

Guides to International Logistics

The Practitioner's
Definitive Guide

Safety & Security

The Singapore Logistics Association
with
Captain Andre Khir

Straits Times Press

REFERENCE

About the SLA

Established in 1973, the Singapore Logistics Association (SLA) champions the causes of the logistics and freight forwarding industry in Singapore. Its vision is to be a major contributor towards promoting Singapore as a world-class hub while its mission is to promote professionalism and excellence in the logistics industry. The association, in close collaboration and consultation with government agencies, trade organisations, logistics professionals, academia and international organisations, crafted its objects:

- to promote, protect and develop a sound logistics industry;
- to develop, promote and enhance Singapore as a premium regional and international logistics hub with a reputation for reliability, integrity and high standards in logistics practice and management; and
- to represent, protect and promote the general interests of its members.

SLA has a membership of more than 420 companies. These are corporations that are drawn from a wide spectrum of the freight forwarding and logistics fraternity ranging from major global companies to local smaller service providers. Membership is voluntary. Ordinary membership is for Singapore-incorporated companies which are actively engaged in the provision of logistics services for a period of not less than two years. Associate membership is open to incorporated or registered organisations which are actively engaged in the provision of logistics and/or ancillary services.

SLA is one of the five industry associations that has been successfully awarded the Local Enterprise and Association Development (LEAD) funding in 2007. The award was presented at the third LEAD Forum held on 26 September 2007 by Mr Lim Hng Kiang, Minister for Trade and Industry.

For SLA, LEAD also encapsulates the key characteristics of the initiatives: Leadership, Excellence, Advancement and Dynamism. SLA will be implementing 11 projects over the next three years. These projects support the association's four strategic thrusts, namely Industry Branding and Benchmarking; Education and Training; Resource and Competence Development; and Business Facilitation and Development. SLA's initiatives will promote the growth of the logistics industry and help Singapore to maintain its leadership position as a regional logistics hub. SLA will commit a total of \$7 million to these projects.

Under the thrust of Resource and Competence Development, one of the projects identified is adoption of best practices. Through the development and publishing of a set of comprehensive books on best practices in logistics, the association endeavours to help logistics companies upgrade their process capabilities through a cost-effective medium. *The Practitioner's Definitive Guide: Safety & Security* is the second publication to be launched under the LEAD project, following a successful launch of *The Practitioner's Definitive Guide: Warehouse Practices* in November 2008, now available in second edition. These publications add to the association's publication series of *Guides to International Logistics*, namely, *The Practitioner's Definitive Guide: Airfreight Forwarding* (2005) - now available in third edition - and *The Practitioner's Definitive Guide: Seafreight Forwarding* (2006) and *The Practitioner's Definitive Guide: Multimodal Transport* (2006) - both currently available in second edition.

Preface

Within days of the 11 September 2001 terrorist attack, the supply chain of manufacturers – from automobiles to electronic products to textiles – began to experience disruptions in the flow of materials into their assembly plants.

These disruptions were not caused by the attack itself, but rather by governments' response to the attack, such as closing borders, shutting down air traffic, restricting cargo conveyance and evacuating buildings.

Unlike the past when most of the terrorist groups and activities were localised, given these groups' national ideologies and demands, today's terrorism involves sophisticated global groups with educated activists who know exactly what globalisation implies and how to take advantage of its weaknesses. They understand how the economic and financial system of the free world works and are determined to undermine it.

With supply chains being vulnerable to terrorist attacks and security lapses, security has become an increasingly important issue for both the public and private sectors.

The challenges associated with supply chain defence are formidable, particularly in today's environment where numerous entities are involved in cross-organisational and cross-border movements, as a product could change hands multiple times. The number of parties involved in these transactions creates significant challenges, since the defence efforts of one firm can be nullified by the inattention or inadequacy of a single supply chain partner.

This book does not cover workplace safety, but rather the "Safety and Security" of the work place, in the sense of being safe and secure from terrorist threats. Put together by a practitioner with on-the-ground, experience-based knowledge in port facility security, vessel security and commercial maritime transport, this book provides a thorough introduction to the topic of supply chain security and a detailed description of the fundamental application of management strategies, policies, procedures, practical measures and technology to prevent supply chain assets from being a target of terrorism or being used to facilitate it.

As a snapshot for this fifth book in the Singapore Logistics Associations' series of Guides to International Logistics, the following is the gist of each of its 18 chapters.

