AUSTRALIAN INSTITUTE OF CRIMINOLOGY

trends & issues

in crime and criminal justice

No. 214

The Detection and Prevention of Cargo Theft

Claire Mayhew

Many companies suffer losses through cargo theft, particularly small businesses, yet it is an area of business crime that receives scant attention. A single truckload of cargo can be worth as much as $3 million. The risk of theft, especially if the goods have a black market value, is very real. Worldwide, the direct cost of cargo theft is estimated at about US$30 billion per year, with indirect costs many times higher.

Cargo theft occurs in freight-forwarding yards, warehouses and during transportation in trucks, as airfreight and on ships. Cargo is particularly vulnerable while in the process of being loaded or unloaded from trucks, or through documentary fraud. For a small business operating on a just-in-time basis, the loss of freight may threaten viability—particularly if insurance cover is inadequate or compensation payments are contested. Further, the illegal sale of stolen cargo undercuts prices in legitimate businesses. This paper provides an overview of cargo theft, and discusses some target-hardening, freight-forwarding and inventory control strategies that can be adopted by smaller organisations to reduce the risks.

Adam Graycar
Director

Cargo theft creates substantial economic losses, however many incidents are not formally reported and media attention is rare. Cargo can be stolen either by employees or by external offenders. The modus operandi can involve hold-ups, theft from freight yards, theft from containers, theft off trucks, or documentary fraud. The cargo can be legitimately in transit, already illegally in the possession of other offenders, or being transported in a way that avoids excise duty or other taxes.

Theft of "hot products" is common (see Clarke 1999, p. 38). "Hot products" are those that are easily disposed of yet retain a high black market value, such as computers, entertainment equipment, name-brand clothing and footwear, perfume, jewellery, cigarettes and prescription drugs (Atkinson 2001; Huska 1998). The resale of "hot product" cargo may be as lucrative as drug dealing but has far fewer risks. For example, a single truckload of cigarettes may be worth up to A$3 million. A container-load of computer hard drives may be worth US$1 million dollars (Badman 2000; Hume 1996, p. 19).

Worldwide, cargo losses have been estimated at US$30 billion a year, and the incidence is probably increasing (Salkin 1999). Organised crime is responsible for nearly half of these losses (RICCS 2000, p. 46). Annual cargo loss estimates for the United States alone range between US$3 billion and $10 billion (Gooley 1999; Salzano & Hartman 1997, p. 40). Indirect costs—such as investigation and insurance payments—can cost between two and five times the direct losses; that is, US$20–60 billion (US General Accounting Office 1980). Road transport is associated with about 87 per cent of the total direct-cost value of lost cargo. Maritime cargo accounts for eight per cent, rail cargo for four per cent and air cargo for one per cent (based on figures cited in DeGeneste & Sullivan 1994, pp. 40–43). In other words, the overwhelming majority of cargo theft occurs in trucking (ICCS 2000, p. 46; Salzano & Hartman 1997).

Because reported cargo thefts can be recorded in several ways, unequivocal data do not exist. For example, in the case cited below, the offender was charged with aggravated robbery, kidnapping,

September 2001

ISSN 0817–8542
ISBN 0 642 24241 0

Australian Institute
of Criminology
GPO Box 2944
Canberra ACT 2601
Australia

Tel: 02 6260 9221
Fax: 02 6260 9201

For a complete list and the full text of the papers in the Trends and Issues in Crime and Criminal Justice series, visit the AIC web site at:

http://www.aic.gov.au

threatening to kill, unlawfully taking a vehicle and theft:

> ...as the driver was getting back in the cab, you jumped in opposite him, put a knife to his side and forced him down onto the floor... you periodically hit the driver with your fist and threatened to stab him...Cigarettes taken were worth over $100,000...The truck owner is a small operator. He was not fully insured and has suffered a significant financial loss. (*R v. Ken Haldane Clarke*, T201/01, High Court of New Zealand, Wellington Registry)

This case also highlights the hardship cargo theft can create for small business owners.

Under-reporting is widespread as freight-forwarders may prefer to protect their supply of customers and fear bad publicity. Many find it cheaper to absorb small losses. The theft of illegal cargo, or cargo upon which duty or GST has been illegitimately avoided, is also highly unlikely to be reported. Further, because much cargo crime remains undiscovered until non-arrival at destination, offenders usually have time to dispose of goods before the loss is discovered. (Most stolen goods are disposed of within 24 hours.) These delays make recovery less likely.

