CONTEXT-SPECIFIC MEASURES OF CCTV EFFECTIVENESS IN THE RETAIL SECTOR

by

Adrian Beck

and

Andrew Willis
Scarman Centre for the Study of Public Order
University of Leicester

Abstract: *This study reports a research project that explored the effectiveness of closed circuit television (CCTV) as a primary crime prevention measure directed against staff and customer theft in the retail clothing sector. It demonstrates the usefulness of a strong before-and-after research design, as well as the benefits of using different measures for different purposes, including loss measured as a percentage of sales, loss by number of units stolen and loss by value. The study also examines whether the costs of CCTV installations are offset by the benefits of reduced loss. It is concluded that robust measures that are "fit for a purpose" allow informed choices to be made about appropriate investment in crime prevention CCTV technology.*

RETAIL CRIME THREATS

The retail sector is one of the largest and most dynamic parts of the United Kingdom's economy (O'Brien and Harris, 1991; Cahill, 1994; Guy, 1994). By the mid-1990s the industry had a turnover of £187 billion, or 14% of the nation's gross domestic product, and it employed 2.4 million persons, or 10% of the British workforce, in some 328,000 retail outlets (Burrows and Speed, 1994; U.K. House of Commons, 1994; Beck and Willis, 1995; Wells and Dryer, 1997).

Growing concern about crime threats to retailing led to the establishment of the Retail Crime Initiative by the British Retail Consortium (BRC). From 1994 there has been an annual report on retail crime and its costs. The survey for the financial year 1995-96 was based on 48,000 U.K. retail outlets with a combined turnover of over one-half of all retail sales (Wells and Dryer, 1997).

The study revealed 5.3 million criminal incidents in the course of a year — the equivalent of 18 offences per outlet. The total annual costs of retail crime were estimated to be £1.9 billion — £1.4 billion sustained as a result of known or suspected criminal incidents, and a further £450 million of expenditure on security hardware and security services. Against annual sales of £187 billion, this was equivalent to 1.13% of total retail turnover. Crime costs amounted to an average loss of £85 from each household in the country.

Customer theft and staff dishonesty dominated retail crime figures. Retailers witnessed, or could quite clearly establish, 5 million instances of customer theft, with 1.6 million offenders apprehended and just over 1 million referred to the police. The gross loss due to customer theft was estimated to be £653 million — £211 million lost due to witnessed incidents and £442 million lost to unwitnessed crimes. The findings are similar to those of a 1993 U.K. Home Office study that identified 5.8 million instances of customer theft, with witnessed incidents accounting for losses of £200 million (Mirrlees-Black and Ross, 1995). The BRC survey also found over 31,000 recorded incidents of staff theft or fraud, involving nearly 20,000 staff of whom 40% were referred to the police. The value of staff theft recorded by stores was £386 million, £39 million derived from witnessed incidents (detected cases) and £347 million attributed to unwitnessed staff thefts (suspected cases).

Findings for the fashion retail sector reflected the broader picture. The BRC survey identified 30,000 outlets with an annual turnover of £19 billion that suffered criminal losses of £128 million, with a further £74 million spent on crime prevention measures. Against annual sales of £19.3 billion, this was equivalent to 1.05% of total clothing retail turnover. Over three-quarters of all losses were attributed to just two offence categories — customer theft at £53 million (41%) and staff theft at £47 million (37%). Earlier retail crime surveys pointed to near-identical findings (Bamfield, 1994; Burrows and Speed, 1994; Forum of Private Business, 1995; Mirrlees-Black and Ross, 1995; Speed et al., 1995), and related studies have also highlighted the extent and costs of retail crime (Ekblom, 1986; U.K. Home Office, 1986;

Ekblom and Simon, 1988; Touche Ross, 1989, 1992; Hibberd and Shapland, 1993; Beck and Willis, 1995).

The data are unequivocal — the criminal threat to the retailer in general, and the fashion retailer in particular, is substantial whether this is measured by the number of incidents or the direct costs of stock loss. There are also consequential costs caused by disruption to trade and taking remedial action, including instituting security measures. All of these costs have to be borne, either by retailers in the form of lowered profits, by the customers in the form of increased prices, or by both. Finally, most of this victimisation remains well outside the purview of the formal authorities; of the 5 million instances of retailer-identified thefts a year only 280,000 offences, or 6% of the total, are recorded as police crime statistics (U.K. Home Office, 1996a; Wells and Dryer, 1997). There is a crime detection deficit, and even when offenders are known, they are not necessarily passed on to the police. These shortfalls suggest that crime prevention initiatives need to be directed at the point where crimes are committed (individual stores) and focused on the problems of customer theft and staff dishonesty. It is at this point that CCTV commends itself as a suitable mechanism.

GROWTH OF CCTV

There is evidence that rising retail crime threats are increasingly being met by the installation and use of security surveillance equipment. All the indicators point towards substantial and continuing growth in the CCTV market. Surveillance cameras are now found in a "bewildering variety* of settings (Honess and Charman, 1992) and are seen as a common feature of public life. In a three-year period from 1994, government has provided £35 million for 350 CCTV installations, mostly in town centres (U.K. Home Office, 1996b). Beck and Willis (1995) estimate that over £300 million a year is spent on video surveillance equipment, with around 300,000 security cameras being sold, and that more than a million may be in use. More specifically, thc rctail sector accounts for thc largcst proportion of capital cxpenditure with over one-third of the total spend (36%), followed by the industrial sector (31%), the commercial sector (17%) and the public sector (16%).

The BRC survey confirms the prominent position of CCTV in the retail environment (Wells and Dryer, 1997). Total crime prevention costs in 1995-96 amounted to £450 million, of which £74 million or 16% was CCTV-related — £54 million capital expenditure on CCTV installations and £20 million on equipment maintenance and monitoring. Earlier sweeps of the survey showed even higher levels of spending — £133 million in 1993-94 and £119 million in 1994-95. In the three-year period from 1993-94 to 1995-96, a total of £326 million was spent on security surveillance in the retail sector. The prominent position of CCTV in retail crime prevention was confirmed by U.K. Home Office research (Mirrlees-Black and Ross, 1995). CCTV was found to be present in 20% of all retail outlets and 36% of the larger outlets; its installation being positively correlated with previous victimisation and a known crime problem. It is clearly being used as a principal weapon in the fight against shop crime.

This enthusiasm for CCTV is buttressed by a number of recurring themes (Beck and Willis, 1995). CCTV supposedly offers a technological equivalent to extensive police or security surveillance, a case of the officer on the beat or security guard being replaced by an omnipresent, near-infallible robot eye in the sky on duty 24 hours a day. It offers day-and-night surveillance, with an unparalleled capacity to deter or to detect the offender. Electronic surveillance promises comprehensive crime control in a neat, high-technology package — an off-the-shelf, state-of-the-art, electronic panacea for crime. There is a seductive appeal to what might be called the "high-tech fix." There is a danger, however, that commitment to (and expenditure on) CCTV, in both the public and private sectors, may be more a matter of "security wish fulfillment" than a judgement based on hard evidence and a reasoned assessment of its effectiveness. CCTV may be receiving a vote of confidence primarily because everyone wants to believe in its effectiveness rather than because its effectiveness has been demonstrated. It may be easier and more convenient to show blind faith in its supposed capabilities than to assess properly its contribution to crime control. To some extent the "hunches' that inform decisions to install CCTV systems are largely a product of a needs-led belief that there is (at long last) a techno-fix solution that guarantees real-life, crime control benefits, but this is far from an evidence-led assessment of its contribution to crime prevention.

In its strongest form, an uncritical belief in CCTV's effectiveness could operate so as to preclude any formal assessment of its merits; and efficacy becomes a presumption that follows from installation. Equally, there can be technical reasons why CCTV remains under-researched or poorly researched (Ekblom and Pease, 1995; Tilley, 1997). Finally, Beck and Willis (1995) have pointed to a raft of unanswered questions about its impact in relation to: the detection of offenders; the deterrence of would-be offenders; the contribution to crime control of displacing criminal activities elsewhere; the relative usefulness of video recordings and real-time images; the ability of operators to monitor and make sense of multiple images; the impact on customers (who may be reassured even when there are no measurable benefits); and the effect on shop staff (who may become less vigilant about crime following its installation). These point to the need for high-quality data, which is seen to be in short supply (Edwards and Tilley, 1994).

Tilley (1997) goes rather further by suggesting that the question "Does CCTV work?" is not susceptible to any consistent answer either because of technically weak evaluations or because different systems will have differential impacts, which implies that the question itself is not "sensible, useful or intelligible" (p. 179). This is too pessimistic, however, because the author promptly proceeds to offer a new approach, called realistic evaluation, that seeks to establish what works for whom and in what circumstances, where CCTV's effectiveness is seen as a "range of outcomes...generated through mechanisms triggered in context" (Tilley, 1997:183; see also Pawson and Tilley, 1994, 1997). What is really being asserted here is the need to establish how CCTV works in defined settings so as to produce particular outcomes.

These reasonable precepts can be applied to the evaluation of CCTV in the fashion retail sector, where outcomes or measures of effectiveness can be understood as the product of the deployment of CCTV in a specific context (fashion stores) for a particular purpose. The critical variable is the purpose for which CCTV is installed, and there are major differences here between the interests of the academic researcher and those of the retailer. The former may wish to explore subtle differences between CCTV's impact on detection or its deterrent effect, or its effect on customer confidence and the fear of crime. The latter has a more straightforward agenda — namely, the effect of CCTV on the store's ability to make money; under normal circumstances the "bottom line" is the "bottom line." This may be none too elegant but it reflects commercial realities. It is a solid enough imperative from the retailer's point of view, and it gives the researcher a clear enough agenda for evaluation, especially with the use of an experimental design.

The research question focuses, therefore, on whether CCTV is fit for the purpose of reducing loss to the point where its costs are more than offset by a reduction of loss due to its deployment. Again, this stands in contrast to Tillcy's (1997) suggcstion that thcrc will "rarcly if ever be sufficient data to assess the full costs and benefits that can be directly attributable to CCTV" (p. 182), but this is to misunderstand the realities of business life. Where the prospect of maximising financial advantage is threatened by crime (stock loss caused by customer theft or staff theft) it is an absolute business imperative — and a straightforward empirical question — as to whether the costs of installing CCTV can be compensated for by reduced stock loss equal to (or greater than) the crime prevention initiative. This is an everyday commercial calculation of the same order as, for example, whether an investment in product advertisement generates additional sales over and above the costs of the publicity.

METHODOLOGY

The aim of the project was to measure the impact of different types of CCTV systems on levels of loss, including its performance over time, and to assess whether its costs were more than compensated for by crime control benefits. The project was carried out in 15 stores operated by a large U.K. fashion retailer with over 180 branches nationwide. All the stores were located in similar retailing environments. Three different types of CCTV systems were installed, each with varying degrees of sophistication. Three stores had a high-level system with between two and four pan, tilt and zoom colour cameras; between eight and 12 static colour cameras; public monitors positioned at all customer entrances; the facility to record; and security staff monitoring the system at all times. The average cost of installing a high-level system was £24,000. Six stores had a medium-level system with between six and 12 static colour cameras, public monitors at each customer entrance, the facility to record, but with monitoring carried out by the store manager from his or her office when time permitted. The average cost of installing a medium level system was £14,000. The remaining six stores had a low-level system with up to 12 dummy cameras, public monitors at all entrances but no facility to record. The average cost of installing a low-level system was £4,000. The terms high-level, medium-level and low-level are used below to refer to stores with these systems. Members of staff in all the stores were given training on how to use the system prior to the research, and all the equipment was in full working order throughout the study period.

The research used a before-and-after experimental design. Prior to the installation of CCTV, a stocktake was carried out in each of the stores to measure the amount lost as a percentage of sales, the number of units stolen and their value. This process was repeated 13 weeks after installation (3 months) and then again after 28 weeks (6 months). Whilst every effort was made to keep strict control over the way in which the stocktakes were carried out, the project had to rely upon the staff within the stores to perform the data collection process. Although the stocktake assessment of loss is an incomplete and imperfect indicator because it fails to discriminate between stock loss due to customer theft and staff theft, as well as failing to distinguish non-criminal, accidental shrinkage of product, it is the method of first choice throughout the retail sector. Although it could be argued that this approach needs refining, it is difficult to see how loss could be assessed other than by some means of checking stock held against stock sold.

EFFECTIVENESS OF CCTV

The primary mechanism for measuring loss is to calculate the value of goods lost expressed as a percentage of all goods sold, in this case before the installation of CCTV and then at a point some three and six months later (Table 1). Within three months of the installation of CCTV, the figures for loss to sales went down from 2.45% to 1.97% for all stores, with a reduction from 1.96% to 1.62% per cent in high-level stores, from 2.53% to 2.03% in medium-level stores, and from 3.08% to 2.38% in low-level stores. The percentage change in stock loss reduction over this three-month period was greatest for stores with low-level CCTV installations (23%), followed by those with medium-level systems (20%) and then those with a high-level specification (17%). The installation of CCTV had a dramatic effect on the levels of stock loss, showing an immediate improvement of 20% overall, with marginally greater improvements in low-level compared with high-level stores.

Findings from the second stocktake, six months after CCTV installation, were much more mixed. Using adjusted figures because only 10 stores completed the experiment in full, the figures for loss to sales over six months remained unchanged at 2.25% for all stores, with an increase from 1.96% to 2.70% in high-level stores, a reduction from 2.40% to 1.97% in medium-level stores, and a reduction from 2.63% to 1.93% in low-level stores.

The percentage change in stock loss reduction over the six-month period was greatest for stores with low-level CCTV installations (27%) followed by those with medium-level systems (18%), suggesting that the initial improvement was being maintained at or above the rates achieved after the three-month stocktake. In contrast, there was a substantial increase in the stock loss to sales figure over the six-month period for stores with high-level CCTV installations (38%). This had the effect of wiping out the initial impact of CCTV across all stores, and the overall percentage of loss to sales figure returned to the pre-installation level.

Table 1: Stock Loss to Sales Before and After CCTV Installation by Type of System

Type of system	Percent stock loss to sales				Percent stock loss reduction from installation	
	Pre-CCTV†	After 3 months	Pre-CCTV††	After 6 months	After 3 months	After 6 months
High	1.96	1.62	1.96	2.70	17.3	37.8
Medium	2.53	2.03	2.40	1.97	19.8	17.9
Low	3.08	2.38	2.63	1.93	22.7	26.6
All	2.45	1.97	2.25	2.25	19.6	0.0

† Base figure derived from 15 stores with complete stocktake.

†† Adjusted base figure derived from 10 stores with complete stocktake and 2 stores with partial stocktake.

Whilst the percentage of loss to sales is the usual way of measuring the rate of loss in retailing, another (widely used) option is to compare the number of units stolen, together with their value, before and after installation. Table 2 presents data covering the three-month experimental period, and Table 3 presents findings obtained over the six-month experimental period, in both cases using the average losses over a one-week period.

Within three months of the installation of CCTV the average number of units lost had fallen from 72 to 52 for all stores — with a reduction from 166 to 100 units in high-level stores, from 54 to 45 units in medium-level stores, and from 44 to 35 units in low-level stores. The corresponding figures for loss by value showed an overall reduction from £900 to £650 for all stores — with a reduction from £2,075 to £1,250 in high-level stores, from £675 to £562 in medium-level stores, and from £550 to £438 in low-level stores. The installation of CCTV had a dramatic effect on the level of stock loss, which was lowered by 28% for all stores — with a reduction of 40% in high-level stores, 17% in medium-level stores and 20% in low-level stores.

Table 2: Average Number and Value of Stock Units Lost Per Week Before CCTV Installation and After Three Months by Type of System

Type of System	Pre-CCTV		After 3 months		Percentage reduction in loss
	Average number lost	Average value lost (£)†	Average number lost	Average value lost (£)†	
High	166	2,075	100	1,250	39.8
Medium	54	675	45	562	16.7
Low	44	550	35	438	20.4
All	72	900	52	650	27.7

†Following company procedures, the value of loss is calculated on the basis of £12.50 per unit lost.

Table 3: Average Number and Value of Stock Units Lost Per Week Before CCTV Installation and After Six Months by Type of System

Type of system	Pre-CCTV		After 6 months		Percent reduction in loss
	Average number lost	Average value lost (£)††	Average number lost	Average value lost (£)††	
High	123	1,538	91	1,138	26.0
Medium	44	550	58	725	31.8
Low	44	550	48	600	9.1
All	64	800	63	788	1.6

†Adjusted base figure derived from 9 stores with complete stocktake and 3 stores with partial stocktake.

††Following company procedures, the value of loss is calculated on the basis of £12.50 per unit lost.

Within six months of the installation of CCTV, the average number of units lost had fallen from 64 to just 63 for all stores — with a reduction from 123 to 91 units in high-level stores, together with a rise from 44 to 58 units in medium-level stores and a rise from 44 to 48 units in low-level stores. The corresponding figures for loss by value showed only a marginal reduction, from £800 to £788 for all stores — with a marked reduction from £1,538 to £1,138 in high-level stores, together with an increase from £550 to £725 in medium-level stores and an increase from £550 to £600 in low-level stores. The short-term impact of CCTV on the overall level of stock loss had all but disappeared, with a reduction of a little more than 1% for all stores. However, high-level stores showed an impressive reduction of 26%, whilst there was an increase of 32% in medium-level stores and an increase of 9% in low-level stores.

The decision to install CCTV in part reflects a commercial judgement about whether it offers value for the money, in this case, a calculation about the expected payback period or the time it would take to recover the cost of the equipment based upon the savings made in the amount that would have been lost to theft. Table 4 summarizes the data on the average weekly reduction in loss compared with the rate prior to installation, the cost of installing the equipment in the experimental stores, and the number of weeks required to pay back the initial cost of installation.

