard 720 progressive lines or 1080 progressive lines
5. Progressive video, every frame uses every line to produce a clear, crisp image at the full resolution.

Limitations include:

1. Limited choice as it is a new technology and products are only being introduced slowly
2. Coax cable lengths are limited to 100 metres (although fibre optic cables do not have this limitation)
3. Recorded video must still be compressed for storage.

IP cameras use a range of methods to transmit compressed video over an IP network. IP cameras are not constrained by the physical topology of the network but rather by the bandwidth at each link in the connection between the camera and the recorder.

Benefits include:

1. Scalable in units of one, to get an additional input only requires adding one more camera and the appropriate software licences
2. Highest Resolution, captures images up to five times larger than HD, although at very low frame rates
3. Shared infrastructure, multiple IP cameras can use the same backbone network to stream data over a large network to a remote location

4. Broad adoption, many software vendors have seasoned products in the market that connect to a wide range of IP cameras.

Limitations include:

1. Cameras and recorders both require IP network configuration to function, this complicates camera maintenance and replacement
2. Devices are susceptible to network attacks, these can re-route video to offsite attackers, disrupt transmission and recording, or display altered video in place of actual footage
3. Incomplete and competing standards, which complicates purchasing and deployment as not all products inter-operate
4. Network delay, while not long enough to allow an event to go undetected, PTZ operation becomes challenging when operators are tracking objects 300 milliseconds delayed on their display
5. Loss of detail in compression, all transmitted video is compressed at the source, high resolution detail in live video is lost in this process and cannot be recovered
6. Shared or second infrastructure, many IT departments believe that IP security can share the same network infrastructure not realising that an IP video load, for even as few as sixteen cameras can fully utilise modern gigabit networks
7. Standards have only recently been proposed with most products continuing to use proprietary protocols for sending video and command and control with the camera.

During the decade to 2010 most IP security development has followed proprietary lines; each major security company has created their own set of video and command and control standards. This has led to significant market turmoil as vendors attempt to lock in security users. Recently two standards have emerged for IP security - ONVIF (Open Network Video Interface Forum) and PSIA (Physical Security Interoperability Alliance). These standards are similar, using web based technologies and a common set of commands to allow device makers to build cameras that can work together in a heterogeneous environment. Whilst best efforts are being made to create products that follow these standards, the industry remains fragmented, relying on software companies to unify different IP cameras in the same site.

(iii) Video Servers

Video Servers are a bridge technology between Analogue and IP surveillance systems. Analogue cameras, video recorders, and video matrices are connected to Video Servers which compress the video and transmit it over the IP network. Video Servers exhibit all of the same strengths and weaknesses of IP Cameras with the key benefit being that existing monitoring assets can be retained rather than replaced.

(iv) Compression

Video surveillance pictures are compressed to allow for storage in a manageable form that can be uncompressed if required. There are different types of compression but the type used in video surveillance produces a copy with noticeable loss of video information when uncompressed. There are ongoing advances in the technology addressing both the compression size and 'readability' but at present a reduction in capacity often results in the loss of capability and usefulness for reviewing purposes.

(v) Recording Devices

There are two types of recording devices for video surveillance:

- Digital Video Recorder (DVR) – compresses incoming video and stores it - typically takes inputs from Analogue, HDcctv, IP Cameras and Video Servers
- Network Video Recorder (NVR) - recorders that only store video - only takes inputs from IP Cameras and Video Servers.

Digital Video Recorder - The Digital Video Recorder (DVR) is a self contained video compression and storage device. In most instances the DVR also possesses a means of reviewing the video on the same unit in Playback.

DVRs may be PC-based running on a general purpose PC, or Embedded/Stand-alone that use special purpose hardware and optimised software to perform only the functions needed.

– **PC-based DVRs**

Benefits include:

1. Most versatile recording option
2. First to market with the newest compression, analytics, and integration to other security systems
3. Easy to maintain and service as the system is made up of off-the-shelf components

4. Can be integrated in the organisation's IT infrastructure for backup, maintenance and monitoring
5. Graphical user interface for simpler operation
6. Hardware configurable for more video, audio or alarm input ports.