Some insurance companies may only follow through if the loss is significant (Salzano & Hartman 1997). Many small transport operators are not insured at all (MAA 2000, p. 23). Likewise, various links in a chain of cargo transportation will usually avoid any potential legal or financial responsibilities for which they may not be liable (Luck 1992).

For small businesses, the formal reporting of cargo loss may cost more time and effort than the returns warrant. For example, of the five small businesses that reported a cargo-loss crime in a recent survey of 4,315 small businesses (conducted by the Australian Institute of Criminology and the Council of Small Business Organisations of Australia), only one made an insurance claim (unpublished data; for an overview of the survey see Perrone 2000). Yet small business is heavily reliant on cargo transportation. This vulnerability is widespread: 95 per cent of total retail outlets come within the definition of a small business (employing fewer than 20 persons) (ABS 2000).

Cargo in Warehouses and Freight-Forwarding Yards

Transportation is increasingly "door to door" with one company having control over cargo for the entire journey. The now widespread use of containers and "track and trace" systems has helped to reduce petty pilferage but allows for large-scale cargo theft. There is now an increased possibility that a truck with cargo can be stolen in transit, or that cargo can be removed at storage facilities or after transportation.

In contrast to many other business crimes, cargo theft from warehouses frequently occurs during business hours (Small 1998). Large-scale theft at freight-forwarding yards frequently follows collusion between a truck driver and a warehouse employee, with between 80 and 99 per cent of cargo thefts in the United States and Australia involving employees in one way or another (Atkinson 2001; Ackerman 1997; Hume 1996). While lone employees have been historically responsible for most cargo theft, crime syndicates pose an increasing threat (Atkinson 2001).

Cargo is at great risk during loading and unloading. It can be carried off while a driver's attention is diverted, "short orders" can be loaded onto a truck, or loose cargo can be concealed for later removal and illegal selling-on. Cars and trucks being transported are common targets and may be shipped overseas, broken down for parts, or have a counterfeit identity created for them (DeGeneste & Sullivan 1994, p. 37). Cargo can also be stolen using fraudulent papers (Luck 1992). For example:

> A truck driver picks up a shipment of 550 cases of frozen seafood, then heads out on the highway. Later, he pulls into a rest area, sets up a lap-top computer, scanner and printer in the sleeping compartment of the cab, and goes to work. Soon he prints out new shipping papers showing 475 cases. En route to the consignee's warehouse, he makes a brief detour to deliver 75 cases to a "friend". (Gooley 1999, p. 1)

"Double-manifesting" practices in Australia occur when an owner/driver pays a fee to a freight-forwarding agent to obtain a load, and the manifest (and payment) is made out to the agent rather than the owner/driver. Subsequently the owner/driver receives only part of the stated price—which may make transportation uneconomic (MAA 2000, p. 126). Threatened insolvency may contribute to a climate within which cargo crime may be considered.

Because containers are not normally opened during transit, illicit substances and cargo can be secreted in the container shell, concealed within items, placed separately (so the consignee can deny all knowledge), or illegally stowed and removed without the knowledge of legitimate parties (Luck 1992). Before the widespread use of containers, regular counts and re-counts of cargo occurred throughout all stages of transportation. While this process was time-consuming, labour-intensive and very expensive, the time and place of cargo theft and likely perpetrators were usually quickly identifiable and liabilities relatively clear (Luck 1992). Since the use of containers has become widespread, identification of the place of crime and of liability is often uncertain—thousands of kilometres and many weeks may elapse before re-inspection (Luck 1992). As a result:

> ...any question of liability and responsibility would be hazy to say the least and, most importantly, no law enforcement agency would accept that there was evidence of a crime having been committed in their jurisdiction and all would be loathe to accept a report of loss. (Luck 1992, p. 4)

Use of a comprehensive inventory system with a manifest, random auditing of cargo and the supply chain, checks on "return to factory" merchandise with suspected faults, and close scrutiny of seals and schedules should be routine (Dickerson & Tully 1998). Double-checking of seals, serial numbers and any assigned numbers on cargo and vehicle parts is essential. Comprehensive IT systems for inventories will reduce documentary fraud, however computer data protection is essential, for example through use of digital signatures and encryption. Special attention should be paid to cargo from vendors with a poor track record and products susceptible to damage (in such cases a Polaroid camera should be available for immediate recording of any damage) (Bolger 1996).