Table 4: Average Weekly Reduction in Stock Loss, Cost of CCTV Installation and Estimated PayBack Period by Type of System

Type of System	Average weekly reduction per store (£)		Cost of installation (£'000)	Estimated payback period (Years)	
	After 3 months	After 6 months		After 3 months	After 6 months
High	371	178	24	1.2	2.6
Medium	52	nil	14	5.2	Never
Low	53	nil	4	1.5	Never
All	116	4	12	2.0	57.6

Three months after the installation of CCTV the average weekly reduction in loss for all stores was £116, which, given average capital expenditure of £12,000 per CCTV system, would mean that it would take two years (103 weeks) to recoup the capital costs of its installation. There was considerable variation in the payback period for the different types of systems. For high-level systems with an average weekly reduction in loss of £371 set against a capital expenditure of

£24,000, the payback period was just over one year (65 weeks). For medium-level systems with an average weekly reduction in loss of only £52 sct against capital cxpcnditurc of £14,000, thc payback pcriod was just over five years (269 weeks), Finally, for low-level systems with an average weekly reduction in loss of just £53 set against a capital expenditure of £4,000, the payback period was one and one-half years (75 weeks).

Like the other measures of loss outlined above, the impact of CCTV was reduced significantly by the time of the second stocktake. Six months after installation the average weekly reduction in loss for all stores was a near-insignificant £4, which, given average capital expenditure of £12,000 per CCTV system, would mean that it would take 58 years to recoup the capital costs of its installation. There was considerable variation in the payback period for the different types of systems. For high-level systems with an average weekly reduction in loss of £178 set against a capital expenditure of £24,000, the payback period was now 2.6 years (135 weeks). For medium and low-level systems, however, the payback period was nonexistent; it could not be calculated because the average weekly reduction in loss had disappeared altogether.

DISCUSSION

The pre-CCTV loss to sales figure of 2.45% was rather larger than that found in the 1995-96 BRC retail crime survey of 1.13% for the whole sector and 1.05% for the clothing sector (Wells and Dryer, 1997), but high-fashion stores may well be more at risk than other outlets. The change in the loss to sales figures over three months (from 2.45% to 1.97% for all stores) represented a 20% reduction in loss, although the low base rate makes extravagant claims about percentage change somewhat suspect. This initial success was maintained in low-level (27%) and medium-level (18%) stores, but high-level stores witnessed a 38% increase in the loss to sales figures over six months.

The corresponding three-month figures for losses by number were impressive, with the average number of units stolen in a week down from 72 to 52, together with a reduction by value from £900 to £650 — a decrease of 28% overall. The six-month figures for losses by number were altogether less impressive, with the average number of units stolen in a week barely changing from 64 to 63, together with a marginal reduction by value from £800 to £788 — a decrease of rather more than 1% overall. Within these figures there was contincalculating the criminal odds, does not reflect the reality of offending behaviour. The concept of the "reasoning criminal" (Cornish and Clarke, 1986) can, however, be reconstituted in terms of a weaker form of rationality — something often referred to as "bounded rationality" or "limited rationality" (Newman, 1997; Opp, 1997). This approach recognises the complexity of factors (social, environmental and cognitive) that influence and shape behaviour. In the retail context, it is likely that the "decision" to offend or not is the product of an interaction between an overall setting that actively encourages criminal behaviour and features within it that act as disincentives to crime (see Wortley, 1997). The retail environment can be seen as a near-perfect example of a crime-encouraging situation, where ease of access to highly desirable product is deliberately engineered — a form of structured enticement, preferably to shop but possibly to steal. Against this, CCTV can be seen as a crime-discouraging behavioural prompt — a visible cue or reminder that "guardianship" is actively present. Although it is unlikely that would-be offenders constantly calculate the likely rewards of crime against its costs, it is highly plausible that CCTV (cameras, monitors and signage) acts as an occasional situational prompt that encourages rationality in coming to a decision about whether or not to commit crime.

The second major observation is that the effectiveness of CCTV had largely disappeared by the six-month point. Using the figures for the number of units lost and their value, although high-level stores showed a decrease in loss (26%) this was wiped out overall because of an increased loss in medium-level (32%) and low-level (9%) stores. In contrast, the figures for loss expressed as a percentage of sales showed an increase for high-level stores (38%), with decreases for medium-level (18%) and low-level (27%) stores. Although the data do not offer a consistent picture, it is worth exploring the possible reasons for success and failure. The explanation for continuing success (decreased loss) is straightforward: would-be offenders are inhibited by the potential that CCTV poses for increased detection, thereby securing a deterrent effect. The explanation for success not being sustained (decreased loss giving way to increased loss) is more problematic, but a likely mechanism is that would-be offenders become progressively inured or desensitised to CCTV's deterrent potential.

It is well-established that CCTV operators can be subject to so-called video blindness, wherein they fail to take in information from a number of screens in a way that allows them to analyse and react to images that give grounds for concern (Broadbent, 1958; Edwards and Tilley, 1994: Beck and Willis, 1995). It is equally possible that newly installed CCTV systems command the attention and respect of would-be offenders (with deterrent impact), but that familiarity over time leads to the equipment becoming a taken-for-granted, routinised part of the retail environment (with diminished deterrent impact). This is consistent with the "bounded" or "limited" perspective on rational choice in offending behaviour (see Newman et al., 1997) where long-term exposure to rationality-enhancing and crime-discouraging environmental prompts (such as CCTV) can lead to inhibition satiation — a case of over-familiarity breeding contempt. This is reflected by the data on loss by number of units and value (see Table 3), where there was continuing effectiveness for high-level systems, which had security staff monitoring the equipment at all times, and diminishing effectiveness for both medium-level systems with occasional monitoring and low-level systems with dummy cameras.

To the extent that the lack of long-term effectiveness is a product of familiarity over time leading to a reduction in deterrence, the crime prevention implications would appear to centre on giving CCTV a high profile and then on maintaining it. Just as retailers routinely redesign the shopping environment in the interests of keeping the honest shopper attracted to product, the security manager may need to consider a similar approach to CCTV in the interests of reminding potential offenders of the in-store security system. At a minimum, this would suggest that CCTV signage should be changed regularly, but it could also include moving the cameras and monitors themselves, or even taking them out and replacing them with new equipment. In each case, the emphasis would be on highlighting the presence of security hardware — and its operators — in order to maximise its deterrent effect. Pawson and Tilley (1997) refer to this as emphasising the "publicity" mechanism associated with CCTV.

Diminishing effectiveness over time could also be a product of an uncritical acceptance of the crime-control attributes of CCTV by in-store sales and security personnel, leading to a relaxation in staff vigilance. Staff may presume that CCTV is making a major contribution to the detection or deterrence of offenders, perhaps in the mistaken belief that it offers a technological panacea for the problem of crime. If they believe that security hardware is a primary factor in crime prevention, this could result in an overreliance on an impersonal, high-tech approach to security. There is some danger that staff could see themselves as being absolved from security responsibilities. As the authors have argued previously, CCTV may be "a double-edged sword where any crime control benefits need to be set against the possible costs of lower levels of staff vigilance" (Beck and Willis, 1995:190). A Home Office guide is also alert to the possibility of CCTV inadvertently producing an "exaggerated sense of security" (Edwards and Tilley, 1994:15). There is a possibility that the introduction of CCTV may cause feelings of security to go up but in the process cause staff feelings of responsibility for crime prevention to go down; a scenario with obvious implications for staff training. The ways in which the impact of security equipment is mediated by the person-centred activities of sales and security staff is a relatively under-explored area.

There is a interesting irony that where the introduction of CCTV can cause store staff to "switch off leading to a reduction in security, its use may reassure members of the shopping public even where there are no measurable security advantages. There is some strength in the point that it does not matter a great deal whether CCTV is genuinely effective or whether members of the public merely believe that it offers real crime control benefits, even though this belief may be mistaken and unfounded. In one recent study, more than nine in ten members of the public held the view that surveillance cameras in the shopping environment were acceptable — 91% in town centres and 96% in shopping centres (Beck and Willis, 1995; see also Honess and Charman, 1992). The ever-present cameras were seen as a symbolic and reassuring affirmation that crime was under control, something that would have the consequence of alleviating fear and anxiety about possible victimisation (which is good in itself) but also operating so as to encourage customers to part with their money (which is good for the retailer). Paradoxically, the security manager may want to play down the effectiveness of CCTV to the store staff in the interests of promoting their vigilance, but emphasise (or even exaggerate) its effectiveness so far as the shopping public is concerned in the interests of promoting a safe and secure shopping environment. The "reassurance" factor should not be underestimated because promoting customer confidence could be seen as a sufficient justification for its installation, irrespective of genuine crime control benefits.

The third major observation relates to the way in which expenditure on CCTV installations can be set against the benefits of average weekly reductions in losses due to theft. Although Tilley (1997) is sceptical about the feasibility of an authoritative cost benefit analysis, on the grounds that there are so many potential variables to consider, it is possible — using the retailers' emphasis on the "bottom line" — to offer a robust and meaningful measure. Retailers argue that there is only one key consideration: whether or not the expenditure on security equipment is more than compensated for by savings attributable to reductions in loss due to crime. The relevant data are unequivocal: taking the six-month review as the longer-term (and stronger) measure, the payback period for a £24K high-level CCTV system is 65 weeks, whereas because there is no measurable impact on loss for a £14K medium-level and a £4K low-level system, there is no prospect of these installations ever paying for themselves. Moreover, these figures represent the most optimistic payback scenarios because they include only the capital costs of CCTV installation and not the recurrent costs of manning the systems.

The hard-nosed retail manager will begin by wanting to know whether a given investment in CCTV will drive down the losses caused by crime, within a certain time frame, to a point that covers the expenditure on it. This is not only legitimate it is an inescapable feature of commercial life. Even where investment in CCTV cannot be justificd in terms of a strict cost-bencfit analysis, it could still bc justified by wider social considerations such as reducing the fear of crime, or by sales and marketing considerations that use it to promote customers' perceptions of a safe and secure shopping environment. This is especially important because research shows that frightened customers who are concerned about crime and nuisance threats to safe shopping will relocate their shopping activities to locations deemed to be safe and secure rather than remain at those that are perceived to be intimidating and unsafe (Beck and Willis, 1995). Even here, the bottom-line analysis of costs against benefits is still crucial: it allows the company to be clear about the grounds for its decision making by articulating a reasoned departure from the bottom line of cost effectiveness.

CONCLUSION

A realistic and feasible evaluation of the impact of CCTV in the retail environment will need to move away from exploratory analysis (Ekblom, 1988) and focus on specific situational variables (Burrows and Speed, 1996) so as to indicate which context-specific mechanisms produce particular outcomes (Pawson and Tilley, 1997; Tilley, 1997). The study confirms that loss to sales figures, the number of units lost and their value all work as robust and "good enough" indicators of the likely impact of CCTV on theft. These may be imperfect but they are easy to collect routinely and they do reflect the private sector's emphasis on profit. The findings indicate that the most likely mechanism is that of deterrence, which is consistent with understanding crime either as the product of opportunity or as a function of rational choice. There is some evidence that the deterrent impact of CCTV diminishes over time, a fact that directs attention to the "publicity" given to it. But there is also a possibility that store staff become less security-conscious when the cameras are turned on. Finally, the cost-benefit analysis indicates that high-level systems alone "pay for themselves" in terms of reduced loss, which covers capital expenditure, although it is possible (and legitimate) to install CCTV for other reasons. The deployment of CCTV in the retail environment has measurable effects with particular explanations, which allows for more informed decision making about its future use and its contribution to crime prevention.

Address correspondence to: Adrian Beck, Scarman Centre for the Study of Public Order, University of Leicester, 154 Upper New Walk, Leicester LEI 7QA, United Kingdom. E-mail: <bna@le.ac.uk>

REFERENCES

Bamfield, J. (1994). *National Survey of Retail Theft and Security 1994.* Northampton, UK: School of Business, Nene College.

Beck, A. and A. Willis (1995/. *Crime and Security: Managing the Risk to Safe Shopping.* Leicester, UK: Perpetuity Press.

Broadbent, D. (1958). *Perception and Communication.* London, UK: Pergamon Press.

Burrows, J. and M. Speed (1994). *Retail Crime Costs 1992/93 Survey.* London, UK: British Retail Consortium.

——(1996). "Crime Analysis: Lessons from the Retail Sector." *Security Journal* 7(1): 53-60.

Cahill, M. (1994). *The New Social Policy.* Oxford, UK: Basil Blackwell.

Clarke, R.V.G. (1980). "Situational Crime Prevention: Theory and Practice." In: J. Muncie, E. McLaughlin and M. Langan (eds.), *Criminological Perspectives: A Reader.* London, UK: Sage.

Cornish, D. and R.V.G. Clarke (eds.) (1986). *The Reasoning Criminal.* New York, NY: Springer Verlag.

Edwards, P. and N. Tilley (1994). *Closed Circuit Television: Looking Out For You.* London, UK: Home Office.

Ekblom, P. (1986). *The Prevention of Shop Theft: An Approach Through Crime Analysis.* (Crime Prevention Unit Series Paper, #5.) London, UK: Home Office.

——and K. Pease (1995). "Evaluating Crime Prevention," In: M. Tonry and D. Farrington (eds.), *Building a Safer Society,* (Crime and Justice, vol. 19.) Chicago, IL: University of Chicago Press.

——and F. Simon (1988). *Crime Prevention and Racial Harassment in Asian-Run Small Shops: The Scope for Prevention.* (Crime Prevention Unit Series Paper, #15.) London, UK: Home Office.

Felson, M. (1994). *Crime and Everyday Life.* Thousand Oaks, CA.: Pine Forge.

——(1996). "Preventing Retail Theft: An Application of Environmental Criminology." *Security Journal* 7(1):71-75.

Forum of Private Business (1995). *Crime and Small Business.* Knutsford, UK: Forum of Private Business.

Guy, C. (1994). *The Retail Development Process.* London, UK: Routledge.

Hibberd, M. and J. Shapland (1993). *Violent Crime in Small Shops.* London, UK: Police Foundation.

Honess, T. and E. Charman (1992). *Closed Circuit Television in Public Places: Its Acceptability and Perceived Effectiveness.* (Crime Prevention Unit Series Paper, #35.) London, UK: Home Office.

Hough, M., R.V.G. Clarke and P. Mayhew (1980). "Introduction." In: R.V.G. Clarke and P. Mayhew (eds.), *Designing Out Crime.* London, UK: Her Majesty's Stationery Office.

Lab, J. (1997). *Crime Prevention Approaches, Practices and Evaluations.* Cincinnati, OH: Anderson.

Mirrlees-Black, C and A. Ross (1995). *Crime Against Retail and Manufacturing Premises: Findings from the 1994 Commercial Victimisation Survey.* (Home Office Research Study, #146.) London, UK: Home Office.

Newman, G. (1997). "Introduction: Towards a Theory of Situational Crime Prevention." In: G. Newman, R. Clarke and S. Shoham (eds.), *Rational Choice and Situational Crime Prevention.* Aldershot, UK: Ashgate Dartmouth.

——R. Clarke and S. Shoham (eds.) (1997). *Rational Choice and Situational Crime Prevention.* Aldershot, UK: Ashgate Dartmouth.

O'Brien, L. and F. Harris (1991). *Retailing: Shopping, Space, Society.* London, UK: David Fulton.

Opp, K. (1997). "Limited Rationality and Crime." In: G. Newman, R. Clarke and S. Shoham (eds.), *Rational Choice and Situational Crime Prevention.* Aldershot, UK: Ashgate Dartmouth.

Pawson, R. and N. Tilley (1994). "What Works in Evaluation Research." *British Journal of Criminology* 34(2):291-306.

——(1997). *Realistic Evaluation.* London, UK: Sage.

Poyner, B. (1983). *Design Against Crime: Beyond Defensible Space.* London, UK: Butterworths.

Speed, M., J. Burrows and J. Bamfield (1995). *Retail Crime Costs 1993/94 Survey: The Impact of Crime and the Retail Response.* London, UK: British Retail Consortium.

Tilley, N. (1993). *Understanding Car Parks, Crime and CCTV.* (Crime Prevention Unit Paper, #42.) London, UK: Home Office.

——(1997). "Whys and Wherefores in Evaluating the Effectiveness of CCTV.* *International Journal of Risk, Security and Crime Prevention* 2(3): 175-186.

Touche Ross (1989). *Survey into Retail Shrinkage and Other Stock Losses.* London, UK: author.

——(1992). *Retail Shrinkage and Other Stock Losses: Results of the Second Retail Survey.* London, UK: author.

U.K. Home Office (1986). *Standing Conference on Crime Prevention Report of the Working Group on Shop Theft.* London, UK: author.

——(1996a). *Home Office Statistical Bulletin Issue 18/96, Notifiable Offences England and Wales, July 1995 to June 1996.* London, UK: author.

——(1996b). *Further Funding for CCTV, Home Office Press Release No. 258/96.* London, UK: author.

U.K. House of Commons (1994). *Environment Committee, Session 1993-94, Fourth Report, Shopping Centres and Their Future. Vol. I, Report.* London, UK: Her Majesty's Stationery Office.

Wells, C. and A. Dryer (1997). *Retail Crime Costs 1995/96 Survey.* London, UK: British Retail Consortium.

Wilson, *J.Q.* (1975). *Thinking About Crime.* New York, NY: Basic Books.

Wortley, R. (1997). "Reconsidering the Role of Opportunity in Situational Crime Prevention." In: G. Newman, R. Clarke and S. Shoham (eds.), *Rational Choice and Situational Crime Prevention.* Aldershot, UK: Ashgate Dartmouth.