Limitations include:

1. Overhead of a full PC and operating system built into the price
2. Weakness to attacks against the operating system, both local and remote
3. Not optimised for multi-channel video recording of high resolution video
4. Lack of front panel controls
5. Subject to departmental 'tug of war' over whether it is a security device or a computer, or whether other non-security software can be installed.

– **Standalone DVRs**

Benefits include:

1. User interface and front panel controls optimised for video playback
2. Dedicated compression with guaranteed minimum levels of performance
3. More efficient chassis design allows more units to be stacked together reducing space requirements
4. Usually cost less than PC-based equivalents
5. Generally less likely to have hardware/software faults
6. Impossible for other departments to 'reuse' or 'share' as there is no host PC.

Limitations include:

1. Configurations tend to be set at the factory; adding channels or changing the compression system is near impossible
2. Storage is limited by the connections provided
3. Adding integration programs is difficult; external Software Development Kits are needed to interact with Stand-alone DVRs on the network
4. Simple network security is provided but devices should never be used on a public network.

Network Video Recorder - A Network Video Recorder (NVR) consists of a network-attached storage server with services for connecting to IP Video devices including IP Cameras and IP Video Servers. They can be PC-based or Embedded/Stand-alone. They are IP based systems and provide tools for managing complex network configurations. Most early NVRs were designed to work only with the IP cameras offered by the same company but industry standards are slowly being adopted.

Benefits include:

1. Inputs scale easily in single units as IP cameras are added
2. Future generation cameras can be recorded alongside older ones
3. Storage is expandable providing flexibility to increase quality or the length that video is retained for
4. Advanced implementations include analytics, location-awareness data, maps, and options to process business rules.

Limitations include:

1. As network devices, any fault or attack on the network can prevent video from being transmitted and recorded
2. Configuration requires Networking skills in addition to security know-how
3. Security networks and IT networks operate completely differently; failure to meet Quality of Service requirements for security translates into missing video footage
4. Viewing video requires a separate PC as most NVRs require all available system bandwidth to record and perform any analysis.

In addition to basic recording, DVRs and NVRs offer security-specific functions such as Alarm Handling, Motion Detection, Data Archiving, and Scheduled Recording. Next generation Recording Devices are capable of a host of Video Analytics, Network Streaming, high reliability RAID Storage, and Video Management. Some of these additional functions are outlined below but, as mentioned previously, careful evaluation of the practical use of such features should be undertaken.

(vi) Alarm Handling

This integrates the Recorder into the sensor-based security topology. Glass-break detectors, door sensors, passive IR, alarm panels and legacy access control can be connected to the recorder or IP camera providing an opportunity to change the recording behaviour in the event of the sensor being tripped. Beyond the basics, Alarm Handling can be used in vehicles when certain operations are performed which are linked to measurable switches such as open and close buttons on loaders or a reverse indicator in a passenger vehicle.

(vii) Motion Detection

Motion Detection extends sensor inputs by looking for changes to the video scene itself. Motion Detection can be triggered by the amount of movement and also the size of the object moving; using these options Motion Detection can be set to ignore small movement, such as by animals, and trigger on large movement such as vehicles.

More advanced versions of motion detection can extract further information from the scene such as the colour and speed of the moving object. This can then be used with business rules to trigger alarms.

(viii) Data Archiving

This allows an operator to make a copy of a portion of the recorded video for use away from the unit. Archives used to be saved primarily to optical disc, but the rapid growth in the size of low-cost flash memory devices has put USB-attached storage as the more common format today.

Access to Data Archiving should be limited as sensitive information could become available if copied by unauthorised parties. More advanced recorders will both limit who can archive video as well as log any video archives that are made. Local laws governing video data should also be taken into account.

(ix) Scheduled Recording

Basic recorders will allow simple day/night, weekday/weekend schedules to be created. More advanced recorders can change the behaviour of nearly any part of the recorder as well as provide a greater number of schedulable times.

With a suitable device Scheduled Recording can be used in conjunction with Motion Detection to record high-quality video during normal operating hours while recording at high-quality during off peak hours only if triggered by motion.

(x) Video analytics

Video analytics have been hailed as the panacea of video security. When Video Analytics are used to compliment a well-supported Active Monitoring Centre the result can be faster detection of dangerous situations and a marked improvement in site safety.