Complicated loading and unloading procedures increase vulnerability. For example, a 90-minute gap between checking cargo and loading it onto a truck invites crime (Salkin 1999). Hence access to loading areas in freight yards should be restricted. If a number of firms use the freight-forwarding facility, security must be carefully coordinated (Hume 1996). Also important are security guards at gates who do not let trucks out of freight-forwarding yards without full documentation and photographic identification of the driver (Boyer & Cole 1995, p. 106). As Tyska and Fennelly (1983, p. 5) argue:

> Cargo is vulnerable when procedures break down, rules are not followed and errors are made. Sound management is needed to forge the chain that will link together all the parts of an operational security system.

Comprehensive prevention requires target-hardening, procedural and inventory controls.

Target-hardening Security Measures

- Freight storage and forwarding facilities should be secured in fenced grounds with locks fitted to doors, windows and skylights, manhole access restricted, heavy doors placed at all passage points, strong roller shutters on entrances and bollards or crash-proof gates inserted.
- Electronic security systems with infrared sensors should be installed to record all personnel movements. Visual gate systems with optical readers can record truck registration and container numbers, and photograph the driver, the truck and the container.
- Surveillance systems can include closed circuit television and motion-sensitive lighting. Lighting should have "glare" projection across grounds and exterior walls to prevent dark corners or hidden storage racks.
- Seals that are difficult to re-secure after breaking should be fixed on all cargo containers and be regularly checked. E-seals on containers allow "track and trace" and identify where and when a container has been opened. Access to unused seals should be tightly controlled.
- Loose cargo should be securely stacked, tagged and/or sprayed with marks that can be detected under ultraviolet light.
- Containers should be stored with doors facing each other so that cargo is difficult to remove. High value goods in a container can be placed on top of a container stack.
- Expensive cargo should have higher-security protection, such as being placed in mesh cages or safes built into solid-walled vaults, or secured with electronic keys. Vehicles should be fitted with immobilisers.
- Security experts should conduct comprehensive risk vulnerability audits at least twice each year, one of which should be unannounced (Atkinson 2001; Adams 1994).

Tight Freight-forwarding Security Procedures

- Strict controls should restrict access to yard and loading docks through the use of gate passes and driver photographic identification badges.
- The amount of time vehicles are left waiting should be minimised.
- Loading and unloading should be carefully supervised, with no new trucks admitted when docks are congested or when staff are not available.
- Merchandise should never be left on loading docks for long periods of time.
- All employee and contractor vehicles should be parked outside the grounds.
- Empty containers should be stored in a separate area to cargo. Also, imported, exported and domestic cargo should be separated.
- Rubbish containers should be regularly checked as they may be used to remove cargo from the yard.
- When unloading vehicles, checks should be made for "forgotten" cartons, despite the fact that this process may be time-consuming (particularly with courier vehicles which typically have a number of packages with different destinations).
- Visiting drivers should be restricted to marked areas where cold drinking water and toilet facilities are provided (if possible).
- Security should be upgraded during lunchtime and other breaks.
- Outbound vehicles should be randomly allocated to security check unloading. A supervisor should be stationed at the gate at the end of shifts to check all departing staff—including the chief executive officer.
- Undercover professional investigators may occasionally be used to identify security weak spots.
- An anonymous "cargo crime-tip line" can be installed with rewards paid following convictions.
- Staff and contractors should be screened before hiring.
- Organisational policies should state that offenders will be firmly dealt with. Penalties should include termination and prosecution (Luton 1999; Ackerman 1997; Adams 1994; Tyska & Fennelly 1983).

Detailed Cargo Inventory and Movement Trails to Prevent Documentary Fraud

Clear documentation of cargo inventory and movements are essential, with audit trails being readily available. The "golden rule" is a strict separation of three internal financial responsibilities: authorisation of transactions, cash collection or payments, and maintenance of accounting records (Dickerson & Tully 1998; Ernst & Young 1989). Since fraud always involves subterfuge and deception, surprise transaction audits and vehicle searches are warranted (Frank 2001). It is important to remember that once an insider devises a successful system for stealing cargo, losses may remain undetected for a very long time—with "fences" often encouraging offenders to steal more and more (Salkin 1999). Yet if insurers believe they are not liable, investigations may not be initiated and losses will not be covered (Luck 1992).