Data, Information and Knowledge Quality in Retail Security Decision Making

Simone Stumpf
(University College London, United Kingdom
S.Stumpf@cs.ucl.ac.uk)

Janet McDonnell
(University College London, United Kingdom
J.McDonnell@cs.ucl.ac.uk)

Abstract: Knowledge creation and organisational learning are as much about questioning assumptions as they are about harnessing what is already known. We describe a procedure for expressing knowledge, theorising from it, identifying data suitable for testing theories, and the value to a business of the outcomes it produces. This technique, called 'theorise-inquire', supports the validation of knowledge once it is expressed in a shareable form and draws attention to gaps in data and to information quality generally. We illustrate the ideas presented with examples drawn from work with profit protection specialists working in large retail organisations in the UK.

Keywords: knowledge quality, data gaps, repertory grids, data analysis
Categories: H.1, H.2, H.4

1 Introduction

Knowledge management, organizational learning and knowledge creation are as much about questioning assumptions as they are about harnessing what is already known. Experts may present a skewed view of reality based on their experience and prejudices, whilst available data may be not useful in questioning experience. We describe a technique, the 'theorise-inquire' technique, which supports specialists in their business decision making. The technique comprises the identification of interesting conjectures from repertory grids elicited from domain experts [Kelly 55], associating these with appropriate data sources against which they can be tested, identification of data gaps and finally the assessment of the conjectures to suggest a course of action. The technique supports business decision making by supporting the comparison of personal experience with factual data, thus putting businesses in a position to consider organisational knowledge in a broader context.

This work is taking place as part of a project concerned with the capture, representation and sharing of knowledge about dealing with the problems of theft by employees in retail organisations. Theft by employees is not well understood considering the size of the problem. In the UK nearly a third of all retail crime losses can be traced back to theft by someone internal to the company [British Retail Consortium 00]. To make decisions about prediction, counteraction and prevention of crime, businesses need to take into account the complex, uncertain and changing nature of staff theft [Felson and Clarke 98]. Improvements in knowledge management can help companies to address issues of loss prevention by providing greater efficiency in processing information using existing knowledge, and by supporting the creation of new knowledge to adapt to a changing environment [Nonaka 94]. Our work deals with retail experts whose focus is on profit protection. They have to operate in an environment that is tuned to processes optimised for customer service and not for important support functions, and this creates a difficult challenge for them.

The aim of our work is to start by making experts' knowledge explicit, and then to use this knowledge to steer data analysis to support individual and organizational learning [Argyris and Schön 96]. It could be argued that knowledge should drive what data is collected, whilst data supports the confirmation of knowledge. On the other hand, [Alavi and Leidner 01] argue that knowledge is "personalised information"; tacit knowledge only becomes information if it is expressed in a processed form that can be shared. Taking these two perspectives together, knowledge management systems should allow individuals to process information to gain knowledge whilst at the same time to express their personal knowledge explicitly in a sharable form. We exploit the routes from knowledge to data and from data to knowledge. Repertory grids and associated "maps of expertise" function as a means to personalise information for an expert and to socialise knowledge in an organisation. The theorise-inquire technique supports the identification of data gaps and the validation of knowledge assumptions.

2 Data Gaps

Poor data quality leads to poor decision making [Redman 98]. Data gaps are often understood solely in terms of inaccurate or incomplete data. [Strong et al. 97] have extended this notion by formulating dimensions of data quality that range over intrinsic, accessibility, contextual and representational issues. Here we give examples of how data gaps and data quality issues cause difficulties in loss prevention, an essential but nevertheless marginalised role in the retail sector. Profit protection managers need to access a variety of data sources to inform their decision making. An investigation into the working processes of eight major UK retailers highlighted that the use of Electronic Point of Sales (EPOS) data presents a number of problems to the security support function. We have found that EPOS data often cannot be accessed at all by specialist decision makers; in other cases, security specialists are overwhelmed by the amount of data – some of it irrelevant – which needs to be retrieved and manipulated (a contextual problem). EPOS data needs to be processed, filtered and reorganised to be of any value as information that is understandable to profit protection managers (a representational problem). This has led to the proliferation of exception reports which filter and aggregate EPOS transactions. Even when they are readily available we find that exception reports themselves need further data associated with them to give sufficient context to inform investigations. As part of an investigation, information about employees needs to be linked to EPOS data, the way that employees are represented differs in these systems; this is a representational problem concerned with consistency.

Decision making about profit protection is not adequately served by data gathered to underpin the (customer-focussed) core functions of the business; thus, organisational security work proceeds in a setting which is not even "data rich, information poor". Support functions routinely lose out in the trade-offs during the design of corporate databases; the data gaps are gaps by design. If we focus on supporting business activities with data we need to add to the data quality issues identified by [Strong et al.] a pre-requisite category to deal with whether data is available at all (an existence dimension) and whether it is in a form that is suitable for automated processing (a digitisation dimension). For example, profit protection managers make use of the knowledge that a fraudulent refund often occurs within a short timeframe of the original sale with which it is associated; in many EPOS databases the link between refund and sale is not captured in the data recorded about till interactions. They also use hand-written records as an important source of clues; these hand-writing clues are not available from electronically recorded data.

Specialist business support units do capture supplementary data to assist their particular data needs. Loss prevention units are no exception; these data resources need to be carefully designed, integrated and maintained to overcome data quality issues like those we have described. A business case has to be made for every extra demand for data collection and management. A major outcome of the theorise-inquire technique, which we describe next, is the identification of data previously overlooked by specialists or the organisation as a whole which may be an important resource for managing security functions.

3 The Theorise-inquire Technique

The 'theorise-inquire' technique proceeds through 4 stages [see Fig. 1]. First, tacit expert knowledge is made explicit – and therefore sharable – through the use of repertory grids as a conversational device. We provide means for organising and analysing repertory grids to derive information on potentially interesting features which allows business specialists to express, explore, clarify and refine their understanding of these features whilst using their wealth of tacit experience to decide what is interesting or what could make an impact on a business process; these are expressed as theories. Features involved in the theories are then associated with appropriate data, either by providing a mapping to data sources or identifying data gaps that need to be addressed. Finally, knowledge is tested by applying data analysis techniques to factual data and comparing the result with experts' theories.

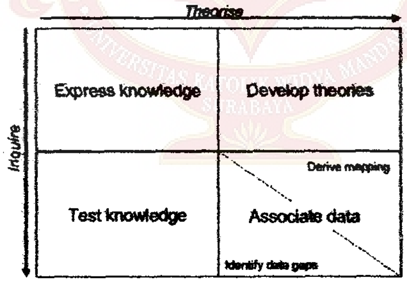
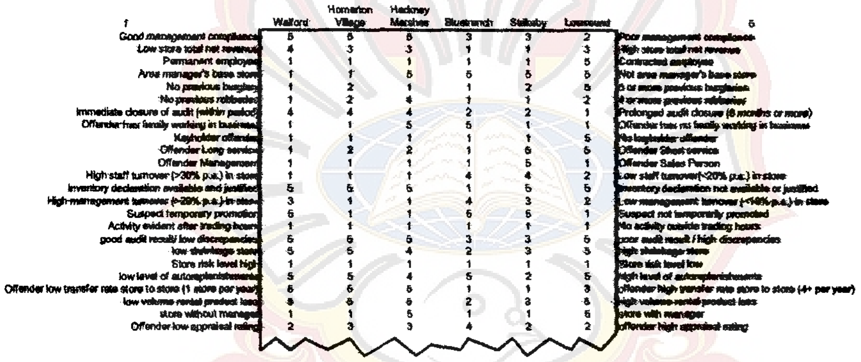


Figure 1: The theorise-inquire technique

3.1 Expressing Knowledge

We capture knowledge about stereotypical situations in very small data sets. To develop these data sets, we make use of the repertory grid technique. The repertory grid technique has been used extensively as a knowledge acquisition tool in expert systems [Boose 88] [Gaines and Shaw 93a] [Gaines and Shaw 93b]; we therefore do not describe it in any detail here. The technique functions as a conversational tool to make tacit expertise explicit and therefore amenable to inspection by knowledge users. As the technique is applied, individual situations that the expert has experienced (elements) are compared to draw out distinctions (constructs) between them. Distinctions are expressed as dimensions of contrasting poles. Each element is rated as to its location between the poles of each construct; ratings appear in the cells of the grid. Whilst distinctions are usually expressed as scalar dimensions, a rating can include binary, continuous and categorical data types [Boose 88].

An extract of a repertory grid for stock theft is given in [Fig. 2]. Elements, in this example cases of stock theft by employees, are shown in columns whereas construct poles are shown to the left and right of the matrix. In [Fig. 2] we use a five-point scale for all constructs for simplicity. A rating of 1 is associated with the construct pole on the left, a rating of 5 with the construct pole on the right.



1	Walford	Homerton Village	Hackney Marshes	Bluestrand	Stillsby	Lovesound	5
Good management compliance	5	5	5	3	3	2	Poor management compliance
Low store total net revenue	4	3	3	1	1	3	High store total net revenue
Permanent employee	1	1	1	1	1	5	Contracted employee
Area manager's base store	1	1	5	5	5	5	Not area manager's base store
No previous burglary	1	2	1	1	2	5	5 or more previous burglaries
No previous robberies	1	2	4	1	1	2	4 or more previous robberies
Immediate closure of audit (within period)	4	4	4	2	2	1	Prolonged audit closure (6 months or more)
Offender has family working in business	1	1	5	5	1	1	Offender has no family working in business
Keyholder offender	1	1	1	1	1	5	No keyholder offender
Offender Long service	1	2	2	1	5	5	Offender Short service
Offender Management	1	1	1	1	5	1	Offender Sales Person
High staff turnover (>30% p.a.) in store	1	1	1	4	4	2	Low staff turnover(<20% p.a.) in store
Inventory declaration available and justified	5	5	5	1	5	5	Inventory declaration not available or justified
High management turnover (>20% p.a.) in store	3	1	1	4	3	2	Low management turnover (<10% p.a.) in store
Suspect temporary promotion	5	1	1	5	5	1	Suspect not temporarily promoted
Activity evident after trading hours	1	1	1	1	1	1	No activity outside trading hours
good audit result/ low discrepancies	5	5	5	3	3	5	poor audit result / high discrepancies
low shrinkage store	5	5	4	2	3	5	High shrinkage store
Store risk level high	1	1	1	1	1	1	Store risk level low
low level of autoreplenishments	5	5	4	5	2	5	High level of autoreplenishments
Offender low transfer rate store to store (1 move per year)	5	5	5	1	1	3	Offender high transfer rate store to store (4+ per year)
low volume rental product loss	5	5	5	2	3	5	High volume rental product loss
store without manager	1	1	5	1	1	5	store with manager
Offender low appraisal rating	2	3	3	4	2	2	Offender high appraisal rating

Figure 2: Example repertory grid

We have helped each retailer to develop repertory grids containing staff theft knowledge for different sorts of offence, e.g. refund fraud, theft of stock, etc. Initial sessions typically extracted repertory grids that contained between 6 and 10 cases of theft or fraud as elements and between 20 and 55 characteristics of these cases as constructs. Follow-on sessions refined the grids until security experts were satisfied; the final grids usually included more cases and fewer characteristics than those produced at initial sessions.

3.2 Developing Theories

Expertise expressed in a repertory grid functions as a tool to think with by encouraging reflection on knowledge. Explicit knowledge can be manipulated, reorganised and analysed to allow the expert to learn new insights about their domain and develop theories. To develop a theory experts inspect the grid and identify constructs and relationships that they believe to be important or interesting. Experts can use analysis techniques to develop "maps" that reflect their theories about some aspects of their domain. The results of analyses are particularly interesting to specialists when they surprise them by challenging preconceived views or by providing new information. Grids can be treated as small data sets, where constructs can be viewed as attributes and elements as records. In principle, many data analysis techniques can be directed at grid data. Commonly used techniques for analysing grids to produce 'maps of knowledge' include decision trees or rules [Gaines 89], hierarchical clustering [Shaw 80] and principal components analysis [Slater 76].

Since we are interested in identifying data gaps and steering analysis of data sources like EPOS data and personnel records we have extended the range of analyses that are available to experts [Stumpf and McDonnell 02a]. For example, we have developed analysis techniques that are based on contrasts between elements, constructs and construct ratings, such as group contrasts [Stumpf and McDonnell 03]; these help profit protection managers in developing theories. Group contrasts are an analysis technique that allows an expert to explore and interpret repertory grids interactively to find significant contrasting relationships between attributes and test these against data sources.

Several of our retailers have developed the theory that employees that have responsibility for keeping store keys are much more likely to be involved in stock theft as a result of work on producing their repertory grids. To a casual reader of the grid in [Fig. 2] this may seem obvious, to the retail companies themselves this is new and important information that was previously hidden amongst the interaction of a large set of staff theft characteristics. A more complex theory concerns the relationship between the number of previous burglaries and the incidence of stock theft by employees in a store. Work is ongoing to develop theories on offender and store profiles that are important in refund fraud and stock theft. The theories resulting from analysis of repertory grids are used as a basis for identifying both data gaps and further tests which can be carried out on existing databases.

3.3 Associating Theories with Data

To allow strategic decision making and policy design in a corporation, it is necessary to move from personal knowledge to organisational knowledge. Repertory grids only carry personal meaning and suffer from restrictions due to the small data sets from which they are constructed (in our work, repertory grids typically characterise 10 cases through 50 attributes). Organisational knowledge rests on adequate generalisation from these small data sets and a formalisation of data requirements.

In this phase of the technique, experts look for attributes in organisational data sets that match features derived from a repertory grid and attempt to apply a mapping between them. In the simplest case, it would be possible to map all features to existing data. Most commonly, in practice, one or more data quality problems are identified during the mapping attempt. For example, all retailers we have worked with have identified issues of data quality in existing business databases. These issues range from incomplete data to data that is not gathered at all, as we have described above for example, those that occur in the use of EPOS and personnel records where we find accessibility, contextual and representational problems.

Where conjectures cannot be tested because the mapping fails, gaps need to be filled by reconsidering the business priorities for collecting data. An assessment needs to be made of the gains to be made in loss investigation versus the costs of data collection. Where steps have to be taken to address the data problems, constructs in a repertory grid can be used to inform data requirements. In this case, constructs taken from a repertory grid have formed a rough-cut structure for gathering further data.

3.4 Testing Knowledge

Where information from data sources has been associated with constructs and elements, the expert's theory can be tested by reference to a wider sample. To apply a test, data sources are analysed using the same technique as the one applied to the initial repertory grid analysis to generate a theory. To support the testing of knowledge we use group contrasts that compare results from both repertory grids and data sources [Stumpf and McDonnell 03]. Testing assesses the quality of knowledge by comparing personal experience and factual data; a pre-requisite to modifying operational procedures which are sanctioned on an organisational level. For example, the theory of key holder being much more likely to be involved in stock theft than non-key holders was tested against data available from a security database. The theory was confirmed and the way that retailers investigates stock theft has been modified.

In the absence of large-scale data sets on an organisational level, promising conjectures can be tested by one-off field investigations. This is the approach taken to explore the relationship between burglaries at stores and the amount of theft of stock by staff and further serves to underpin a business case for policy change.

On contrasting the theory and the test – the former derived from repertory grids, the latter from existing data sources – it would be tempting to give greater credence to the test with a larger data set. If this is all we get, it could be argued that we are merely showing how representative or otherwise the small set of cases used in the repertory grid are of cases overall. However, these tests are as much about questioning assumptions as they are about harnessing what is already known. A theory that is rejected still has its use in this context as an opportunity for an expert to reflect on their knowledge and revise their (mis)conceptions. Furthermore, our investigation raises an interesting question for the businesses involved when a theory and its test resulting from existing data sources diverge widely. Neither appear to be perfect: experts may present a skewed view of reality based on their experience and prejudices, however it is also possible that it is the existing data that is suffering from data quality problems. In either case, the comparison draws businesses' attention to issues based on evidence rather than speculation.

4 Conclusion

We have presented our work with retail security specialists investigating staff theft. The 'theorise-inquire' technique was described; this procedure enables experts to express and capture knowledge, develop theories, associate these theories with data, identify data gaps and test theories to establish and improve organisational knowledge. Using this technique supports business decision making by specialists and organisations as a whole by allowing the comparison of theories based on experience with factual data.

However, there are some potential pitfalls. Seeing elements and constructs as records and attributes invites criticism about the sample size a grid is based on. Such criticism displays an impoverished understanding of repertory grids and detracts from the value of the technique: the repertory grid technique originates from expressing the way that an individual construes experiences. However, the quality of a grid is very sensitive to the conversational approach used to elicit it in the first place and, associated with this, the quality of 'items of experience' which are used to construct a grid. Thus, great care must be taken to choose stereotypical elements that cover the range of the domain under investigation [Gaines and Shaw 93b]. The issues that remain in our work are that counterexamples to staff theft are not readily available; hence, conceptions of what is not suspicious need to be reintroduced at some stage.

We find that the knowledge an organisation holds cannot easily be shared across organisations although, in the case of our work, organisations are both willing and anxious to learn from each other [Stumpf and McDonnell 02b]. Once grids are in a form that supports organisational learning – within one organisation – we find that the most interesting insights are not easily transferable to others. It suggests that the sorts of grids, theories and tests which promote learning within retailers are not those which promote 'best practice' exchanges between organisations.

Results of data analysis techniques are difficult to interpret by domain experts. Whilst we have identified a number of analysis techniques that are useful, work remains to make the results of these analyses understandable to security experts without mediation by others.

Loss prevention makes an important contribution to retail profits, however, these knowledge-intensive support activities suffer to a more extreme degree from the tension between experts' intuition and factual evidence than work that supports core business activities where feedback from data to a business strategy is more readily available. A study of knowledge management in these areas highlights problems arising from the tension more generally. The 'theorise-inquire' technique helps to make visible issues associated with data, information and knowledge quality, which is the first step in quantifying their impacts on an organisation.