Chapter 1 gives an introduction to supply chain security and describes the importance of trade and the vulnerability of the supply chain. It highlights the importance of looking at the supply chains in totality, covering the safe and secure packing of a shipment from point of origin to final point of deconsolidation.

Chapter 2 presents a general overview of several different security initiatives around the world. It looks at their compatibility and identifies critical essential security measures that must be put in place.

Chapter 3 provides an introduction to the nature of terrorism, from its early history to the present day, as well as a look at its various definitions. It also includes an overview on how terrorists can be categorised by the way they operate, their origin, motivation, the weapons and tactics they use, and the targets they attack.

Chapter 4 discusses how a terrorist operates and describes methods the private sector can adopt to prevent, deter and respond to terrorism.

Chapter 5 describes the categories of weapons of mass destruction (WMD) that terrorists may seek to acquire and use in a WMD terrorist attack and how these inflict harm on the human body. This chapter also discusses about how the public and private sectors can play a key role in reducing the risks of WMD entering the supply chain.

Chapter 6 covers security systems and their components, and how these components interact to meet the threat of terrorism.

Chapter 7 highlights the need to have policies and procedures in place for managing the risk of staff and visitors exploiting their legitimate access into a facility to obtain the organisation's assets for unauthorised purposes or to sabotage its operations.

Chapter 8 discusses the use of physical security devices – the most commonly thought of security measures – as the first and basic measures in developing a layered defence for protecting assets.

Chapter 9 looks at controlling access to a facility or building interior – a vital part of a facility's security programme.

Chapter 10 focuses on the importance of security education and training programmes. Like the analogy of the weak link in the chain, an organisation's security cannot be

stronger than the weakest day-to-day behaviour of its employees and their individual security responsibilities.

Chapter 11 deals with the typical requirements for documentation processing and procedural security. It also highlights the importance of ensuring that the processing and control of documents are always complete and secure.

Chapter 12 discusses how to safeguard the custody and integrity of cargo as it transits from point of consolidation to point of deconsolidation.

Chapter 13 introduces the fundamental concepts of information and information technology security and outlines the threats against which data and systems must be defended.

Chapter 14 explains the purpose of business partner security and stresses the importance of screening and selecting business partners.

Chapter 15 discusses the role of investigation in an organisation's efforts to protect assets.

Chapter 16 describes a method for conducting a vulnerability and security assessment, and how to use it as a tool for constructing a security management system.

Chapter 17 outlines the methods for responding to bomb incidents and fire and medical emergencies.

Chapter 18 presents management procedures for handling emergencies and discusses contingency planning for business continuity and recovery.

Increased threats of terrorism require heightened awareness of supply chain security. This book serves as a practical guide for those involved in developing and implementing security measures in their premises and supply chain.

Captain Andre Khir

Contents

Chapter One Supply Chain Security 17

- Introduction 17
- International trade 17
- Threat to the supply chain 18
- International regulation 18
- The supply chain 19
- Supply chain security programmes 20
- Basic profile of programmes 20
- Paradigm shift in supply security 21
- Challenges 22
- Supply chain security measures 22
- Conclusion 23

Chapter Two International, National and Industry Security Initiatives 24

- Introduction 24
- International Ship and Port Facility Security (ISPS) Code 24
- Aviation - EU Regulation 2320/2002 26
- Regulated Air Cargo Agent Regime (RCAR) 27
- U.S.: Customs-Trade Partnership against Terrorism (C-TPAT) 28
- Canada: Partners in Protection (PIP) 29
- Free and Secure Trade (FAST) Programme 29
- Sweden: StairSec 30
- New Zealand: Secure Export Partnership (SEP) 30
- Singapore: Secure Trade Partnership 31
- European Union: AEO Customs Programme 32
- World Customs Organisation - Framework of Standards to Secure and Facilitate Global Trade 32
- Container Security Initiative (CSI) 33
- 24-Hour Advance Manifest Rule 34
- Technology Asset Protection Association (TAPA) 35
- Multinationals' implementation of own standards 36
- ISO supply chain security management system standards 37
- Conclusion 38

Chapter Three Nature of Terrorism 40

- Impact 40
- Brief history 41
- Many faces of terrorism 43
- Definitions of terrorism 44
- Motives of terrorist groups 45
- Policing priorities 47
- Conclusion 48