Additional fraud prevention measures include the following:

- Security procedures in cargo contracts should be clearly specified.
- Cargo with questionable paperwork or any packages that appear tampered with should not be accepted.
- IT security systems can be installed, such as digital signatures and encryption to reduce the risks of documentary fraud.
- Incidents of theft should be subject to immediate in-depth investigation.

- Cargo should be reconciled with documentary records and sign in / sign out dispatch records.
- "Shrinkage" estimates should be tracked to their sources (Ackerman 1997).
- Electronic cargo management systems with computerised stock and accounting procedures can be implemented in larger organisations. For smaller freight businesses, the cost of implementing these systems may take some years to recoup.

To assist with more secure international movement of cargo, the Customs Legislation Amendment and Repeal (International Trade Modernisation) Bill 2000 provides a new Australian legal framework. All users of the new Customs Integrated Cargo System will use a public key system employing encrypted digital certificates that are linked with the Australian Business Number system (Stonebridge 2001). This system should facilitate more secure international business transactions.

Container Security

- Insurance companies may argue that a seal placed by the consignor that is still intact at point of discharge is prima facie evidence that goods have not been tampered with—even if the goods are missing. Thus, seal integrity is crucial. While seals are now usually of a high standard, the system of application and recording can fall short, particularly if seal numbers do not appear on interchange records, the bill of lading or on the manifest.
- It should not be possible for container doors to be opened during transit without it being immediately identifiable. Bolting mechanisms on doors and panel security are also crucial.
- The bill of lading should show the weight of the container, based on original documents. Regular weighing and checking of any discrepancy may quickly highlight losses (Luck 1992).

In-transit Truck Cargo

The overwhelming majority of cargo losses occur during road transport (Salzano & Hartman 1997). In Australia, trucks are used in the movement of most cargo, with 218,816 truck fleets operating as at July 2000 (MAA 2000, p. 32). This industry also employs over 4.5 per cent of the national workforce (MAA 2000, p. 143). However, extensive subcontracting may facilitate cargo theft (Luck 1992). Trucks carrying cargo are vulnerable because they are highly visible, easily identified, may be parked unattended for relatively long periods of time, and they are exceedingly mobile (Gooley 1999).

The theft of cargo from a truck may be pre-planned or opportunistic. The typical gang includes an inside informer who supplies cargo and schedule information, a "spotter" who follows the truck and acts as lookout, a "hands-on" offender who is usually an experienced truck driver, and a "fence" who disposes of the stolen goods quickly (Boyer & Cole 1995, pp. 105–6). The driver may be either a direct participant, an informer, or be bribed to "look the other way". The trucks may be held-up on a highway, goods may be stolen while the driver is having a rest break, or vehicles in inner city areas may be diverted into dead-end streets where the gang can hold-up and pilfer the cargo more easily (DeGeneste & Sullivan 1994, p. 49). A major theft may result in insurance premiums increasing substantially (Hume 1996).

Faxed invoices may contribute to cargo crime as they may be leaked, copied or sold to criminals (Huska 1998). Similarly:

> ...computers have made it easier for insiders to gain access to shipment information, share it with accomplices and create fraudulent documentation. (Gooley 1999, p. 1).

The printing of catalogues and advertising of expected sale goods may alert offenders that a truckload is expected (Hume 1996). The theft of older trucks may be related to insurance fraud when vehicles need replacement or expensive repairs. Boyer and Cole (1995) argue this type of cargo fraud typically results in insurance cheques being used as a down payment on newer vehicles.

There is a range of prevention strategies specifically applicable to truck cargo:

- Departure times can be varied, with schedules kept confidential.
- Use of flat-top trucks should be avoided.
- Schedules can be arranged so that shipments are made without overnight stops.
- Convoy travel can be timetabled whenever a number of company trucks are heading in the same direction.
- Security escorts should be provided for high-risk items.
- Electronic vehicle tracking technology can be placed in cargo to enhance rapid recovery.
- All fleet drivers should be notified of any missing cargo and vehicles so they can keep a "look out" (Badman 2000; Salzano & Hartman 1997).