References

[Alavi and Leidner 01] Alavi, M., Leidner, D. E.: "Knowledge Management and Knowledge Management Systems: Conceptual Foundations and Research Issues"; MIS Quarterly, 25, 1 (2001), 107-136

RETAIL CRIME PREVENTION STRATEGIES: CORPORATE JUSTICE -V- CRIMINAL JUSTICE; AND OHS CONSIDERATIONS IN RETAIL VIOLENCE

Denny van Maanenberg, Ass. Dip (Sec. Man.) M.I.S.M.

Managing Partner, Retail Risk Management Services

Retail industry in Australia employs over one million staff which represents 13.5 per cent of Australia's total employment population. In 1992, there were 172,000 shopfront locations which recorded a $96 BILLION dollar turnover (Madden 1993, pp.1-2). These figures released by the Australian Bureau of Statistics for the period 1991—1992 indicates the size of the retail industry. More than one in ten of our employment population works in retail. Certainly a sizeable work force.

I am often told, that to work in this industry, you are expected to acquire the patience of a saint, the logic and rationale of a philosopher, be a skilled negotiator to handle the many facets of human behaviour encountered in the industry and at the same time be able to make sales.

Much research and many books have been written on all aspects of retail, including marketing strategies, environmental design, advertising, buying, shop layouts and merchandising and how to get that elusive one million dollar sale. Not surprisingly then, the retail industry concentrates its efforts on its major objective, and that is simply to maximise sales. Without sales, the retailer cannot survive. Every store manager, sales supervisor or sales manager at state and national level direct all their energies toward achieving that objective. Nothing else matters. There is nothing wrong with this philosophy, and you cannot help but get excited when you listen to the enthusiasm of sales staff relating end of day figures, that budgets have been smashed and product is going out the door faster than you can get re-supplies in. Retailing like this, is exciting and you cannot help but get spirited along with the sales staff.

It is a different story however, that when, at the end of the accounting period, stocktakes are finally completed, the figures are in, and suddenly all those sales and the healthy bottom line that had been posted for sales, has been eroded, in some cases drastically, by the most hated topic in the retail industry, the ubiquitous "shrinkage". It is at this point when managers are sacked, sales supervisors demoted, knee jerk policy and procedures are implemented, ancestry of loss prevention managers are questioned and general panic ensues. It is my experience that somewhere between sales and shrinkage, there lies a huge void, a black hole that retailers shun and do not wish to acknowledge. It is alien to them. Most do not wish to discuss it. Retailers thrive on positives, motivation and sales.

Shrinkage is negative, de-motivating and means losses. To most, shrinkage is the dark side of retailing. Retailers understand the factors conducive to good retailing, but sadly enough do not properly understand the factors that can cause good retailing to go bad. It is hardly surprising then, that research into this area has not had the same degree of attention as the other more positive aspects of retailing. In other countries such as the US, Great Britain and Canada, retailers are presented with masses of data relating to all aspects of shrinkage loss. In Australia however, rather than develop our own local research, we have tended to rely on the experience of other countries. That situation has now been changed, but I do believe that our lack of local data has helped create the current situation, and allows the "void or black hole" between sales and shrinkage to continue.

Up until the release of, *The First Australian National Survey of Crimes Against Business* (Walker 1994), there had been little or no real research undertaken as to what constitutes loss and that which could be compared against overseas data.

So how much do we lose? There have been some excellent publications relating to retail theft in Australia such as Dennis Challinger's book, *Stop Stealing From our Shops*, which gave us great insight into loss caused through the hands of thieves and other offenders. But even Challinger admits that, "The total losses suffered by Australian retailers as a result of criminal activity are not known" (Challinger 1988, Foreword). In very general terms, loss prevention specialists throughout Australia pointed, toward a 2 per cent loss (calculated at cost value of goods) of total sales.

Based on these guesstimates, retailers throughout Australia could be losing up to $1.9 BILLION dollars annually. These industry guesstimates have proven to be correct. When we compare this figure against the Crime Against Business survey results, we see a similar figure (Walker 1994, p.111). This figure represents approximately 1.97 per cent of gross sales.

So how do we compare with overseas figures? In the absence of the complete international study, we can obtain general comparisons. Three fairly recent surveys show results from overseas. These are shown as a guide only and should be used for comparison only. For complete interpretation, readers should refer to the source.

COUNTRY	SHRINKAGE LOSS	SOURCE
UNITED STATES	1.58 per cent (Median)	(Berlin, Sep, 1993 p. 1)
CANADA	2.3 per cent (Average)	(Berlin, Nov/Dec 1991 p.1)
UNITED KINGDOM	1.1 per cent (Average)	(Braithwaite, 1992 p.4)
AUSTRALIA	1.97 per cent (Average)	(Walker, 1994, p.111)

So what is "shrinkage"? The terms origin seems to have been lost in antiquity, and really is a misnomer. Shrinkage is simply the term used to differentiate between theory and actual levels of stock. I would prefer to use the term, "retail loss", as this term has the potential to describe all areas of economic loss. Be it the loss of stock, a lost sale, or lost time due to sickness etc., rather than just the loss of stock calculated through stocktakes.

So how do we define retail loss? One simple definition;

> Retail loss occurs as a result of direct natural disaster, a careless, negligent or criminal action caused through either internal or external sources.

In very broad terms, we can place retail loss into two main categories. Known Loss and Unknown loss. Known losses are those to which a reason can be attributed. For example, a cash shortage of $100.00. The loss is immediately known, but the cause may not be instantly clear and may need to be investigated. The loss may be due to error, negligence or plain dishonesty. Other known losses result from:

- Natural disasters such as fire and flood;
- Armed Robbery;
- Burglary;
- Cheque Fraud;

- Credit Card Fraud;
- Reported known thefts both internal and external; and
- Cash discrepancies.

Unknown losses however, are those to which a reason cannot be attributed. These unknown losses are referred to generally as the ubiquitous shrinkage and usually occur through any one or more of the following causes:

- Human or Administrative Error;
- Employee Malpractice; and
- Customer Dishonesty

I could spend the remainder of this presentation detailing cause and effect, loss prevention strategies and recommend a thousand and one policies and procedures that retailers should adopt to reduce retail loss through the many variables. But rather than use this forum as a platform to discuss retail loss prevention strategies in general. Given the nature of this conference and the time constraints imposed, I would like to focus on only two areas which are often the subject of concern. One usually expressed by employers, the other expressed by employees.

My first topic relates to the concerns retailers face on deciding a prosecution policy. The second, relating to employee safety in the workplace with regard to violent situations.

CORPORATE JUSTICE OR CRIMINAL JUSTICE

In brief, the criminal justice system involves dealing with the police processes that include the taking of statements, interrogation, finger printing and the laying of charges. It includes all subsequent court appearances, bail and appeals, and includes the terms of imprisonment. In short, the criminal justice system is the legal process and procedure involved from the time a person is arrested, processed, charged, tried, imprisoned, and paroled. To the moment he or she is returned to society as a free person.

Corporate justice on the other hand, deals with employee malpractice and customer dishonesty at an internal level within the given business corporation, rather than that business reporting the matter to law enforcement authorities. *The First Australia Survey of Crimes against Business* reports that 60 per cent of businesses who were victims of crime did not report it. Reasons given included;

- Lack of evidence;
- Not serious enough;
- Police could do nothing; and

- Too much trouble (Walker 1994, p.37).

Additionally, only 16 per cent of businesses had contacted police for advice (Walker, 1994 p.86). This tends to show a general reluctance by businesses to report instances of crime. Does this indicate a lack of support for the criminal justice system? Is the general business community generally apathetic? Answers are many and varied. The survey suggests that one reason why such a high proportion of crime is not reported to police is the "on-costs" factor. In other words, reporting the crime and following it up is often more costly than the crime itself. It is more economical to pass on the cost to consumers through price increases (Walker 1994, p.100).

The practicality of involving police for every crime related incidence also comes into question. In a report on shoplifting, the now defunct National Retail Crime Prevention Council stated; "..If retailers always called police to attend their shops when they detected a thief, the police might have little time for anything else" *(*Challinger 1988, p.138). Ten years ago, one paper on this topic suggested that existing criminal justice systems were seen to be largely, 'expensive, counter productive and ineffective', (Stenning 1984, p.85). It would appear that nothing much has changed.

It is appropriate to say that all retail operations are profit orientated and that the first consideration must be to regain the funds or the property that was misappropriated. Retailers have little interest in long drawn out court cases which may or may not arrive at a result favourable to them. There is little satisfaction in the knowledge that a person who was handed over to police, was subsequently sentenced to two years imprisonment, and then was unable to repay the thousands stolen. There may be a question of principle, but for many retailers, principles do not put dollars in the till. Retailers faced with this situation are more inclined to negotiate the matter internally to the satisfaction of all parties concerned.

On the other hand, many see that the failure of reporting crime to the police only increases its occurrence. If shopstealers are aware that a particular retailer has a non-prosecution policy, then opportunities are created that will undoubtably increase the levels of theft. Likewise, if a retailer chooses to dismiss staff for gross misconduct on proven grounds of dishonesty, rather than reporting the matter to police, this leaves the retailer wide open for criminal abuse by other employees.

Another consideration is, 'self inflicted crime'. By self inflicted crime, I refer to policy and procedures such as open ended cash refund policies some retailers adopt that clearly invite theft. Thieves simply steal product and moments later, cash refund the item without questions being asked. In these

THE ARGUMENTS FOR	THE ARGUMENTS AGAINST
HAVING A POSITIVE PROSECUTION POLICY IS A NATURAL DETERRENT.	THE COMPANY MAY HAVE A LACK OF CONFIDENCE IN THE JUDICIAL SYSTEM.
BY NOT PROSECUTING, THE RETAILER ONLY SAVES MONEY IN THE SHORT TERM.	SOMETIMES CORPORATE JUSTICE IS BETTER SERVED THAN CRIMINAL JUSTICE.
PROSECUTION SENDS MESSAGES TO ALL EMPLOYEES THAT THE COMPANY DOES NOT TOLERATE MALPRACTICE.	THE COMPANY DOES NOT BELIEVE IN "DOBBING", AND WOULD RATHER JUST GET RID OF THE PROBLEM.
POSITIVE PROSECUTION POLICIES REINFORCE THE COMPANIES CODE OF CONDUCT.	PROSECUTION COULD LEAD TO STRAINED RELATIONSHIPS WITH UNIONS.
PROSECUTION IS A CIVIL DUTY.	PROSECUTION IS EXPENSIVE AND TIME CONSUMING.
PROSECUTION PROTECTS EMPLOYERS FROM ALLEGATIONS BY FUTURE EMPLOYERS OF FAILING TO DISPLAY A "DUTY OF CARE" TOWARD THE RETAIL INDUSTRY.	PROSECUTION INVITES UNFAVOURABLE PRESS.
	A VIGOROUS PROSECUTION POLICY DAMAGES A COMPANIES IMAGE IN THE MARKET PLACE.

Let us look at one case study. For the sake of this presentation, I have included the three basic common denominators for crime to occur;

- NEED
- OPPORTUNITY
- RATIONALISATION

In very simple terms, if one of these three elements is missing, then theft is eliminated.

Case Study ?
A senior employee was caught out after she had conducted a fraudulent and fictitious refund to the value of $40. The incident was then reported and subsequent interviews with all parties concerned revealed that the employee had been with the company for many years, and in recognition of her service was transferred on promotion to a remote location. Her husband gave up a good job to go with her. After some time on site, she was again transferred to another remote location on further promotion and once again her husband gave up his new job to accompany her. At the latest location, no work was available for the husband, accommodation was hard to come by, and expensive. The cost of transferring was high and reserve funds were depleted. It was between paydays, the cupboard was bare and the weekend loomed... There was no cash around, so she "borrowed" the $40.
The case for the employee;

NEED	Overwhelming economic need due to sudden loss of spouse income
OPPORTUNITY	Senior employee with open and unlimited access to company regional sites and cash registers.
RATIONALISATION	"They owe it to me for all the moves I've made, besides I'm only "borrowing" the money, and I'll repay it when we're on our feet!"

Management considerations. Management had a responsibility and an accountability, not only to the proprietors of the organisation, but also to their employees to ensure that line supervisors were sufficiently tuned into employee needs. This also extends to such practices as employee assistance programs in making available temporary emergency cash loans, or advances on pay etc.

Management also failed to take into account the high costs involved of transfer, or to ensure that the staff member had sufficient capital in the short term to meet those interim costs. Additionally, management had also failed to convey to the staff member that emergency staff loans were available to any staff member who needed temporary cash funding. Cash handling controls and refund procedures were being monitored through independent deficiency analysis by central computer monitoring. Sound paperwork trails that needed to be verified through review resulted in this act of malpractice being reported to management.

Arguments designed to eliminate rationalisation included company codes of conduct, and clear statements relating to employee malpractice were promulgated throughout the organisation and reinforced by competency based fraud awareness training. Generally, employees of this organisation were explicitly told that malpractice would not be tolerated under any circumstances. Although the employees training records did not indicate attendance at any malpractice related training course.

To prosecute or not? The decision to prosecute or not, is an individual retailers choice. Decisions must be based on the situation and can change as situations change. Whatever event occurs that requires an examination of corporate moral and ethical standards needs to be done on its own merits using logic and rational thought processes. If a retailer believes, after taking into account all the possible variables, that the interests of all parties concerned are best dealt with at corporate level, then that decision can hardly be described as being unethical, inappropriate or illegal.

Conversely, the retailer may well decide the interests of the business would be better served if the matters were dealt with by the police, and again this decision may be equally correct.

In this particular case, the employee was severely reprimanded, informed that she would not be considered for future promotions, and demoted. At the same time, however, the company concerned gave her an immediate company loan to overcome her pressing financial need.

OCCUPATIONAL HEALTH & SAFETY CONSIDERATIONS IN RETAIL VIOLENCE

The latest figures indicate that 11,780 robberies occurred in Australia, up nearly 25 per cent on previous years. In the 1991—92 period, NSW reported 5,973. Queensland reported 1511 and Victoria, 1933.

The Crimes against Business survey showed that 1.6 per cent of the total survey population of 966 reported an armed robbery. Although the 1.6 per cent indicated the total figure, it does not necessarily reflect a true representation. For example; whilst small businesses only showed a small percentage, (1.5 per cent), larger businesses reported occurrences three times higher (4.4 per cent.). We could therefore make an assumption that employees working for larger businesses are more likely to be involved in an armed robbery than those employed by a smaller one (Walker 1994, p.43).

Discussions with the author of the Crimes Against Business survey reveal that 24 robberies were reported. This indicates a ratio of 1:40. Although the survey indicated it was extremely rare for an armed robbery to occur, we can make an assumption that although an armed robbery may be unlikely for a fair percentage of retailers, chances of it occurring are still relatively high.

But violence does not only relate to robbery situations, it also includes assaults on staff by customers. The survey indicated that 1 in 10 businesses experienced an assault on staff, (Walker 1994, p.4). Once again the larger the company, the more likely an assault (ratio 1:20). The smaller the business, the less likelihood of assault (ratio 1:60) (Walker 1994, p.122). These figures show that assaults can still take place anywhere. Take these three case studies for example;

A staff member believed that a customer had placed some items into his bags and requested a bag inspection. As she bent over to look into the bag, she was "king hit" by the customer. She suffered a depressed fracture of her cheek bone.

On closing time, a lone sales person was cashing up, when a male offender entered the shop and without a word, bashed the staff to the ground, and began kicking her. She managed to grasp a fixture attachment, and hit the offender with it who promptly ran out of the shop.

A pizza shop employee was punched in the face when he tried to reason with an irate customer. The employee went outside the shop to speak with the customer, who verbally abused then punched him.

More serious are those instances where an armed robbery takes place. Not only do employees face the risks of serious physical injury, more often than not, the emotional and psychological injuries suffered are far greater than any physical ones.

Emotional stress and questions of self worth, cowardice, why did it happen to me, often ensue resulting in the employee taking extended sick leave to undergo post trauma counselling. Quite often is the case that the employee is unable to return to the workplace at all. Retailers generally do not see the threat of violence against their staff as being a major problem. Many in my experience, just deal with these situations as they occur. Many believe that these types of instances are rare, only affect high risk areas such as banks, building societies and other high cash carrying premises. These assumptions are plainly wrong.

When discussing these types of situations with new retail sales staff, I often ask the question, "What would you do if....?" I'm often surprised by the responses of young males who state: "I'd bash 'em!" "Give them nothing", "They'd have to kill me first". I sometimes wonder if the influence on society through the media, generates a false sense of bravado on young people. Action movies often falsely portray: "A manly image", and to, "hit back". The "don't let them get away with it", syndrome. Under these circumstances, it is often difficult to instil in our employees that, "caution is not cowardice".

I often wonder what would happen if an employee, faced in a violent robbery, hit back, and was suddenly seriously injured. If this person had not been given any training in this area by his employer, would he or she have grounds for an action against the employer? The answer is simply yes. Two courses are open. Firstly the employee could sue the employer under Common Law provisions of Duty of Care. Considerations include;

FORESEEABILITY	Could the incident have been one which the employer should have foreseen?
PROBABILITY	Was the incident one which could reasonably be expected to occur?
PREVENTABILITY	Could the incident have been prevented through training awareness or its effects minimised?
CONSEQUENCES	Were sufficient procedures in place to adequately address all consequences such as post trauma counselling etc.?

Under Common Law provisions of Duty of Care, an employer's liability extends to;

- Providing a safe place of work;
- Laying down a safe system of work;
- Providing safe and adequate tools and equipment;
- Providing employees with competent fellow employees; and
- Adequately instruct in, and supervise the performance of work.

Secondly, relevant state authorities could take action against the employer under applicable state or federal occupational health and safety legislation. In Victoria, Section 21(1) of the *Occupational Health & Safety Act* states;

Responsibilities of Employers. (Section 21(1).