Chapter Four Counterterrorism 49

Introduction 49
Exploitation of the media 50
Kidnap and assassination 50
Suicide attack 51
Vehicle bomb attack 52
Direct action attack 54
Terrorist preparation 55
Antiterrorism versus counterterrorism 56
Counterterrorism in the private sector 57
Conclusion 60

Chapter Five Weapons of Mass Destruction 61

Introduction 61
Material threats 62
Chemical weapons 62
Biological weapons 66
Radiological weapons 72
Nuclear weapons 73
Explosive weapons 74
Summary 75

Chapter Six Security System Design 77

Introduction 77
Security system defined 77
People component 78
Physical safeguards component 79
Process component 80
Testing the security system 81
Design 83
Conclusion 83

Chapter Seven Personnel Security and Pre-Employment Screening 84

Introduction 84
Records of interest 85
Employee authorisation to release information 86
Reference checks 87
Drug and alcohol tests 87
Paper-and-pencil tests 88
Periodic background checks 88
Conclusion 89

Chapter Eight Managing Physical Security 90

Introduction 90
Types of protected assets 91
Defence in depth 92

- Barriers, fences and walls 93
- Barrier protection 96
- Gates and other barrier breaches 98
- Inside the perimeter 100
- Parking 100
- Lighting 101
- Sensors 105
- Intrusion detection systems 109
- Lock and key systems 111
- Inspection 114
- Summary 115

Chapter Nine Managing Access Control 116

- Introduction 116
- Access control system 116
- Doors to sensitive areas 117
- Employee identification card 120
- Access controls for visitors 121
- Control of vehicles 122
- Materials control 123
- Package control 124
- Guard patrols and inspections 125
- Alarms 126
- Closed-circuit television (CCTV) 127
- Conclusion 128

Chapter Ten Security Education and Training Programme 129

- Introduction 129
- Security awareness 129
- Changing mindset 130
- Awareness is local 131
- An ongoing process 131
- Developing a Security Awareness Programme 131
- Security awareness topics 134
- Avoiding apathy 137
- Conclusion 138

Chapter Eleven Documentation Processing and Procedural Security 139

- Introduction 139
- Cargo documents 139
- Advance cargo manifest 143
- Shipping and receiving 145
- Deadlines for receiving and processing documents 147
- Procedural security 147
- Incoming/outgoing cargo and receiving material 149

Secure storage areas 150
Staging empty and loaded container 151
Container pre-loading inspection 151
Container dispatch procedures 152
Container seal storage, issue and control 152
Material and property removal 154
Inventory control 155
Conclusion 155

Chapter Twelve Cargo and Conveyance Security 156

Introduction 156
Container inspection 156
Ensuring container integrity 157
Container seal integrity programme 161
Types of seals 164
Smart container technologies 167
Truck security programme 169
Conclusion 171

Chapter Thirteen Information and Information Technology Security 173

Introduction 173
IT security and Internet security 173
Information security policy 174
About information 175
Sensitive information 176
Computer protection 181
Data protection 183
Password security 184
Internet 185
Intranet 187
Industrial espionage 188
Competitive intelligence 190
Conclusion 192

Chapter Fourteen Business Partner Security 193

Introduction 193
Screening business partners 193
Prohibiting subcontracting 194
Business partner security 194
Reviewing adherence to security guidelines 195
Monitoring business environment 196
Customer screening 197
Conclusion 198

Chapter Fifteen Managing Investigation 199

Introduction 199
Internal theft 199
Fraud 201
Investigation and analysis 204
Physical evidence 207
Evidence collection 207
Conclusion 208

Chapter Sixteen Risk and Vulnerability Assessment 209

Introduction 209
Methodology for security risk assessment and development
of countermeasures 209
Conclusion 220

Chapter Seventeen Incident Management 221

Introduction 221
Bomb incidents 221
Responding to bomb threats 222
How to search 226
Discovery of a suspicious device 228
Letter and parcel bombs 230
Fire emergencies 231
Medical emergencies 236
Cardiopulmonary resuscitation (CPR) 239
Defibrillation 241
Conclusion 242

Chapter Eighteen Emergency Management 243

Introduction 243
Emergency management 243
Contingency planning 244
Emergency response 245
Crisis management 248
Business continuity 250
Business recovery 253
Business resumption 253
Conclusion 254

Abbreviations 255

References 256

Index 259