Rail Cargo

Cargo security must be assured at rail freight yards and during truck–rail interchanges. As with other cargo transfers, site security, seal integrity, checking of documentation, storage of empty containers away from goods, restriction of access, and particular care with high-value items is required. Rail freight can be shipped in convoys, and surveillance enhanced on both rail lines and nearby arterial roads (DeGeneste & Sullivan 1994). Interagency coordination strategies should be routinely established between rail, port and transport authorities. While most cargo carried by rail is very difficult for passengers to access, the rail lines themselves are comparatively unsecured.

Airport Cargo

Violent crimes are rare at airports, although theft of unattended baggage from jet-lagged passengers and of cargo consignments is more common. Nunn (1993) has argued that the bright lighting, abundance of people and high levels of police presence significantly reduce the risk of crime. That is, most airports have "designed out" the potential for crimes against individuals. However, for cargo proceeding through airports there are some security challenges. For example, consignments may be placed on pallets and under tarpaulins in secured yards rather than in security warehouses (Nunn 1993).

While precise estimates are very difficult, the United States Customs Department reported a loss of US$93 million in air cargo

in 1994 (cited in Salzano & Hartman 1997, p. 41). Identification of cargo theft is complicated by:

- miss-shipping and international liaison difficulties;
- overlapping responsibilities between airlines, customs, police and airport security; and
- multiple carrier-handling involving freight-forwarding companies, consignors and consignees.

For example, customs officials may seize cargo that is suspect, but there may be a delay before consignors are aware of this. Conversely, a cargo crime committed in the country of origin may only be noted at the designated arrival point. Further, the Warsaw Convention may limit liability for lost international cargo, and insurance companies may dispute liability if missing goods are liable to customs duty (Nunn 1993).

The majority of airlines have well-developed methods to overcome cargo crime. At some airports, special cargo crime prevention officers are allocated responsibility for a number of freight-handling agents within a designated geographical area (Nunn 1993). Routine prevention strategies include video-recording vehicle number plates, replaying past crime scenarios during staff training, providing rewards for crime detection, conducting regular meetings between police and airport security staff, and storing cargo in secure compounds where only those with correct documentation and photographic identification are admitted (Nunn 1993).

Maritime Cargo

Maritime cargo crime occurs in ports, on vessels at sea, and on offshore platforms. The losses are significant. For example, just one company—the American Institute of Marine Underwriters—reported cargo losses of US$245 million in 1994 (cited in Salzano & Hartman 1997, p. 41). There are four basic types of maritime cargo crime.

1. Thefts from docks and during cargo loading or unloading operations are common. Historically up to 30 per cent of the cargo from some ships landing on Sydney wharves were tampered with (Luck 1992, p. 43) although this proportion has probably decreased substantially. The introduction of containers reduced pilfering, but now the containers themselves are being stolen and sold on the black market, particularly expensive refrigerated ones (Hollingsbee 1999). The majority of containers used in international shipping are registered with the *Bureau International des Containers* (BIC) in Paris which acts as a clearinghouse, collates ownership records and issues a single BIC registry code (DeGeneste & Sullivan 1994, p. 42). Containers are then marked with this code and other identifying information such as a safety compliance mark, technical specifications and weight data.