Retail Crime: Prevention through Crime Analysis

John Burrows

CRIME PREVENTION UNIT: PAPER 11
LONDON: HOME OFFICE

Editor: Kevin Heal
Home Office Crime Prevention Unit
50 Queen Anne's Gate
London SW1H 9AT

Discussions with the author of the Crimes Against Business survey reveal that 24 robberies were reported. This indicates a ratio of 1:40. Although the survey indicated it was extremely rare for an armed robbery to occur, we can make an assumption that although an armed robbery may be unlikely for a fair percentage of retailers, chances of it occurring are still relatively high.

But violence does not only relate to robbery situations, it also includes assaults on staff by customers. The survey indicated that 1 in 10 businesses experienced an assault on staff, (Walker 1994, p.4). Once again the larger the company, the more likely an assault (ratio 1:20). The smaller the business, the less likelihood of assault (ratio 1:60) (Walker 1994, p.122). These figures show that assaults can still take place anywhere. Take these three case studies for example;

A staff member believed that a customer had placed some items into his bags and requested a bag inspection. As she bent over to look into the bag, she was "king hit" by the customer. She suffered a depressed fracture of her cheek bone.

On closing time, a lone sales person was cashing up, when a male offender entered the shop and without a word, bashed the staff to the ground, and began kicking her. She managed to grasp a fixture attachment, and hit the offender with it who promptly ran out of the shop.

A pizza shop employee was punched in the face when he tried to reason with an irate customer. The employee went outside the shop to speak with the customer, who verbally abused then punched him.

More serious are those instances where an armed robbery takes place. Not only do employees face the risks of serious physical injury, more often than not, the emotional and psychological injuries suffered are far greater than any physical ones.

Emotional stress and questions of self worth, cowardice, why did it happen to me, often ensue resulting in the employee taking extended sick leave to undergo post trauma counselling. Quite often is the case that the employee is unable to return to the workplace at all. Retailers generally do not see the threat of violence against their staff as being a major problem. Many in my experience, just deal with these situations as they occur. Many believe that these types of instances are rare, only affect high risk areas such as banks, building societies and other high cash carrying premises. These assumptions are plainly wrong.

When discussing these types of situations with new retail sales staff, I often ask the question, "What would you do if....?" I'm often surprised by the responses of young males who state: "I'd bash 'em!" "Give them nothing", "They'd have to kill me first". I sometimes wonder if the influence on society through the media, generates a false sense of bravado on young people. Action movies often falsely portray: "A manly image", and to, "hit back". The "don't let them get away with it", syndrome. Under these circumstances, it is often difficult to instil in our employees that, "caution is not cowardice".

I often wonder what would happen if an employee, faced in a violent robbery, hit back, and was suddenly seriously injured. If this person had not been given any training in this area by his employer, would he or she have grounds for an action against the employer? The answer is simply yes. Two courses are open. Firstly the employee could sue the employer under Common Law provisions of Duty of Care. Considerations include;

FORESEEABILITY	Could the incident have been one which the employer should have foreseen?
PROBABILITY	Was the incident one which could reasonably be expected to occur?
PREVENTABILITY	Could the incident have been prevented through training awareness or its effects minimised?
CONSEQUENCES	Were sufficient procedures in place to adequately address all consequences such as post trauma counselling etc.?

Under Common Law provisions of Duty of Care, an employer's liability extends to;

- Providing a safe place of work;
- Laying down a safe system of work;
- Providing safe and adequate tools and equipment;
- Providing employees with competent fellow employees; and
- Adequately instruct in, and supervise the performance of work.

Secondly, relevant state authorities could take action against the employer under applicable state or federal occupational health and safety legislation. In Victoria, Section 21(1) of the *Occupational Health & Safety Act* states;

Responsibilities of Employers. (Section 21(1).

> An employer shall provide and maintain so far as is practicable for employees a working environment that is safe and without risks to health'.
>
> Duties of Employers. (Section 21(2)).
>
> 'An employer shall provide and maintain;
>
> a. SAFE PLANT AND SYSTEMS OF WORK
>
> b. SAFE USE, HANDLING, STORAGE AND TRANSPORT OF PLANT AND SUBSTANCES
>
> c. SAFE WORKPLACES
>
> d. ADEQUATE FACILITIES FOR EMPLOYEES WELFARE
>
> e. INFORMATION
> INSTRUCTION
> TRAINING
> SUPERVISION
>
> To enable employees to perform their work safely.

It would appear then, that the risks associated with failing to provide employees with adequate training to equip them in the event of violent situations, could leave retailers and the general business community wide open to legal prosecution. For the retail community at large, this should be a very real concern. When discussing general loss prevention strategies with retailers, one consideration is awareness training that provide employees with the skills, knowledge and attitudes necessary to minimise the effects of a violent situation. I also ask if the retailer has a post trauma counselling policy. More often than not, I find that retailers do not consider that training in these areas are necessary. I find that situation disturbing.

In conclusion, the *Crimes Against Business* (Walker 1994) has provided the general business community, particularly retailers, sufficient information and data that enables further development on loss prevention strategies, and subsequent development of policy and procedures that address crime prevention issues. There is much to be done. In Australia, the survey indicates that we tend to spend less on security and crime prevention measures than some other western countries (Walker 1994, p.111). Once again we can use overseas figures for comparison.

Retail Crime: Prevention through Crime Analysis

John Burrows

CRIME PREVENTION UNIT: PAPER 11
LONDON: HOME OFFICE

Editor: Kevin Heal
Home Office Crime Prevention Unit
50 Queen Anne's Gate
London SW1H 9AT

First published 1988

Crime Prevention Unit Papers

The Home Office Crime Prevention Unit was formed in 1983 to promote preventive action against crime. It has a particular responsibility to disseminate information on crime prevention topics. The object of the present series of occasional papers is to present analysis and research material in a way which should help and inform practitioners whose work can help reduce crime.

ISBN 0 86252 313 3

Foreword

A recent report by the Home Office Standing Conference Working Group on Shop Theft laid considerable emphasis on the need for retailers to introduce preventive measures based on detailed analysis of the crime problems they were facing. This too was the message of an earlier volume in this series (CPU Paper No. 5), which looked specifically at theft by shop customers.

The present report draws on the experience of a large retailer — the Dixons Group — who have implemented this strategy in a bid to tackle not only theft committed by customers at their stores, but a great many more of the crime problems familiar to other retail companies. It offers a convincing case for other retailers to apply the principles of 'crime analysis' to their problems, as well as practical — step by step — advice as to how they should do so.

This report is illustrative of the progress being made in developing ways of analysing crime problems and of devising preventive measures. It also demonstrates the growing willingness to exchange ideas and information in an endeavour to control crime. John Burrows, formerly a member of the Crime Prevention Unit, now works with the Dixons Group where he is Group Security Adviser. It is pleasing to see the development of such a systematic and imaginative approach to crime within a major company, and the willingness of Dixons to share, through this publication, its experiences with others in the retail sector.

J A CHILCOT
Deputy Under Secretary of State
Home Office, Police Department
February 1988

Acknowledgements

Thanks are due to Stanley Kalms, Chairman of Dixons Group Plc, for his readiness to support publication of this report and to Dick Andrews for his co-operation and advice in its preparation. Comments on early drafts by several former colleagues at the Home Office — Lorna Smith, Gloria Laycock and Paul Ekblom — were also much appreciated.

JOHN BURROWS

Contents

than one in five of the major retailers they approached were able to provide this (see Home Office, 1986 p 18). It was equally evident in the fact that those who were able to respond to this survey were only able to attribute 11% of their 1985 losses to *known* instances of crime. The remaining 89% of 'unidentified' loss represented an average 0.9% of their turnover: though of course because all losses come straight off the bottom line of a company's profitability (comprising the handling and cost price of the goods as *well* as lost profit margin) the real cost is much more significant.

The financial costs are only one side of the problem: there are also important human and social costs associated with this crime. As well as facing personal attack or intimidation as the 'guardians' of their own (or their employees') interests, those working in retailing have to put things in order — and liaise with the police — after burglaries and other non-personal incidents. The anxiety and fear this creates is naturally carried forward into their personal lives. The impact is quite often not restricted to the individuals directly involved: it is known that some retail outlets — newsagents, local post offices and so on — act as important focal points within neighbourhoods, where conversations about crime can affect residents' perceptions of the locality (Shapland and Vagg, 1985).

Prevention through Crime Analysis

The retailer who is concerned to tackle the problem of crime is faced with some difficult options. There are a variety of methods he might pursue: these could range from the implementation of more comprehensive staff training or supervision; could encompass the installation of technologically advanced controls (CCTV, 'tagging systems', alarms, etc.); and might even include modification of merchandising, sales or distributive procedures. The payoff from any of these methods is uncertain. But, in a competitive environment, the effort and expenditure devoted to prevention and control is bound to require some reasonable assessment of the dimensions of the initial problem and what remedial action will achieve.

One way of moving towards this goal is to apply what has come to be labelled as the technique of crime analysis. The logic of crime analysis derives from a range of well documented cases demonstrating that a good proportion of criminal incidents occur at certain locations or times, or in particular circumstances[4]. These crimes can often be separated from other, more randomly distributed, incidents. They generally follow patterns because each 'trouble spot' offers opportunities to those inclined to offend: thus shoplifting is perceived to be easier in certain vulnerable areas of a shop,

(4) Much of the recent work of Home Office researchers underlines this basic point. At a broad level, the British Crime Survey (Hough and Mayhew, 1985) for example, has emphasised the different risks of burglary to houses in different areas and studies of police records have shown how incidents are patterned against particular targets (see Ramsey, 1982). In addition, specific research has highlighted, for example, how burglary risks within small areas are affected by occupancy or surveillance levels (see Winchester and Jackson, 1982), how car thefts are affected by the vulnerability of different makes (Burrows, 1979) or the presence of steering column locks (Mayhew, 1976) or how crime within concise areas like shops (Ekblom, 1986) or hospitals (Smith, 1987) is directed at specific locations at specific times.

burglaries are committed at branches where security is poor or at times when the chances of apprehension are deemed to be low, and theft by staff occurs because administrative or procedural practices are lax. The purpose of crime analysis is to identify these weaknesses, in order to block the opportunities.

There are four steps in the preventive process (these are discussed by Ekblom, 1986, in the context of shoplifting incidents):

(a) Crime analysis: defining the problem
(b) Identifying means of preventing it
(c) Implementing the chosen strategy
(d) Evaluation (is the response effective?)

It goes without saying that the type of activity involved at each stage will vary widely according to the characteristics of the 'presenting' problem. Thus shoplifting may be assessed either by routine monitoring of stock control records, by specific experimentation at certain sites, or by analysis of those incidents where offenders are caught (or by a combination of these methods). And of course any investment in prevention (and subsequently, any evaluation of its impact) is bound to be dictated by the size and seriousness of the problems identified by these analyses.

Following an earlier report in this series on the need for crime analysis to tackle the problem of shoplifting (see Ekblom, 1986) this report attempts to make the case for applying similar methods to a wider range of retailers' problems: from theft by staff themselves to burglaries. Its primary objective is to highlight the sort of issues which crime analysis in a retail environment might want to address and — in doing so — to offer practical advice on methods of collecting, recording and analysing data. Although every attempt has been made to cover a wide range of the crime problems experienced by retail outlets, the report focusses on the loss of stock and cash from shops and distribution networks, and does not deal with equally important areas such as computer fraud. It is primarily based on a system established in two electrical retailing chains — Dixons Limited and Currys Limited — that form part of the Dixons Group of companies.

Structure of the Report

Chapter 2 presents a more detailed case for applying crime analysis techniques to the problem of retail crime. Chapter 3 then outlines the wide variety of operations covered by Dixons and Currys - ranging from the problems of distribution to over 900 individual branches, through their sales operations, and on to the need to provide a customer delivery service for larger goods — and explains the broad principles of the computerised system which they use to record and analyse reported crimes. Chapter 4 looks at some of the issues that need to be addressed in each sphere of operations and how information on each can be accumulated and analysed. Chapter 5 offers advice on establishing computerized databases.

CHAPTER 2: THE CASE FOR CRIME ANALYSIS

In responding to the challenge of crime, most retailers would accept the wisdom of the adage that 'prevention is better than cure'. They would be right to do so, and not simply in token terms. Substantial criticisms can be made of policies aimed at 'cures' for retail crime.

First, it is clear that most crime is not committed by a distinct or finite criminal fraternity — who might, in time, be detained and dealt with by the police and courts — but by a much wider sector of the population. Looking specifically at shoplifting, for example, various studies have suggested that at least 1.5% and perhaps as many as 8% of customers going into shops take something without paying (see Murphy, 1986 for review). Though not a numerically large percentage, extrapolating these results to a sizeable department store — dealing at any time, say, with 1,000 shoppers — means that between 15 and 80 of these shoppers are likely to be removing something without payment. Few will be caught and fewer still referred to the police. Whilst it is true that a very large number of almost all types of crime generally remain unreported or unrecorded (see Hough and Mayhew, 1983 and 1985), evidence from official statistics of *known* crimes also shows that crime is an activity not restricted to a few aberrant individuals: recent studies have suggested that nearly 1 in 3 (30%) males will have at least one conviction for a 'standard list' offence by the time they reach the age of 28 (Home Office, 1985)[1].

Despite this wide involvement in criminal activity (albeit often on a petty scale) the chances of catching the perpetrators of crime are small. This is simply because those involved do all they can to avoid being caught, and there are countless opportunities during the retailer's trading day for them to do so. A similar point has been recognised for some time as a major constraint on conventional deterrant policing and has been supported by the large body of research which has shown that increasing police patrols does not reduce crime (see Clarke and Hough, 1984 for review). It applies with equal force in the retail environment. Research interviews with known offenders have also shown that the low chances of apprehension are well appreciated by those involved in crime (see, for example, Bennett and Wright, 1984).

Finally, even if retailers were able to identify and pass on to the police those responsible for their losses, criminologists have thrown serious doubts as to whether the criminal justice system — in isolation — can provide any effective 'cures' to prevent re-offending. Different treatments — prison, detention centres, probation (or different regimes with each) have proved little better than one another in reducing recidivism (see Brody, 1976 for review). Indeed, the evidence shows that the likelihood of continued offending increases as the offender becomes more deeply

[1] As well as excluding offences which do not come to the notice of the police, these 'standard list' offences exclude most summary motoring offences, and other summary offences such as drunkenness or prostitution. This Home Office bulletin points out its findings are "not out of line" with Farrington's (1981) estimate that over 40% of males would eventually be convicted of an indictable offence at some time in their lives.

involved in the criminal justice system (see Home Office, 1987). Moreover unless the numbers of offenders sent to prison increased dramatically (at impossibly high cost), research has indicated that the simple act of 'incarcerating' offenders has little impact on overall levels of crime (see Brody and Tarling, 1980).

But are the prospects for preventive action any brighter? The purpose of this report is to suggest that they are, especially so if preventive action is based on rigorous analysis of each retailers' particular problems and their strategies tailored accordingly. This process — crime analysis — can point to the more obvious solutions as well as aiding the development of innovative (and, occasionally, cost free) preventive strategies. The application of such analysis is aimed at complementing the work of the police and other criminal justice agencies in combating crime, by fostering a philosophy of 'self help' amongst retailers.

Crime analysis can also be used to gauge whether existing security expenditure is being put to best effect. Even leaving aside the cost of insurance, retailers spend vast sums on preventive measures: on security hardware (from door locks to closed circuit television); on in-house security personnel; and on the services of the private security industry. Indeed, retailers are amongst the principal users of the services provided by this large — and apparently rapidly proliferating — industry[2].

The process is essentially aimed at reducing the opportunities available to commit crime. The case for it is that customers or staff are not simply either 'law abiding' or 'dishonest', but may be tempted and subsequently triggered into committing criminal acts by the opportunities presented by particular environmental conditions. Crime analysis enables retailers to address the *situation* in which crime occurs rather than being concerned to understand complex questions of how psychological and social factors affect the *motivation* of the potential offender. Specifically, research has shown that an individual requires both an occasion to take a certain course of action, and the inducement (the appropriate conditions — where the perceived risk of being discovered is low) to do so. Reducing opportunities and increasing risks of discovery can therefore be powerful means of prevention.

This logic can be applied to most decisions to engage in crime (see Mayhew *et al*, 1976), but it is not restricted to criminal activities alone: Clarke (1983) cites many examples from other walks of life. It is argued here that the critical analysis of crime in retail settings is a necessary prerequisite to identifying the points at which thieves take advantage of the opportunities offered to them, and to successfully blocking these.

This argument is both simple and familiar to those in retailing: familiar, in that retailers are routinely concerned with increasing both the occasion and the inducements to purchase their goods. As styles of retailing have developed (see Walsh, 1978) in such

(2) There are no centrally held statistics. A 1979 Home Office discussion paper on the industry did however note that some 80,000 people responding to the 1971 census recorded that they were employed in private security functions: at this time the regular police force numbered 97,000 (Home Office, 1979). Only a proportion are employed directly by security organisations.

a way as to make goods increasingly accessible to the buying public, most recognise that this has involved a calculated risk. Unfortunately for retailers, this 'buying public' includes those likely to be tempted by the opportunities retailers have afforded for theft, as well as those who are not. As there is little prospect that current styles of merchandising will change significantly, critical thinking is required to reduce the inherent risks. There is a commercial tightrope to be trodden: between adventurous and successful merchandising on the one hand, and that which is too adventurous, leading to substantial losses from theft, on the other.

A similar delicate balance exists on the non-sales side. How are retailers to provide operating procedures that will ensure the fast and efficient movement of goods from warehouses to their shops, and indeed within them, without sacrificing accountability and allowing blatant opportunities for staff to steal?