(xi) Object and People Counting

Object counting was originally developed for retailers to count the number of items placed on the counter at a register and verify that the sales tally accounted for the same number. In supply chain security applications, object counting can be used to ensure and bring attention to discrepancies and account between a manifest and palletised cargo in restricted areas such as bonded warehouses.

People counting, like object counting, can be used at entrances and exits to monitor, automatically, for tailgaters without the need for cumbersome turnstiles.

(xii) Object Left/Removed

Elevated cameras can be configured to provide a vital tool in the defence against terrorism and general safety. They check such things as whether vehicles are left in ‘keep clear’ areas. Public areas in buildings can be monitored for unknown packages being left or passageways, such as fire exits, being obstructed. Additionally, yards can be zoned such that security works with logistics to ensure that cargo is not moved before it should be.

(xiii) Facial Recognition and Search

Facial Recognition can be used not only to complement Access Control systems, but also expanded to participate with law enforcement to ensure that individuals passing onto the site are not a threat and that they match their credentials. Facial Search can be used after the fact to review all instances of when an individual passed an entrance, exit or other monitored portal. Facial Recognition can also be used in high-traffic areas to register truck drivers automatically, negating the need for registration clerks.

Container detection and screening equipment

The use of equipment to check the contents of containers has been constantly promoted by the USA as a means of reducing the risk of containers arriving at their land, sea or air borders containing illicit items and both pressure has been put on and assistance given to operators in countries exporting to the USA. In considering the installation of container detection and screening equipment operators should not forget the benefits that may be brought to their operations, the operations of their supply chains and the countries in which they reside.

The equipment used to check containers:

- Non-intrusive inspection (NII) equipment
- Radiation portal monitors (RPMs)
- Radiation isotope identification devices (RIIDs).

NII equipment uses x-rays or gamma-rays to penetrate containers and produce an image of the contents. Officials review images for the presence of anomalies which may indicate contraband, weapons or illicit material in the container.

Containers are driven through a Radiation Portal Monitor where the presence of radiation emissions is detected. The equipment is passive in that it absorbs radiation from the container or its contents as it passes through the portal. The resulting graphic profile of the radiation reading is automatically assessed and the presence of any radioactive material will trigger an alarm. False positive alarms will result from cargo which is naturally radioactive.

The sensitivity of RIIDs is such that they are able to differentiate between the natural radiation emitted from ceramic tiles, granite, cat litter, fertiliser or food products containing potassium eg. bananas and avocados. This is in addition to the capability of detecting weapons, radioactive and nuclear materials. Furthermore, it can detect other radioactive materials which might be used in the construction of a so-called 'dirty bomb.'

For any operator in the supply chain wishing to introduce container detection or screening equipment there are numerous practical considerations that must be resolved. These may include:

- The area required to set up the equipment
  - Whether this will impact on traffic flow
  - Requirements for an additional inspection area for containers that alarm
- Whether the equipment can capture all required containers by being positioned in one area or will multiple or mobile systems be required
  - Multiple entrances
  - Multiple transport types ie. train, truck, barge, ship
- The speed at which the process will need to be conducted so as not to impact on traffic flow
- Resources required to operate the equipment
  - Who will operate it
  - How will positive readings be responded to
  - Will additional or longer movements of containers be required.

Data Exchange Protection

Data are exchanged between many of the parties in the supply chain. The key protection issues are:

- Confidentiality: can the information be seen by unauthorised agents
- Integrity: is the same information as was sent
- Non-repudiation: can the sender prove that the recipient received the information sent.

With paper-based processes, these requirements are usually handled by sealing envelopes, signing for the receipt of documents and keeping local copies, with suitable archive and retrieval processes so that historical records can be reviewed as required.

For supply chain data exchange, data volumes will increase dramatically and most exchanges are likely to occur over public networks. The technologies needed to support the supply chain data exchange protection requirements are well understood and are reasonably simple to implement.