   Secure controls over access to port facilities are crucial, including cargo-handling areas, docks and terminal buildings. "Model port" guidelines for security and control have been proposed in the United States (see ICCS 2000, pp. 244–7). Security and customs authorities should be aware of all vessel movements, have up-to-date detailed cargo information (destination, consignees, special handling) and be alert to unusual documents because discrepancies may indicate illegal activity (DeGeneste & Sullivan 1994, p. 39). Officers are usually well trained in cargo tracking systems and in the use of technological aids for searching containers (Hollingsbee 1999). Close liaison between port authorities and local police is essential as the handover of illegally acquired cargo may occur outside port authority areas. Shipping companies that have strictly controlled invoicing systems and tight cargo-sealing discipline are likely to have reduced levels of cargo crime (DeGeneste & Sullivan 1994, pp. 46–7).
2. Thefts from in-port vessels typically involve cash and portable high-value goods. Organised crime gangs involved in drug smuggling or illicit arms shipments may also hide items on vessels or in listed cargo that is later stolen (Hollingsbee 1999).
3. Vessels at sea may be hijacked for off-loading of cargo. Cargo-related piracy typically occurs in specific high-risk waters such as South East Asia, the north-east coast of South America and West Africa (DeGeneste & Sullivan 1994, pp. 36, 53). Theft of maritime cargo in South East Asian waters tends to be concentrated in the crowded Malacca and Singapore Straits and the Phillip Channel. While the incidence of cargo piracy appears to be increasing, reporting remains unreliable. The ship itself may be stolen, fictitiously renamed, reregistered and forever lost to its owners—with resultant losses transferred to the insurance company (Ellen 1991). Such vessels are usually known as "phantom" ships. Difficulties for authorities include restricted coverage of the Geneva Convention and the United Nations laws on piracy in *territorial waters* (in contrast to coverage on the *high seas*) (Chalk 1998). Nation state enforcement is also more difficult where there are contested sea boundaries.
4. Document-related cargo fraud may involve sale of non-existent goods, substitution, scuttling for insurance fraud (usually in an area where retrieval is difficult), illegal diversion, or charter fraud where freight fees are pre-paid but no vessel is chartered to forward the cargo. One classic scam is fraudulent sale of "cheap" Nigerian oil cargoes (Chalk 1998).

Even with tight document security, professional offenders may be able to anticipate container contents that are worth stealing because of loading principles that place certain cargo in certain areas of a ship.

Conclusion

Cargo theft occurs across a range of freight-forwarding and storage operations, but the greatest risk is during truck transportation or when vehicles are in the process of being loaded or unloaded. The losses to owners and insurers are large, with worldwide costs estimated to exceed US$30 billion a year. Nevertheless, much cargo theft remains unreported. These cargo theft losses not only affect the victimised transportation companies and their insurers—the illegal sale of stolen cargo also undercuts prices in legitimate businesses. For small businesses with limited stock that operate on a just-in-time basis, non-arrival of ordered goods may result in the loss of a valued

customer and may even threaten continued viability.

Strategies for reducing cargo theft include:

- physical target-hardening security measures in freight-forwarding yards, warehouses and vehicles;
- tight freight-forwarding security procedures that limit access to cargo; and
- detailed cargo inventory and movement trails that allow for rapid auditing and pinpointing of losses.

Security remains an essential part of overall risk management. Hence comprehensive risk vulnerability audits should be regularly conducted.

While the costs of implementing some of the more sophisticated target-hardening security controls suggested in this paper may be too high for some freight-forwarding companies, tight inventory controls are within the reach of most small businesses. Thus cargo losses may be significantly reduced.

Acknowledgment

Funding for this study was received from National Crime Prevention, Commonwealth Attorney-General's Department.

References

Ackerman, K. 1997, "Mysterious disappearances", *Practical Handbook of Warehousing*, fourth edition, Chapman and Hall, New York.

Adams, J. 1994, "Clamping down on warehouse and dock theft", *Security Australia*, vol. 14, no. 10, pp. 34–5.

Atkinson, W. 2001, "How to protect your goods from theft", *Logistics Management and Distribution Report*, no. 3, March; see http://www.manufacturing.net/lm/index.asp?layout=articleWebzine&stt=001&articleid=CA68557&pubdate=03/01/01 (accessed 11 September 2001).

Australian Bureau of Statistics (ABS) 2000, *Retail Industry, Australia, 1998–99*, cat. no. 8622.0, Australian Bureau of Statistics, Canberra.

Badman, R. 2000, "Cargo security in orbit", *Security Australia*, vol. 19, no. 11, p. 5.

Bolger, D. 1996, "Operations management: More receiving tips that boost profits"; see http://furninfo.com/bolger496.html (accessed 11 September 2001).

Boyer, G. & Cole, L. 1995, "Truck, trailer and cargo thefts", *Investigation of Vehicle Thefts*, third edition, Lee Books, Novato, California.

Chalk, P. 1998, "Contemporary maritime piracy in Southeast Asia", *Studies in Conflict and Terrorism*, vol. 21, no. 1, pp. 87–112.