If it is pursued successfully, crime analysis offers substantial dividends to the retailer. Put briefly, it offers straightforward commercial advantage. In the public sphere, the strength of the case for crime analysis is diminished somewhat by the prospect of crime displacement: the possibility that more committed offenders — denied opportunities to commit crimes in one area or at specific times — will divert their attentions to other areas or times. To the extent they do so, they remain a 'problem' to the police and other criminal justice agencies. But, while this likelihood underlines the need for the retailer to be constantly on the lookout for alternative circumstances in his own stores which may be exploited, it assumes little significance for the retailer who may successfully persuade offenders to target his competitors instead!

Case Study: Preventing Credit Card Fraud

As crime analysis has not been widely applied in the retail trade, any assessment of its impact must be deferred. However, one area where crime problems have been subject to an analytical approach for some time is within the cheque and credit card companies. The peculiarities of their business — particularly the fact that they bear practically all the losses resulting from fraud, but have to rely on others (largely retailers) to 'police' transactions on their behalf — make it a necessity that they invest heavily in prevention rather than detection.

Barclaycard's Fraud Prevention Department — for example — have the responsibility of monitoring frauds committed against any one of approximately 9 million Visa holders, and they currently expect to have about 1,000 of these cards reported lost or stolen each day. Three-quarters of these frauds take place in the retail trade, which means they have to focus carefully on this area to protect their customers and business interests.

Some of the analyses regularly carried out by Barclaycard illustrate the sort of approach taken:

* *The number of frauds committed against individual merchants is monitored closely.* This information is primarily used to reward or penalise merchants according to their performance (by determining both the 'floor limits' Barclaycard will impose on each, and their dealer charge). The figures have also yielded other useful patterns, such as instances where shopkeepers have regularly accepted transactions on stolen cards because they have been in collusion with the fraudster. (On an individual basis, Barclaycard pay £50 rewards to those who recover cards on their behalf — to the tune of £809,000 last year).

* *Card holders' patterns of usage are monitored.* This information is often used to identify unreported theft: customers who only irregularly use their Visa cards but who then suddenly appear to have embarked on a 'spending spree' are frequently found to have had the card stolen.

* *The value of frauds is carefully monitored.* This information is employed to inform preventive action, and to bring to the attention of retailers. In fact, the average value of a fraud is around £30 (it is believed that thieves think that higher value transactions have to be checked by the retailer).

* *Analysis shows where frauds are committed in departmental and other larger stores.* Again this is for use in determining whether special precautions (e.g. the installation of 'readers' that transmit card details direct to Barclaycard headquarters) are necessary. It also assists training programmed: retailers are frequently warned that the first 'strike' committed by the fledgling fraudster is often in the perfume department of larger stores: because this is invariably on the ground floor, and staff are perceived to be 'locked' behind a large counter, making escape easier.

* *Frauds are monitored 'by dealer class'.* Again this highlights the need for special precautions and serves to educate retailers. Supermarkets and garages frequently top the list, largely because they tend to employ younger, more inexperienced staff and staff turnover is high.

As well as performing this sort of analysis, the fraud department at Barclaycard are routinely involved in studying patterns of fraud against their counterparts overseas (particularly in the US) in order to assess whether preventive action is required in advance at home. Similarly, they engage in considerable experimentation. For example, to combat the theft of cards in transit in the post (which account for about 20% of those lost), they have mounted experiments in high risk areas which require customers to pick up their cards from a local bank. In other areas, there have been experiments to assess whether pre-mail shots ('a card will arrive in the next X days') or post-mail shots ('your card should have arrived X days ago') prove effective. In addition, some 64 different types of envelope are used to disguise card renewals sent through the post.

Whilst these analyses and enquiries may seem an integral part of proper management of the theft problem, they are far more sophisticated than those practiced in many other parts of retailing. This is, of course, to be expected given that their business (even more than that of the retailer) depends so heavily on balancing 'acceptable' against 'unacceptable' risks. However, in Barclaycard, they have proved their worth by reducing fraud losses as a percentage of the company turnover. Moreover, in 1985, they were instrumental in actually reducing the gross fraud loss overall: a considerable feat when set against a 5% annual increase in turnover, and the increasing spiral of other forms of crime (Home Office, 1986: paras 35/36).

Summary

The logic underpinning crime analysis is certainly not new. Indeed, it might be seen as doing nothing more than applying sound management principles in the security field: that strategy should be based on detailed and reliable analysis of the problems faced. On the other hand, this logic can constitute a significant departure from common practice in much of retailing: where security resources are diverted without careful consideration of the consequences[3], expenditure is often allowed without proper evaluation of its impact, and a premium is placed on making arrests rather than instituting preventive programmed. Above all, it marks a rejection of the anachronistic idea that 'security issues' can somehow be divorced from routine commercial decision making.

[3] See, for example. Ekblom's comments on the 'diminishing returns' of deploying store detectives to apprehend thieves (Ekblom, 1986).

CHAPTER 3: THE DIXONS GROUP

The aim of this chapter is to describe, in broad terms, something of the retail operations of Dixons Ltd. and Currys Ltd: how they are organised, the crime problems they face and the means by which crimes are reported and recorded. The main purpose in doing so is to allow other retailers to identify problems common to their own operation, and to put in context the subsequent discussion of the crime analysis database.

Retail Activity

The two companies are electrical retailers selling relatively 'high ticket' items, mainly in small to mid-size (one to four thousand square foot) high street locations. The network of stores is large — Dixons Ltd. currently comprises some 330 stores and Currys Ltd. some 400 — and is spread across the entire country. In addition, Currys run a chain of over 50 'superstores', which are very much larger and are generally located on the periphery of major towns. The merchandise stocked in each chain has many similarities: both sell 'brown goods' — TVs, video recorders, microwaves and so on. But whereas Currys stores also stock large 'white' merchandise, like fridges and washing machines, Dixons specialise in smaller electrical goods like cameras. Together, the two chains achieve the highest sales per square foot in the high street.

Branches receive most of their goods through deliveries from central warehouses. By and large, the content of each delivery is dictated by each branch's sales record, which are monitored at head offices. The warehouses (one serving all Dixons branches; two serving Currys branches) are similar to those operated by other chain store retailers: they handle goods received from suppliers (often in container form), store them and distribute them across the branch network. With the exception of peak periods like the 'run-up' to Christmas — when deliveries increase to match turnover — most deliveries are made on a weekly basis. 'Trunking' arrangement (i.e. the movement of goods to local depots, and then on to branches) are used in connection with deliveries to more distant locations.

In addition to these warehouse operations, Currys Ltd. has a series of stock or distribution centres which provide a customer delivery service for larger stock items. Each centre services a designated number of branches. Again, these operations broadly correspond to those used by other retailers merchandising larger goods (particularly the multiples).

The wide geographical distribution of the branch network militates against central control. Central control is strong in certain areas — such as merchandising policy, supply etc — and is exercised through regional teams (four in Dixons, six in Currys) which monitor sales, day to day operations, personnel selection and training, and other issues. Set against this, individual branch managers are allowed considerable discretion: both companies place considerable weight on the operational autonomy of individual branches in achieving sales, and offer branch teams substantial advice and incentives to match or improve on sales targets set by the centre.

Crime Problems

Like any large retail organisation, there are a range of opportunities both for 'outsiders' aiming to steal goods from each company, and for company staff intent on doing likewise. Problems are exacerbated to the extent that both Currys and Dixons trade in some of the most 'desirable' goods available in the market place: items which are of high value (but not as easily traceable as many other high value goods like jewellery), many of which can be easily concealed on the person (especially tapes, films, batteries, etc.) and which can either be used for the thief's personal enjoyment or can be readily sold to others.

The problems are wide ranging. For example:

* burglary risks are high: not only at high street branches, but against 'out of town' warehouses, stock centres, and superstores.

* shoplifting is a problem, particularly in high street locations: although smaller stock on open display is vulnerable, larger items can also be stolen. As well as the theft of stock, the branches are at risk from all the fraudulent activities well known in the high street: cheque and credit card frauds, frauds against their own credit arrangements, etc.

* another problem, shared in equal degree with other retailers, is staff theft (both of cash and stock). In several respects the scope for 'backdoor theft' is greater than that in other, larger, shops — both because of the absence of extra 'layers' of senior management on site, and because of the high degree of autonomy vested in branch managers (to match prices being offered by other high street competitors, for example).

* lorries carrying high value loads from the warehouses have to be protected against hi-jack as well as staff theft. In addition, smaller vehicles delivering goods direct to customers can be subject to attack or to 'tailgate' thefts when drivers are making deliveries.

* staff in certain areas can be subject to threats of violence by youths. Less frequently, they experience actual violent attacks either in the branches themselves or when banking the day's proceeds.

In short, the problems faced represent an amalgam of those experienced — to a greater or lesser degree — by other retailers. Yet despite the frequency with which crimes are reported to the centre, neither company is able to attribute more than a small proportion of their total losses to specific instances of theft: a problem shared alike with others (see Home Office, 1986). The lion's share remains 'unexplained'.

Crime Recording

A recurrent theme in this report is that the principles of 'crime analysis' should not be restricted to *known* instances of crime. It is clearly important to draw as much information as possible from those cases that do come to light. But to achieve a more complete picture, the process should encompass specific investigation or research in areas where crimes are likely to be under-recorded.

All incidents of crime that do come to notice in Dixons or Currys are reported by 'phone to the Security Departments located at the head office of each company. Details are recorded on 'Security Reports' and circulated to relevant parties — including stock audit (for adjustment of branch stock), insurance companies and the security officers located in each region (who will investigate).

The introduction of security databases, aimed specifically at improving each department's facility to perform crime analyses, required that these reports should be entered direct into a computer. One of the priorities was to ensure that — instead of simply extracting the 'bare bones' of each incident to meet the direct needs of audit, investigating officers, and so forth — considerably more detailed information had to be elicited from those with direct experience: the branches themselves. To meet this need, 'menu-type' programmed have been developed which broadly mean that — rather than completing a pre-printed form, akin to a police crime report — those receiving reports pose a different series of enquiries depending on the characteristics of the incident that is being reported[1]. The assumption that separate types of crime have to be singled out and subjected to specific enquiry is axiomatic to crime analysis procedures: this is simply because potential criminal activity — in any environment — is so wide-ranging that incidents have to be separated if meaningful enquiries are to be made about each. Another underlying principle of this system — and an important one in developing similar databases — is that information that might direct future policy or action *has* to be elicited immediately from the victim (or his closest representative) or it is effectively 'lost'. (A more detailed description of the configuration of the system is provided in Appendix 1.)

Chapter 4 discusses the sort of issues raised by the different kinds of crime problems outlined in this chapter, and gives an indication of the type of information that might be required to resolve them. Chapter 5 returns to the process of setting up and initiating a crime database.

[1] Thus a report of a break-in prompts a series of questions about how perimeter security was overcome, whether alarms activated, and so on. In contrast a report of a shoplifting prompts entirely different questions about the type of display, the area of the shop from which the goods were taken, suspect details and so forth.

CHAPTER 4: DEFINING THE PROBLEM

The purpose of this chapter is to focus on the first stage of the crime analysis process: to highlight some of the questions which need to be addressed and the information that might be required to throw light on these.

Key Issues

The discussion deals primarily with the analysis of crimes that do come to the notice of the retailer. This does not, of course, mean that such statistics are intrinsically the best source of information: in most instances, stock control data is likely to give a more comprehensive account of what has been lost and will be a more desirable substitute. On the other hand, it is appreciated that in many retail companies stock control data are not yet sufficiently detailed to identify either specific areas of loss, or to separate crime losses from those produced by poor administrative procedures.

This said, the question of whether recorded crime statistics give an *accurate representation of true levels of crime* should be paramount. Each retailer is best placed to judge this question for himself. Retailers records of burglaries, for example, are likely to be reasonably accurate: simply because entry to retail premises will generally be forced; the resulting damage will require repair; and the administrative requirements for audit will demand a record of any stock stolen (a stark contrast to domestic burglaries, for example, which are significantly under-recorded in police statistics: see Hough and Mayhew, 1985). In contrast, cases of shoplifting are likely to be under-recorded. This may happen to a limited extent in smaller, closely supervised, retail environments (such as those where counter service is provided) or those where electronic article surveillance (EAS) systems operate and may deter. At the other extreme, shoplifting may be grossly under-estimated in larger stores selling smaller, easily concealable merchandise.

It will be noted that the discussion that follows frequently refers to the need to collate details of *how* particular incidents were carried out with details of the *environment* in which the incident took place. For example, to derive appropriate preventive strategies, it is important to know whether the type of goods merchandised, the displays, or the supervision levels in certain sections of a department store make them more vulnerable to theft by customers.

In practical terms, this information may be collated in one of two ways. The necessary environmental details can be elicited each time an incident is reported: a solution which may be necessary when the targets 'at risk' are too numerous to be conveniently categorized or are mobile (such as company vehicles). Doing this, however, can prove time consuming and less than comprehensive. Alternatively, the environmental or descriptive detail of each target 'at risk' (i.e. different levels in a department store, different types of vehicles on a distribution network, and so forth) can be collated and recorded in advance. The latter system has been employed in the Dixons Group database where all incident reports are filed with reference to a branch number: the computer is then able to link these to a comprehensive 'inventory' — held within the database — which records key details about the layout, design and security features of each store.

Another basic, but nonetheless frequently overlooked, consideration is that recording systems should log all attempted offences (i.e. those that proved unsuccessful) as well as those that led to loss. Although it is notoriously difficult to gauge the impact of preventive action (for how can one measure something that hasn't happened?), the ratio of attempts to completed offences provides one useful indication. It follows that systems should provide facilities to record what contributed to the failure of any criminal incident, so that the strengths of existing procedures or barriers are properly identified.

Defining the Problem

The sections below set out some — but certainly not all — of the issues that an elementary system of crime analysis will need to address. Needless to say, there is a common core of questions which will need to be raised in all circumstances: such as details of when and where the incident occurred, the amount of loss or damage, or details of any suspects. These questions are not reiterated under every heading: they are nonetheless raised in places where illustration of their different use might prove instructive.

Burglary

Retailers spend large sums aimed at protecting their premises overnight and at other times when they are not trading: expenditure is directed not only at 'perimeter' protection (like grilles and alarm systems) but also at more costly services (like external CCTV or guards). Analysis should be aimed at evaluating the benefits derived from such expenditure, identifying systems or procedural practices that may reduce risk, and at deriving lessons for future development. The questions might include:

* When do incidents occur?

Alarm systems can provide a reasonably concise record of when burglaries occur. Where stores are frequently attacked, establishing an appropriate preventive strategy can depend heavily on identifying high risk times: for example, unsophisticated attacks committed around pub closing times might indicate a need for the provision of guards at this time. The information is likely to be essential if police surveillance or intervention is required (indeed more sophisticated attacks may often be carried out to coincide with times when local police shifts change!).

* How was entry effected?

Information should be elicited with a view to identifying the weak spots of the exterior of each store: at a certain cost, protective devices are available to reduce each and every vulnerability. Any additional expenditure should be directed by proper reference to known loopholes, rather than on a 'chance' basis.

* What was the contribution of existing security hardware?

Equally, existing hardware needs to be evaluated: if this failed, did it do so because of 'operator failure' (for example, shutters being left unlocked) or because the hardware was subject to a type of attack or level of force it was unable to deal with? One points to the need for training — or the design of 'failsafe' locking procedures — the other to more stringent standards on equipment.

* Did alarms operate properly?

While it is important to examine alarms as part of the general security hardware, it is equally essential that 'false' activations should be properly analysed[1]: if only because it seems sensible to assume that the police will be unlikely to respond with equal speed to activations on systems known to have been faulty in the past.

This aside, most retailers will appreciate the difficulties involved when the police refuse to provide continuing cover, as well as the associated cost (of the restoration of this cover, continuing to meet insurance requirements in the interim, etc).

* What was the cost of each incident?

In the case of burglary, the cost of repairing damage (and providing interim cover) can sometimes outweigh the losses of any stock. Any assessment of alternative means of protection should include consideration of repair costs.

* Are incidents opportunist or well-planned?

Although judgments are bound to be subjective, the details outlined above should contribute towards a reasonable assessment about what type of preventive action is called for. Opportunist offences could perhaps be prevented by better lighting, the removal of more desirable stock items from shop windows at night, or by similar straightforward remedial action. Well-planned attacks may require the installation of more sophisticated equipment (such as CCTV recording facilities triggered by alarm activations) aimed at physically identifying the perpetrators.

Theft by Customers

There is a considerable body of research that has established that many more people take things from shops than is commonly assumed. 'Following studies' — where

[1] Typically, some 97-99% of alarm activations recorded by police forces are classified as 'false'. Although it is impossible to provide an accurate breakdown of the causes, it is generally accepted that roughly 40% of false activations are due to operator error, a similar proportion to system failures, and that the remaining 20% are attributable to non-criminal incidents (e.g. drunks leaning against a window!).

shoppers have been followed at random to see if they pay for the goods they remove — carried out in the US have indicated that between 1 in 7 and 1 in 15 remove items without payment[2] (see Astor, 1969 and 1971). The only comparable study in the UK (Buckle and Farrington, 1984) suggests a lower figure — 1 in 56. Nonetheless, when considered in the context of the number of shoppers visiting a retailer during any one day's trading, even this lower figure has serious implications.

First and foremost, the research, implies that the number of arrests of shoplifters made by retailers represent the tip of the iceberg. For these reasons, the lessons derived from recorded incidents should be treated with caution. Equally, it suggests that the losses many retailers attribute to shoplifting may be grossly under-estimated: even though the value of stolen items recorded in 'following studies' has proved relatively low. In the Dixons Group, it has been necessary to carry out specific data collection exercises to try to gauge the true extent and characteristics of shoplifting offences.