The basic building blocks are already widely deployed and used: all web sites that support secure transactions (eg. for credit card payment) have a 'digital certificate', which uses 'asymmetric encryption' to provide unforgeable information about the site, including the name of the organisation that owns the site and a key that can be used to encrypt data. These data can then only be decrypted by the organisation that owns the site, using a separate key that only that organisation knows. These two keys for an organisation are known as the Public Key (in the digital certificate) and the Private Key (that only the company knows). Digital Certificates are standardised by the ITU-T X.509 standard. In general, these certificates are used for authenticating and exchanging information by many different types of entities, such as individuals, and underpin many enterprise-scale security systems, including Microsoft Active Directory.

The simple concept to understand is that a message encrypted with a Public Key can only be decrypted by the corresponding Private Key and vice versa. Making it straightforward for company A to send a private message to company B by encrypting the original message using company B's Public Key. Company B can then decrypt the message using its Private Key.

This simple regime can be used to address the data exchange protection requirements of supply chains and the complexities can largely be masked from the users in the supporting software. It already underpins internet based replacement for existing supply chain messages that used to be exchanges through VANs (Value Added Networks). However, the details of the exchange mechanisms do need to be worked out between counterparties, even if the supporting software is available 'off the shelf' as part of existing enterprise software.

Annexe 1 – Information Sources

(a) Bibliography

Aaker, D.A. (1996) "Measuring brand equity across products and markets", California Management Review, Vol. 38, No. 3, pp 102-120.

Bichou, K. (2009) "Security and risk-based models in shipping and ports: review and critical analysis" in OECD/ITF Roundtable 144 "Terrorism and international transport: towards risk-based security policy", OECD/ITF Transport Research Centre.

Crutch, M. (2006) "The Benefits of Investing in Global Supply Chain Security", Executive Summary from the November 2006 CVCR Roundtable Meeting, Leigh University Center for Value Chain Research.

First Ondemand Ltd, "Extensible Logistics Identities & Their Role in Meeting 21st Century Compliance Regimes and Delivering Efficiency" (October 2007). A White Paper distributed to members by ICHCA.

Gordon, P., Moore II, J.E. & Richardson, H.W. (2009) "Economic Impact Analysis of Terrorism Events: Recent Methodological Advances and Findings", in OECD/ITF Roundtable 144 "Terrorism and international transport: towards risk-based security policy", OECD/ITF Transport Research Centre.

Hintsa J., Gutiérrez X., Hameri AP., and Wieser P. 2009. "Supply Chain Security Management: an overview." International Journal of Logistics Systems and Management, Vol. 5, Nos. 3/4.

Jones, S (2006) "Maritime Security: A Practical Guide", Nautical Institute.

Lee, H. and Whang, S., "Higher Supply Chain Security with Lower Cost: Lessons from Total Quality Management" (October 19, 2003). Stanford GSB Research Paper No. 1824.

OECD (2003) "Security in Maritime Transport: Risk Factors and Economic Impact", Maritime Transport Committee, Directorate for Science, Technology and Industry.

Peleg-Gillai, B., Bhat, G., Sept, L., (2006) "Innovators in Supply Chain Security: Better Security Drives Business Value", Manufacturing Innovation Series, Stanford University.

Pyzdek, T. (2003) “The Six Sigma Handbook”, McGraw-Hill.

Rice, J. & Spayd, P (2005) “Investing in Supply Chain Security: Collateral Benefits”, Special Report Series, IBM Center for The Business of Government .

Ritter, L., Barrett, J. M. & Wilson R. (2007) “Securing Global Transportation Networks”, McGraw Hill.

Rowbotham, M (2007) “Marine Reporting and Maritime Security”, in Bichou, K., Bell, M.G.H. & Evans, A. “Risk management in port operations, logistics and supply chain security”, 2007, Informa, London.

Sodhi. M. & Sodhi N. (2005) “Six Sigma Pricing”, Harvard Business Review, 2005 May, 83(5):135-42.

Ya Deau, A. & Westley P. (1992) “Terminal Security”, Through Transport Club.

(b) General references

International Ship and Port Facility Security Code (2003),
International Maritime Organisation.

ISO 28000, International Standards Organisation.

ISO 28001, International Standards Organisation.

International Ship and Port Facility Security Code and SOLAS Amendments 2002 (2003), International Maritime Organisation.