Clarke, R. 1999, *Hot Products: Understanding, Anticipating and Reducing Demand for Stolen Goods*, Police Research Series, no. 112, Home Office, London.

DeGeneste, H. & Sullivan, J. 1994, *Policing Transportation Facilities*, Charles C. Thomas, Illinois.

Dickerson, L. & Tully, G. 1998, "Protecting assets: Preventing employee theft", *The John Liner Review*; see http://www.chubb.com/library/article1.html (accessed 11 September 2001).

Ellen, E. 1991, "Maritime Crime", *International Criminal Police Review*, no. 429, pp. 25–29.

Ernst & Young 1989, *White-Collar Crime: Loss Prevention Through Internal Control*, report prepared for Chubb Group of Insurance Companies; see http://www.chubb.com/library/wcrime.html (accessed 11 September 2001).

Frank, C. 2001, "Knocking out opportunity", *Security Management*, vol. 45, no. 3, pp. 109–12.

Gooley, T. 1999, "Hands off", *Logistics Management and Distribution Report*, no. 2, February; see http://www.manufacturing.net/lm/index.asp?layout=articleWebzine&articleid=CA123245 (accessed 11 September 2001).

Hayes, R. 1991, *Retail Security and Loss Prevention*, Butterworth-Heinemann, Boston.

Hollingsbee, T. 1999, "Policing the Ports", *International Police Review*, March/April, pp. 44–45.

Hume, J. 1996, "Transport security: How to slash your company's losses", *Security Australia*, vol. 16, no. 5, pp. 18–19, 35.

Huska, K. 1998, "Truck hijackings and cargo theft in Mexico", *Issues in Global Crime*, United States Department of State, Bureau of Diplomatic Security, Washington DC, pp. 70–75.

Interagency Commission on Crime and Security (ICCS) 2000, *Report of the Interagency Commission on Crime and Security in US Seaports*, ICCS, United States.

Luck, K. 1992, *Crime and the Container*, ICC International Maritime Bureau, Barking, United Kingdom.

Luton, D. 1999, "Stopping warehouse thieves", *Modern Materials Handling Online*, no. 3, March; see: http://www.manufacturing.net/mmh/index.asp?layout=articleWebzine&articleid=CA120885 (accessed 11 September 2001).

Motor Accidents Authority (MAA) 2000, *Report of Inquiry Into Safety in the Long-Haul Trucking Industry*, Motor Accidents Authority of New South Wales, Sydney.

Nunn, L. 1993, *Crime Investigation in a Commercial Environment—Airports*, Home Office, London.

Perrone, S. 2000, "Crimes against small business in Australia: A preliminary analysis", *Trends and Issues in Crime and Criminal Justice*, no. 184, Australian Institute of Criminology, Canberra.

Salkin, S. 1999, "Safe and secure?", *Warehousing Management*, no. 10, December; see http://www.manufacturing.net/wm/index.asp?layout=articleWebzine&articleid=CA121823 (accessed 12 September 2001).

Salzano, J. & Hartman, S. 1997, "Cargo crime", *Transnational Organized Crime*, vol. 3, no. 1, pp. 39–49.

Small, S. 1998, "Secure Measures", *Warehousing Management*, no. 6, June; see http://www.manufacturing.net/wm/index.asp?layout=articleWebzine&articleid=CA149032 (accessed 12 September 2001).

Stonebridge, J. 2001, "Digital signature: Passport to customs integrated cargo system", *Journal of the Australian Customs Service*, vol. 4, no. 1, pp. 21–22.

Tyska, L. & Fennelly, L.1983, *Controlling Cargo Theft: A Handbook of Transportation Security*, Butterworths, Boston.

US General Accounting Office 1980, *Report by the Comptroller General of the United States: Promotion of Cargo Security Receives Limited Support*, US General Accounting Office, Washington DC.

At the time of writing, Dr Claire Mayhew was a Senior Research Analyst at the Australian Institute of Criminology. She currently works for the Taskforce on Prevention and Management of Violence in the Health Workplace, Centre for Mental Health, New South Wales Department of Health.

General Editor, Trends and Issues in Crime and Criminal Justice series:
Dr Adam Graycar, Director
Australian Institute of Criminology
GPO Box 2944
Canberra ACT 2601 Australia

Note: Trends and Issues in Crime and Criminal Justice are refereed papers.