Various experiments have been carried out, using different methods, at branches chosen to provide a reasonable representation of the chain as a whole. One of the most effective methods has been to inconspicuously label goods available on open displays (using different markers to denote different types of merchandise, and means of display) and require sales staff to remove and log these labels when making sales. Regular counts of the goods on display are then compared with the sales records. Although it requires careful planning and supervision (and strict discipline amongst staff in participating stores) these exercises serve to identify what types of goods are stolen, the specific times when goods disappear, and which displays are most vulnerable. Other methods might include balancing till-based sales data against stock audit counts (a method which might not satisfactorily exclude 'staff' thefts) or drawing on the lessons provided by known shoplifters (see, for example, Price Waterhouse, 1986 or alternatively the methods used in Bennett and Wright's interviews with burglars, 1983).

The second major lesson from research is that one long-established means of preventing shoplifting - the provision of plain clothes store detectives - is only likely to have a limited impact on the problem. The 'following studies' have repeatedly shown how few of those removing items without payment are actually seen by store detectives (Astor 1969 & 1971). There is, in addition, the danger that the presence of detectives can allow ordinary staff to 'switch off looking for crime. Finally, Ekblom's (1986) study of shoplifting in the HMV shop in Oxford Street (a store which at that time employed the greatest proportion of store detectives — per square foot of sales space — in this premier shopping area) has served to demonstrate the limited returns detectives can achieve. Even on the lowest estimates of the total number of shoplifters (and assuming the peak efficiency of store detectives in processing each arrest), he suggested that this particular store would need to employ 17 times its usual number of store detectives to have a capacity to arrest all the shoplifters likely to enter

[2] The word 'theft' is avoided quite deliberately: as Murphy (1986) points out, theft requires 'intent' and the courts decide this.

the store on any day. This points to the need both to augment store detectives' contribution, either by increasing their visibility (posting notices or deploying them as uniformed guards) or by raising staff awareness of the problem; it also underlines the importance of looking at alternative preventive strategies, such as store layout and display methods.

Important questions are:

* Which merchandise is stolen most often?

This is the most fundamental question and answers will generally have to be provided by stock control exercises. It is likely that experimentation is necessary: for even the most rigorous stock control system (for example, one that was able to isolate theft losses from 'other shrinkage') would be unable to separate any losses attributable to staff theft from customer thefts.

* Where do losses occur?

Are specific areas of the shopfloor particularly vulnerable? If so, attention should be focussed on why this is the case (prevention might hinge on the removal of an obstruction that impedes observation, means of 'rechannelling' customers through the shop, etc). Alternatively, particular types of display may suffer disproportionate losses and may require design modification. In clothes shops, fitting room procedures deserve repeated scrutiny.

* When do losses occur?

Rates of loss are likely to fluctuate at different times of the day or days of the week: these may prove to be times when staff are stretched (Bank Holidays, Saturdays or times when children leave schools and 'pour into' local shops) or when staff/customer ratios are at their lowest. More vulnerable displays may need to be specially protected (or removed) at these times.

* Do different methods of merchandising affect rates of loss?

Alternative methods may be found for displaying vulnerable goods. Experimentation can establish simple rules: for example, whether audio tapes sold in different pack sizes suffer different risks, or if clothes hung from hangers facing different ways are less likely to be removed 'en masse'. At a more sophisticated level, new designs can be tested: for example, smaller items may be less vulnerable if sold from custom-built dispensers rather than open 'bins', or if they are given a large card backing.

* Can methods of stealing be distinguished?

If widely practised methods of stealing can be identified (either from store detectives records or by specific observation), these should at least be brought to the attention of staff. Other obstacles can also be put in the way of the thief. If price labels are removed by thieves, then this needs to be made more difficult. 'Bag parks' may be necessary to combat thieves who use their own bags; or bag sealing methods used if thieves make legitimate purchases only to secrete additional items in the retailer's own bag.

Theft by Staff

Retailers have long debated how far their theft losses are attributable to customers or staff. While police statistics for 1986 show that average loss for each theft by a customer is much *lower* than those from staff thefts (see Home Office, 1986) — and that the total known losses from 'employee theft'[3] far outweighed those from customers — nearly all observers recognise that these figures may be totally unrepresentative of the huge numbers of offences that do *not* come to retailer's notice (or even of those that are dealt with internally by retailers). There is no reliable means of establishing the appropriate balance. While undoubtedly those seeking to prevent crime should recognise the wide range of opportunities which staff may have to steal, it should not be assumed that losses will therefore automatically outweigh those inflicted by sheer numbers of shoplifters[4].

Staff integrity should of course feature as the central tenet of preventive action. But to achieve this aim, thought has to be given to devising foolproof systems for controlling stock and cash — systems that will not only avoid offering staff the temptation to steal (thus keeping 'honest staff honest') but provide the means of identifying those who submit to the temptation. Apart from implementing systems checks, most large retailers rely on: pre-employment reference checks; fostering high staff awareness through training and the maintenance of clear rules; and establishing procedural practices — from enquiries by regional security staff, 'test shopping'[5], to staff searches — aimed at identifying wrongdoers. Underpinning this effort, it is important to ensure that those frauds or thefts which do come to light will not be viewed as isolated instances, but as an indication of loopholes that others are bound to have found and exploited. As such, they should be removed.

* Who committed the theft?

Information on the age and sex of known offenders can be put to a variety of uses: it might suggest that the company should ensure a particular mix of employees at each department or shop (so that high risk groups are better supervised); it could suggest

[3] It should however be noted that the offence of 'employee theft' (Home Office Category 41) also includes theft by employees outside retailing; set against this, it excludes frauds committed by employees.

[4] Calculations made by Peter Berlin from the 1986 Price Waterhouse Shrinkage Survey of US retailers (Price Waterhouse, 1986b), for example, suggest that for employee thefts to outweigh customer thefts, the dollar value of each employee theft would have to be 20 times greater than those per shoplifting incident. Berlin thought this was improbable. This estimate was however based on retailers' subjective assessments of the proportion of employees and customers who stole goods (calculated at 6.7% and 45% respectively).

[5] Test shoppers are commissioned by many retailers to visit them various outlets — as normal (or even difficult) customers — and to report back on the service they received and the standards they observed.

the need for more thorough pre-employment screening of particular groups; it might even need to be considered in formulating a company-wide employment policy.

* How were goods removed?

The methods by which goods are removed can vary widely: for example, stock may be hidden in clothes or bags when staff leave at the end of the day, may be secreted outside the premises (for example, in rubbish) for later collection, or simply removed by those who could appear to be performing 'normal' duties (such as helping a customer to his or her car). Each requires different safeguards.

* Do incidents involve collusion with 'outsiders'?

Separate provision may be required to monitor thefts by this particular means. They can range from the relatively simple — for example the friend of the salesman who receives additional goods to those legitimately purchased or any other favours (discounts, the 'replacement' of goods bought elsewhere, etc.) — to the more audacious: such as the deliveries which are dispatched to a bogus customer via a particular carrier, Checks and balances may be required to counter them.

* When did theft(s) take place?

As the point above suggests, it should not be taken for granted that staff will only steal at their departure each evening. Times when staff take lunch or tea breaks may figure regularly — or particular days (such as those when the manager or cashier are away).

* Were efforts made to 'cover' for the stolen goods?

Not infrequently, those carrying out thefts (particularly if they are in a position of authority or intend to continue the practice) will attempt to conceal the loss in order to avoid inevitable enquiries when their branch or department is next audited. Identifying the means by which they do this (for example, by claiming particular items on a delivery never arrived) can prove to be an invaluable means of detecting other offenders.

* How was cash taken?

Just as with the theft of stock, there area variety of means — each involving different degrees of sophistication (or levels of access to the till) — which can facilitate the theft of cash. Indeed the simple removal of cash is probably the least attractive, given that the failure to 'balance the till' at the close of business should prompt immediate investigation. Details of each method — from the underringing of a purchase to the more complicated transaction (such as those involving credit agreements etc.) need to be collated.

Theft through Distribution Networks

Merchandise moving through any retailer's distribution network is subject to a range of threats: from short warehouse deliveries by suppliers to vehicle thefts. In general terms, the threats can be sub-divided into two main types: threats by 'outsiders' (which can either be in the form of burglaries of warehouses and other stock holding centres, or thefts from vehicles) and those by staff (those working in warehouses etc. or those manning vehicles).

There are a number of factors that tend to make the distribution sector particularly vulnerable to theft. First, goods in transit are inevitably protected by fewer physical barriers than those in fixed premises. Indeed, given that warehouses are generally situated well away from residential areas or main thoroughfares, they are probably themselves more vulnerable than high street stores. Second, drivers and others handling goods in transit are subject to less supervision — and thus face greater opportunities to steal — than their counterparts elsewhere.

Probably the main factor, however, is that difficulties can be faced in establishing accountability at all stages of the distributive process. One of the cornerstones of any preventive strategy must be to determine precisely who is responsible for what stock at any one time. Difficulties arise where goods are checked into vehicles inaccurately, where a driver may be required to make multiple 'drops' and others may need to have access to 'his' load, and if deliveries are not checked off the vehicle at the time they are received. There can be similar difficulties establishing accountability in warehouses themselves, particularly if they are asked to act as 'holding' bases for stock that has been transferred to the books of the retail outlet: unsuccessful deliveries, damaged goods and so forth. In short, procedures and controls must be exacting.

* Do procedural loopholes encourage staff theft?

In view of the difficulties outlined above, special attention deserves to be given to the 'inducements' faced where staff — particularly drivers — are known to have stolen goods. Providing drivers with stock that is plainly *not* accounted for by stock handling procedures — for example any stock which has no accompanying paperwork — is clearly offering an unnecessary temptation to steal.

* What is the backgound of the offender?

Apart from the criteria of routine significance (age, sex, etc.), length of service may be important. Temporary drivers are frequently needed to meet unanticipated demands in distributive activity. But, given that losses may not be identified immediately, the inducement to steal is particularly attractive to the 'temp'.

* Where do vehicle thefts occur?

Information is required at two levels. Clearly it is necessary to establish if vehicles operating in particular *geographical areas* of the country are subject to unusual risks.

At another level, it is important to ascertain if particular *stages* of the driver's routine prove more hazardous: such as overnight stops or times when vehicles are left unattended for customer deliveries.

*How and when are such thefts committed?

These sort of details should dictate preventive action: needless to say, the response to attacks on vehicles parked overnight in a 'secure' enclosure will be quite different from those against drivers and their crews who are making deliveries.

Violence to Staff

Although the actual numbers of violent crimes committed against those in shops, and other elements of the retail trade, are probably small (there is no reliable means of establishing numbers), many shop staff are familiar with incidents which the police will classify as 'intimidation': from the threat uttered by the dissatisfied customer, to the crowd of youths who openly steal goods knowing their numbers will prevent anyone intervening. At a more serious level, retailers can experience problems when dealing with customers caught stealing. They also share the risks experienced by anyone who has to routinely handle and transport valuable goods or large quantities of cash[6].

A recent report by the Health and Safety Executive on the subject of violence to staff (Poyner and Warne, 1987) has strongly recommended the use of crime analysis methods in tackling these problems. Although the main recommendations of this report are aimed at those staff subjected to greatest risk (such as those working in licensed premises, or on buses) it is nonetheless important that retailers should establish a means of collating basic details about violent incidents. In doing so, it is advisable to define what constitutes violence in order to establish concise guidelines about *what* should be reported. Unless this is done, there is the danger that standards will vary and those in locations where violent abuse and threats are relatively more commonplace — such as poorer areas of the inner city — will see little justification in reporting 'minor' incidents. Alternatively, the issue may require systematic enquiry amongst staff in areas deemed to be facing greatest risks.

Some key points are:

*Who hit/abused whom?

What correlation can be drawn between the aggressor and his/her victim? Were these of the same — or widely different — ages, the same sex or ethnic background? Did they know each other in any way?

[6] Indeed there is a school of thought that retailers are increasingly subjected to violence because banks and other major cash handlers have done so much to protect themselves from attack

* What led to the incident?

If there was a dispute that triggered the incident, what was this about: complaints about goods, about the service provided — or did staff perhaps try to intervene and prevent a suspected shoplifter? The information can either point to recommendations for reducing 'friction', or perhaps better training in handling difficult incidents.

* What was the level of violence?

This information is essential to establish the seriousness of the problem. Linked to data about where incidents occur, it could point to the need for better protection, more effective means of summoning assistance, or simply the deployment of 'bigger' staff at regular flashpoints.

This chapter has deliberately focussed on the type of information that might be required to perform detailed crime analysis. It has not sought to provide a comprehensive review of information requirements: these will vary considerably according to the characteristics of each retailer. If the list nonetheless appears formidable, it has to be borne in mind that these requirements can be tailored, and that the recording — and subsequent analysis — of details of any incident can be done speedily if these are entered directly into a computerised database. The main argument against restricting data collection is a practical one: details not committed directly to record are not easily recalled when their relevance becomes more apparent (those reporting incidents forget, or cannot be traced). Moreover the value placed on recorded incidents should take into account the fact that these will often represent a small proportion of other similar, and perhaps even more costly, incidents which go unnoticed.

Little emphasis has been placed on the *solutions* which might result from crime analysis. This is primarily, of course, because this report has aimed to suggest the type of information required to address problems, but it also reflects the fact that there is a sizeable literature and a number of periodicals which offer ways and means of combating retail theft (see, particularly, Home Office 1983a). But whereas ideas are not in short supply, it will often require major changes to establish that crime problems deserve to be the subject of analysis. The principal contribution of crime analysis — as Ekblom (1986) has pointed out — is to offer guidance as to *which* of the wide range of ideas, security products or services (most of which are well known to those in retailing) are appropriate *in which circumstances*. In short, the process is primarily aimed at selecting the area, times and circumstances where preventive action should be directed.

CHAPTER 5: ESTABLISHING A SYSTEM

This chapter offers a few words of practical advice to those retailers wishing to develop systems that will record and collate data of the sort outlined in Chapter 4. It then suggests that crime analysis systems need not only be restricted to dealing with those crimes that have come to the retailer's attention, but can be enhanced to take into account 'inferential' data that might identify hidden crime.

Data Collection and Analysis

Although there is a growing body of literature recounting the lessons learnt from either *retrospective* analysis of crime records (see, for example, Laycock's 1985 study of burglaries recorded by the police) or specific *one-off* surveys (e.g. Smith's 1987 survey of hospital employees), little attention has been given to ways and means of establishing systems that *routinely* collect and process the sort of detailed information that is required. Indeed, the first generation of crime analysis systems developed by the police has tended to rely on the reappraisal of data collected with other purposes in mind[1]. Establishing a system capable of receiving and processing a substantial amount of information on a day to day basis imposes different requirements.

Systems will almost certainly need to be computer-based where the details of crime incidents have to be subject to routine, but not necessarily standardised, enquiry. Data capture may either involve staff entering details of crimes — as they are reported — directly on to a computer, or by the more lengthy procedure of encoding and then entering existing paper reports. Either way, the advantages of computer-based systems — which allow the analyst to reassemble data in a different format, to compare different data sets or variables against each other, and so forth — are important if the process is to successfully identify patterns or trace causal relationships. The falling costs of personal computers makes this a feasible alternative for even the smaller retailer.

Chapter 3 highlighted two major priorities for any system if it is to be capable of performing routine crime analysis:

(1) to obtain information from those with a close knowledge of the incident *as quickly as possible*. Direct entry of information to the database is certainly a useful means of achieving this.

(2) the need to cull *detailed* information about each incident and to design *different enquiries* for different types of crime.

[1] The primary constraint on the police is of course that they have first to meet the legal and statistical data requirements set by the Home Office and other agencies: this should not however preclude officers directly providing information that can be used to shape preventive strategies. The implemention of the Metropolitan Police's Crime Report Incident System (CRIS), which will provide facilities to analyse crime reports at some 2,000 terminals located in London's police stations, will represent the largest scheme aimed at utilising this information in an operational role (see Police Review, 1987).

A detailed guide to the techniques of collecting crime information and analysing it for patterns has been produced by Ekblom (1988). Nonetheless, there can be no blueprint capable of meeting the individual needs of all retail stores. Those who choose to adopt approaches used by others should ensure that systems can be modified or expanded to meet their own particular requirements. In this sense, each retailer has to develop a *prototype:* unless the planning and introduction of the system (and the training of those involved in its use) is progressed meticulously, it is judicious to expect the teething problems associated with any new arrangement. At the very least, it is important to maintain tried and tested paper-based procedures for recording crimes until such a time as the new system has been subject to extensive trials (or to run these side by side for an interim period).

Formulating a System Specification

The starting point for any development is a comprehensive specification, detailing what the system is designed to achieve, how this will be done and the expected payoffs. This is an important stage even for systems which are likely to involve little change in operating procedures (and which are not going to be the subject of critical questioning by the finance director approving the expenditure!). It assumes even greater significance as the number of interested parties grows (from those reporting and recording incidents, to the recipients and users of the system), more radical changes in established operating procedures are envisaged, or if any software development is to be sub-contracted out. In these circumstances, the user needs to be precise in specifying details such as what will be required from those registering and receiving reports, computer response times, installation dates and so forth. This specification should be the subject of a detailed consultation exercise before it is finally approved.

The key issues which should be considered in drawing up a specification are considered in Appendix 2. These include:

What information is needed and what value will it have?

How should each incident report be structured?

What will reporting procedures be?

What performance criteria are required from any computer?

Extending the Scope of Crime Databases

Retailers devising databases, like police forces engaged in the same exercise, may have good grounds for suspecting that the crimes they record are not a true reflection of those that do *not* come to their notice. They may also feel constrained in that, although a crime analysis system will provide a much more reliable means of developing future policy, it may not be an effective means of pinpointing where they may *currently* be subject to fraud and theft.