(c) Referenced websites

For BASC: http://www.wbasco.org/english/documentos/bascstandards.pdf

For CSI: http://www.cbp.gov/xp/cgov/trade/cargo_security/csi/

For C-TPAT: http://www.cbp.gov/xp/cgov/trade/cargo_security/ctpat/

For EU AEO:
http://ec.europa.eu/taxation_customs/customs/policy_issues/customs_security/index_en.htm#auth_eco

For ISPS Code: http://www.imo.org/

For ISO 28000:
http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=41921

For PIP: http://www.cbsa-asfc.gc.ca/security-securite/pip-pep/menu-eng.html

For Secured Export Partnership:
http://www.customs.govt.nz/exporters/Secure+Exports+Scheme.htm

For TAPA: http://www.tapaonline.org/

For WCO Framework: http://www.wcoomd.org/home.htm

(d) Further reading

Supply Chain Security Guide, Michel Donner & Cornelis Kruk, 2009 (The International Bank for Reconstruction and Development / The World Bank).

Annexe 2 – Flash Guide to Supply Chain Security Initiatives

Initiative Name	Mandatory	Voluntary	Borders & Customs	Supply Chain Security	Location Specific	Business Type Specific	Security / Anti-terrorism
BASC		●	●	●			
CSI		●					●
24 Hour Rule	●		●				●
C-TPAT		●	●	●	●		
EU AEO		●		●			●
ISPS	●			●		●	
PIP		●	●		●		
SEP		●	●		●		●
TAPA		●				●	
WCO		●	●	●			
ISO 28000		●		●			

For further information contact the TT Club at one of its underwriting centres or at any point in the network.

The TT Club underwriting centres

London
Through Transport
Mutual Services (UK) Ltd
90 Fenchurch Street
London EC3M 4ST
United Kingdom

T +44 (0)20 7204 2626
F +44 (0)20 7549 4242
E london@ttclub.com
GMT 0

Hong Kong
Thomas Miller (Hong Kong) Ltd
Suite 1201-1204 Sino Plaza
255 - 257 Gloucester Road
Causeway Bay
Hong Kong

T +852 2832 9301
F +852 2574 5025 & 2574 5062
E hongkong@ttclub.com
GMT +8

New Jersey
Thomas Miller (Americas) Inc
Harborside Financial Center
Plaza Five, Suite 2710
Jersey City, New Jersey 07311
United States of America

T +1 201 557 7300
F +1 201 946 0167
E newjersey@ttclub.com
GMT -5

Singapore
Thomas Miller
(South East Asia) Pte Ltd
61 Robinson Road
#10-02 Robinson Centre
Singapore 068893

T +65 6323 6577
F +65 6323 6277
E singapore@ttclub.com
GMT +8

Sydney
Thomas Miller (Australasia) Pty Ltd
Suite 1001, Level 10
117 York Street
Sydney, NSW 2000
Australia

T +61 2 8262 5800
F +61 2 8262 5858
E sydney@ttclub.com
GMT +9

The TT Club Network

Antwerp
T +32 3 206 9250
F +32 3 206 9259

Auckland
T +64 9 303 1900
F +64 9 308 9204

Barcelona
T +34 93 23 09310
F +34 93 23 09311

Buenos Aires
T +54 11 4311 3407/09
F +54 11 4314 1485

Dubai
T +971 488 101 67
F +971 488 109 55

Durban
T +27 31 368 5050
F +27 31 332 4455

Genoa
T +39 010 83 33301
F +39 010 83 17006

Hamburg
T +49 40 36 98 180
F +49 40 36 98 1819

Moscow
T +7 495 935 8620
F +7 495 981 1529

San Francisco
T +1 415 956 6537
F +1 415 956 0685

Seoul
T +82 2776 4319
F +82 2771 7150

Shanghai
T +86 21 6321 7001
F +86 21 6321 0206

Taipei
T +866 2 2736 2986
F +866 2 2736 2976

Tokyo
T +81 3 5442 5001
F +81 3 5442 5002

Wellington
T +64 4 473 5742
F +64 4 473 5745

£36.00 UK

ISBN 978-1-85330-019-9 (Printed)
ISBN 978-1-85330-019-6 (PDF)

www.ttclub.com