Systems can, however, be enhanced so as to highlight areas that require immediate investigation. Police forces do this by developing crime intelligence systems (through the office of the divisional collator) to help them engage in proactive investigation rather than reactive — fire fighting — activities. Retailers, too, can follow this lead and supplement data about *known* crime with that which *might* provide indications of criminal activities. Just as police intelligence systems demonstrate their principal advantages in a finite area — namely in matters affecting those whom they have previously dealt with (i.e. offenders and suspects) — the main strength for retailers is in investigating malpractice by staff.

It falls beyond the remit of this report to discuss this dimension in detail. One or two examples can however help illustrate the sort of approach envisaged:

* One of the main indicators that something may be awry (although not a precise means of indicating *where* the fault may lie) is that the profit margin of a branch or department is falling below the normal, or its own previous, level.

* Another may be that the 'stock turn' is declining: in other words that the sales achievement of any unit does not match the deliveries it has received. Investigation may indeed reveal that stock is building up: alternatively, the additional deliveries may have been organised to sustain substantial thefts.

* Numbers of 'till reversals' may be another important indicator. Although it is necessary to provide a function on the till to cater for stock which is returned by customers, it can provide an opportunity for staff to buy back fictitious stock and pocket the refund money.

* Patterns of 'delivery discrepancies' could also be important. Again, most stores require a means of notifying a warehouse of any shortfall or extra stock they may have received, but there is again a possibility that bogus reports can be raised — which will enable staff to conceal a theft. Alternatively, the absence of any discrepancy reports may indicate another problem: that stock is not being checked at all, or that 'extras' are noticed but not reported.

In short, the aim is to investigate 'exceptional' trading patterns that might reveal theft or fraud.

It is always important to maintain a strict demarcation between known crimes and indicators of possible criminal activity like these. However, provided this is done, the data can be integrated into one system, and the same principles can be applied to the assembly and analysis of data. Information gained from stock audit systems (for example, about areas of highest shrinkage, products most liable to be lost etc.) should be drawn into the analysis. In addition, retailers should be keen to exploit to its full potential the information that can be derived from electronic point of sales (EPOS) computers — for example about till voids, discounting procedures, etc.

CHAPTER 6: SUMMARY

Crime analysis techniques have been strongly advocated as central to modern policing. They are a means of making the most efficient use of an expensive public resource (Home Office, 1983b) and can prove to be an essential tool in targetting preventive action (Joint Departmental Circular, 1984). The value of this approach has been demonstrated in a series of diverse situations, and the lessons apply equally well to retailers considering how to tackle their own crime problems.

This report has sought to provide practical advice to assist those retailers who wish to apply these techniques. By doing so retailers will be in a stronger position to identify the precise nature of their crime problems, to explore how these might be tackled, and to assess the effectiveness of remedial action they might adopt. The need for this sort of approach is the more pressing given that there are severe limitations to some security practices adopted in retailing — such as the arrest of shoplifters and their referral to the police — but also because of the potential payoffs offered by detailed reappraisal of administrative or procedural practices, or by the glamorous technological systems on offer in the market place.

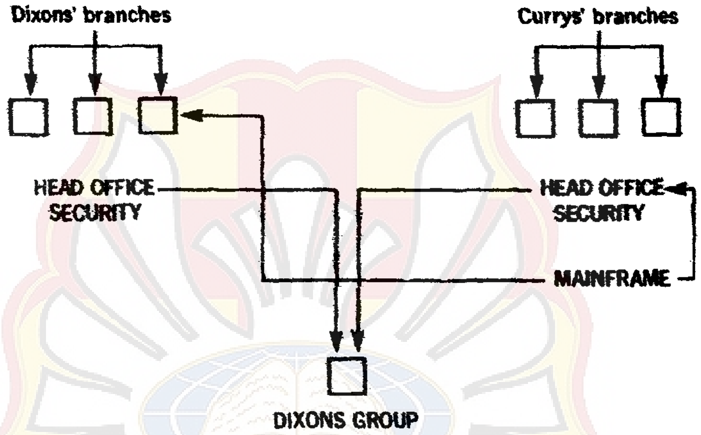
The message offered is, in many respects, a mundane one: security considerations should be subject to the same standards of rigorous analysis as other aspects of retail management. The collection and analysis of reliable information on security issues is an important first step in this direction.

APPENDIX 1

DIXONS GROUP DATABASE

The broad structure of the security database operating in the Dixons Group is laid out below:

(a) Hardware configuration



The day to day operating procedure is as follows:

1. Individual branches telephone through details of any crime to their respective head offices.

2. Security department staff receive these calls on any one of a series of workstations (networked together) and put to the branch staff the relevant enquiries which are fed to them by the software programme (see below).

3. Each company system operates as a 'stand-alone' entity, capable of taking in reports, producing printed summaries, producing routine analysis and of special interrogation. (In time, other Dixons Group companies may adopt similar reporting procedures).

4. Data from both companies is downloaded onto a central Group computer (for analysis of inter-company patterns, overall trends, etc.)

(b) *Software*

There are two major components to the data system:

1. *The security report.* A set of menu-driven enquiries which pose questions to those reporting criminal incidents.

2. *The branch database.* A file providing details about the environment, physical design and protective devices of each branch (or warehouse).

These two files are capable of being interrogated alone (e.g. to establish how many burglaries of a particular type have been committed in a specified period) or in tandem (e.g. to establish how many occured in specific locations).

The crime file is obviously in most frequent day-to-day use. The screen enquiries record details of where and when all incidents occurred; the type of incident and the methods used by the offender (there are different questions according to the incident 'type'); the details of property stolen (here direct access to mainframe product lists speed up recording); a short precis of events; details of suspects/offenders and what follow-up action is required.

The branch database requires less frequent update. In addition to information about fixed premises (encompassing details of security hardware in use), it also incorporates details of branch personnel and assembles trading details that can provide possible indications of criminal activity: for example, stock audit results, till discrepancies, etc.

APPENDIX 2

KEY ISSUES IN DEVELOPING A SYSTEM SPECIFICATION

Central points are:

* What information is required?

The step by step approach that was discussed in Chapter 4 will help to identify the ideal information requirements for specific types of crime. This process can be assisted by 'sample searches' of existing crime reports to identify likely sub-categories of data: thus every 'Xth' burglary report can be scanned to see the main points of entry, the main methods of entry, etc.

The danger of this process is that it can yield many more data 'fields' than the respondent (the person reporting the crime) can reliably provide and the system can process. While it is important not to reject information that might point to innovative preventive strategies at an early stage, the next important question therefore is to assess the *feasibility* and *reason* for eliciting that information from the respondent. If the respondent is only likely to be able to provide reliable information in selected cases, there is no reason to collect it: here it is often useful to apply the computer analyst's 'GIGO' dictum ('garbage in, garbage out'). Equally if, once collected, users cannot foresee to what use the information will be put, it should be discarded.

* How should each incident report be structured'?

Decisions about the format of each crime enquiry should be influenced by the type of crime the retailer mostly experiences; by current methods of handling reports, with which staff will be familiar; and by direct experience of the way in which those reporting criminal incidents typically recount what has happened.

Taking these priorities separately, it is clear that the reporting format should aim to encompass most, if not all, criminal incidents affecting the retailer: only a small minority should fall outside these categories. In most circumstances, the main headings will be broadly similar (encompassing shoplifting, theft by employees, burglary, incidents involving violence) but sub-categories may vary widely according to each retailer's requirements (for example, thefts by staff may be sub-divided to distinguish theft of goods, of cash, etc; or to distinguish those committed by shop floor staff from those by distribution staff; or to separate those committed by staff of different rank, etc).

Reference to earlier means of reporting is essential to avoid misunderstandings that might arise if different meanings are applied to similar labels or terms, and indeed to enable comparisons to be made between reports on a new system and those recorded before its introduction. Finally it is axiomatic that reports should attempt to start at the logical 'beginning' (when and where did the incident happen?), fill in details of what happened, and end with details of any suspects arrested, how they were dealt with, etc.

For the purposes of subsequent analysis, the reports should of course attempt to allocate as much information as possible to pre-coded fields. This is unlikely to eliminate the need for a narrative section where the 'story can be told': indeed some software programs now provide "free text retrieval" package to enable users to search such narrative accounts for common words or phrases. The need for the expansion or modification of pre-coded fields should also be borne in mind: not only because users are likely to identify data categories initially overlooked, but also because those committing crimes will inevitably adopt new methods to overcome obstacles in their way.

* What will reporting procedures be?

As a general rule, it will be expedient to utilise and build upon established reporting routines, unless these prove thoroughly impractical. Thus any new system that proposes to completely abandon a long-standing procedure where 'reporting' branches or departments of a store are used to completing pre-printing crime reports (and perhaps replace this with a telephone reporting method) is likely to face perhaps unnecessary difficulties (e.g. staff unused to questioning over the phone, etc).

The advantages of asking those reporting incidents to complete a 'boxed' report form are that they are able to cull a more considered assessment of what took place than the immediate phone-in. Moreover, report forms can be expanded or changed at little additional cost; and details can be subsequently entered directly on to 'off the shelf' spread-sheet computer programs (like Lotus 123). The disadvantages are that questions posed on a pre-printed report can be liable to different interpretation, and that — unless lengthy and very complicated — they cannot embrace the amount of detail that might be requested by someone operating a computer at the other end of the phone. Here software programs can be written for the operator to be guided to different questions according to the nature of the incident that has been reported (see, for example, the Dixons Group system described in Appendix 1).

* What volumes of data will be held on computer? What performance criteria must be met?

In assessing the hardware needs of any computer system (particularly the question of whether the system should be micro, mini or mainframe based), the developers need to be aware not only of the amount of information likely to be recorded on each and every criminal incident, but details about the number of cases that the user wants to hold 'on record' at any one time. In addition, the user should specify details of how quickly the system should respond in carrying out particular operations: for example, it is probably essential that response time should be fast when entering details recounted from someone at the other end of a phone, but speed may not be essential for subsequent analysis of reports, etc.

* Do reports have to be circulated?

In most larger retail companies — as in the police service — there is generally a requirement that paper reports of some (if not all) criminal incidents be circulated both to those needing to take action on their contents, and to those requiring them 'for information only'. Copies may be required by auditors (to account for stock loss), by those dealing with insurance (for claims purposes) or simply by senior management who wish to be informed of major incidents.

Inevitably, those who have been used to seeing short, succinct, accounts of criminal incidents will not wish to see much of the more detailed information that is elicited for crime analysis purposes. There is no need for them to do so: the computer software should separate those items of information that are of interest and leave the remainder 'hidden'.

* What analysis should be available?

Again, those developing software for any crime analysis system should be given specific details of what type of analysis may need to be performed. In some circumstances it may be sufficient to provide facilities to identify and list incidents of particular type(s), committed at particular times or locations, etc. In others, the statistical tests and routines available from most social science software packages may be required. Needless to say, there is no use at all eliciting information that cannot subsequently be retrieved and made use of.

* What are the training requirements for system users?

The introduction of a crime analysis system will at the minimum require consultation with, but perhaps formal training of, three groups: those reporting criminal incidents, those recording these, and those likely to utilise data provided by the system.

To deal with each: those *reporting* incidents will need to be advised about how to complete new kinds of reports or that they need to be equipped with more comprehensive details when phoning through a report. Those *recording* incidents occupy a key position in determining the standard of information entered into the computer: they require training on how the system will work, what interpretation to put on different questions, and so forth. A system manual may be necessary to ensure that common conventions are used consistently. Finally, there is little advantage in providing a system that is not fully utilised: so *staff who are likely to benefit from data analysis routines*, etc. available in the system (from directors to regional security personnel) need to be made aware of the facilities and encouraged to use them.

References

Astor, S. D. (1969). 'Shoplifting: far greater than we know?' *Security World* Vol 6, No. 11 pp 12-13.

Astor, S. D. (1971). 'Shoplifting Survey'. *Security World* Vol 8, No. 3 pp 34-5

Bennett, T. and Wright, R. (1984). *Burglars on Burglary: prevention and the offender.* Aldershot: Gower.

Brody, S. R. (1976). *The Effectiveness of Sentencing: a review of the literature.* Home Office Research Study No. 35. London: HMSO.

Brody, S. R. and Tarling, R. (1980). *Taking Offenders out of Circulation.* Home Office Research Study No. 64. London: HMSO.

Buckle, A. and Farrington, D. P. (1984). 'An Observational Study of Shoplifting', *British Journal of Criminology* Vol 24, No. 1.

Burrows, J. (1979). 'Police Car Security Campaign' in Burrows, J., Ekblom, P. and Heal, K. *Crime Prevention and the Police.* Home Office Research Study No. 55. London: HMSO.

Burrows, J. and Lewis, A. (1987). 'Stereotyping Shoplifters'. *Policing* Vol 3, No. 3.

Clarke, R. V. G. (1983). 'Situational Crime Prevention: its theoretical basis and practical scope' in Tonry, M. and Morris, N. (Eds). *Crime and Justice: An Annual Review of Research,* Vol 4. Chicago: University of Chicago Press.

Clarke, R. V. G. and Hough, J. M. (1984). *Crime and Police Effectiveness.* Home Office Research Study No. 79. London: HMSO.

Ekblom, P. (1986). *The Prevention of Shop Theft: an approach through* crime *analysis.* Crime Prevention Unit Paper 5. London: Home Office.

Ekblom, P. (1988). *Getting the Best out of Crime Analysis.* Crime Prevention Unit Paper 10. London: Home Office.

Farrington, D. P. (1981). 'The Prevalence of Convictions'. *British Journal of Criminology* Vol 21 No. 2.

Home Office (1979). *The Private Security Industry: a discussion paper.* London: HMSO.

Home Office (1983a). *Shoplifting, and thefts by shop staff.* London: HMSO.

Home Office (1983b). *Manpower effectiveness and efficiency in the police service.* Circular 114/83.

Home Office (1985). *Criminal Careers of those born in 1953, 1958, and 1963.* Statistical Bulletin 7/85. London: Home Office.

Home Office (1986). *Report of the Working Group on Shop Theft.* London: Home Office.

Home Office (1987). *Report of the Working Group on Juvenile Crime.* London: Home Office.

Hough, M. and Mayhew, P. (1983). *The British* Crime *Survey: First Report.* Home Office Research Study No. 76. London: HMSO.

Hough, M. and Mayhew, P. (1985). *Taking Account of Crime: key findings from the 1984 British Crime Survey.* Home Office Research Study No. 85, London: HMSO.

Joint Departmental Circular (1984). *Crime Prevention.* Home Office 8/1984; DES 1/84.

Mayhew, P. Clarke, R. V. G., Sturman, A. and Hough, J. M. *Crime as Opportunity.* Home Office Research Study No. 34. London: HMSO.

Murphy, D. J. I. (1986). *Customers and thieves: an ethnography of shoplifting.* Aldershot: Gower.

Levi, M. (1986). *The Incidence, Reporting and Prevention of Commercial Fraud.* Unpublished report to Home Office, in conjunction with James Morgan, Arthur Young.

Police Review (1987). 'New Met computer will cut manpower costs.' 28 August.

Poyner, B. and Warne, C. (1987). *Violence to Staff: a basis for assessment and prevention.* Tavistock Institute/HSE. London: HMSO.

Price Waterhouse (1986a). 'Shoplifters evaluate retail security measures'. *The Peter Berlin Report on Shrinkage Control.* April edition.

Price Waterhouse (1986b). '1986 Price Waterhouse Survey'. *The Peter Berlin Report on Shrinkage Control.* April Edition.

Ramsey, M. (1982). *City-centre crime: a situational approach to prevention.* Research and Planning Unit Paper No. 10. London: Home Office.

Shapland, J. and Vagg, J. (1985). *Social Control and Policing on the ground in High Wycombe.* Unpublished report to the Home Office. Oxford: Centre for Criminological Research.

Smith, L. J. F. (1987). *Crime in Hospitals: diagnosis and prevention.* Crime Prevention Unit Paper 7. London: Home Office.

Smith, L. J. F. and Burrows, J. (1986). 'Nobbling the fraudsters: crime prevention through administrative change'. *Howard Journal of Criminal Justice* Vol 25, No. 1.

Walsh, D. P. (1978). *Shoplifting: controlling a major crime.* London: MacMillan.

Winchester, S. and Jackson, H. (1982). *Residential Burglary: the limits of prevention.* Home Office Research Study No. 74. London: HMSO.

Crime Prevention Unit Papers

1. **Reducing Burglary: a study of chemists' shops.**
   Gloria Laycock. 1985. v + 7 pp. (0 86353 154 8).

2. **Reducing Crime: developing the role of crime prevention panels.**
   Lorna J. F. Smith and Gloria Laycock. 1985. v + 14 pp. (0 86252 189 0)

3. **Property Marking: a deterrent to domestic burglary?**
   Gloria Laycock. 1985. v + 25 pp. (0 86252 193 9).

4. **Designing for Car Security: towards a crime free car.**
   Dean Southall and Paul Ekblom. 1985. v + 25 pp. (0 86252 222 6).

5. **The Prevention of Shop Theft: an approach through crime analysis.**
   Paul Ekblom. 1986. v + 19 pp. (0 86252 237 4).

6. **Prepayment Coin Meters: a target for burglary.**
   Nigel Hill. 1986. v + 15 pp. (0 86252 245 5).

7. **Crime in Hospitals: diagnosis and prevention.**
   Lorna J. F. Smith. 1987. v + 25 pp. (0 86252 267 6).

8. **Preventing Juvenile Crime: the Staffordshire Experience.**
   Kevin Heal and Gloria Laycock. 1987. v + 29 pp. (0 86252 297 8).

9. **Preventing Robberies at Sub-Post Offices: an evaluation of security initiative.**
   Paul Ekblom. 1987. v + 34 pp. (0 86252 300 1).

10. **Getting the Best out of Crime Analysis.**
    Paul Ekblom. 1988. v + 45 pp. (0 86252 307 9).