MAKING CRIME PREVENTION PAY: INITIATIVES FROM BUSINESS

John Burrows

CRIME PREVENTION UNIT PAPER NO. 27
LONDON: HOME OFFICE

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

First published 1991

Crime Prevention Unit Papers

The Home Office 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 629 9

Foreword

One of the constantly recurring questions in relation to the promotion of crime prevention is whether the potential benefits warrant the financial and social costs. This report offers a wide ranging commentary on many of the cost-effective initiatives taken by businesses to reduce crime.

The measures range from the simple to the very sophisticated but they each share the common feature of having been developed out of strong management commitment and clear headed analysis of the problems faced. They illustrate that preventing crime can be worthwhile even against the most exacting criteria - many of the examples report hundreds of thousands of pounds saved.

One of the most progressive signs to come from this review is the extent of cross-industry co-operation - many businesses are now working together with their commercial competitors to produce an effective 'industry response' to a shared problem.

If we are to successfully tackle crime at a national level then we must see more initiatives of the kind reported here.

I M BURNS
Deputy Under Secretary of State
Home Office
May 1991

Acknowledgements

This enquiry was entirely dependant on the goodwill of those willing to find time for meetings with me, and their readiness to disclose details of the initiatives they have taken to tackle crime. Thanks are particularly due to the many, very busy, individuals who made time to assist in this way. These included (in alphabetical order); Vic Bassi (Courage); John Boyd and Hammond Coppinger (Digital); Mike Britnall (BT); Tony Burns-Howell (Dixons) Jane Cooper and Helen Reeves (Victim Support); Tim Clement-Jones (Kingfisher); Dermot Davy (Northern Ireland Electricity); Paul Elliott (P and O); Bill Floyd (Sony Music); Mike Fromant and Bob Wooley (Barclays); Ian Harley (Argos); Mike Hoare and Peter Alleman (Post Office); Michael Hyland (Midland); Len Lambert (Abbey National); Ken Lewis and Andrew Hilton (NHLC); Peter Loadman (Royal Mail); Chris Mason (B and Q); James Morgan (JM Associates); Peter Nievans (Hanson); Mike O'Leary (Trafalgar House); Dick Pearson and Cliff Conings (Whitbread); Ivor Rickwood (National Savings); Mike Steers (M and S); David Trower (Lloyds Bank); Gwyn Waters (TAC); Don Williams (Tesco) and Colin Woods (Securicor).

There were many more who, although not necessarily cajolled into finding time for meetings, were equally helpful in affording direction by telephone or letter. Finally thanks go to my friends and former colleagues - especially Gloria Laycock and Kevin Heal at the Home Office and Mike Levi at Cardiff University - who helped with advice on the developing draft.

John Burrows
May 1991.

Contents

1. Introduction

There is now widespread acceptance that the business community has a significant responsibility to prevent crimes to which they, or their employees while at work, could fall victim. This proposition is of course at odds with perspectives of the not-too-distant past, which held that crime prevention was the sole domain of the police. But business has not been alone is assuming the mantle of this new responsibility: over the recent decade there has been growing government, and police, emphasis on the importance that the individual citizen should attach to protecting themselves, and their property, from crime. In both cases official exhortation has been backed by a far more powerful driving force - the self-interest of the potential victim.

This report documents a short, and unstructured, enquiry into a range of crime prevention initiatives adopted by business, and follows in this same tradition. The objective of the enquiry was to identify innovative examples of crime prevention practice within commercial environments and - more particularly - to furnish case studies of initiatives that have demonstrably contributed to profitability by cutting crime losses. It was intended that these could lend encouragement to those who remain sceptical of the ability - or indeed still harbour doubts about the legitimacy ~ of business itself taking action against crime.

Background

Whereas the drive to persuade the individual citizen to protect him or herself from crime has many notable landmarks - in the form of ministerial pronouncements, circulars and campaigns - business has moved to a state of substantial self-sufficiency in crime prevention without much debate or dissension. Inmost medium to large size companies, internal security departments now have a history spanning several decades. Moreover it is commonly accepted that these security practitioners, and the very wide range of security contractors and investigators whose services they draw on, has for some time exceeded the size of the regular police force. There can be no doubt that this reflects a burgeoning demand from business.

There have however been important changes in the nature of the relationship between the police and businesses. Up until the early 1980's, for example, there was a general consensus in governmental circles that the security personnel and services paid for by the private sector simply acted to **supplement** the protection afforded by the police.

The 1984 Joint Circular on Crime Prevention, while focusing entirely on the critical relationship between police and local authorities, marked a watershed. One of its key messages was that "since some of the factors affecting crime lie outside the control or direct influence of the police, crime prevention cannot be left to them alone". By publicly acknowledging the constraints on the police function, self-sufficiency moved one step closer.

Although not addressing business problems or a business audience the case made in the 1984 circular for developing crime prevention **on a local basis** has increasingly characterised police dealings with business. Fostering the view that communities must do more for themselves, the arguments used were that preventive strategies need to be borne out of rigorous analysis of specific crime problems - and that remedies must become a responsibility y of those who can manage, design or change the opportunities that exist for crime to occur.

Businesses, which in a very direct sense create and control the environments in which a large proportion of the working population spend many of their waking hours, have not actively challenged these assumptions. Indeed the mushrooming growth of the security services used by business predated the 1984 circular, which suggests that its principal logic was already being acted upon. And while there have most certainly been bones of contention between government and business on crime prevention issues in the last decade, these have seldom been directly about the boundaries between the workplace and the public domain.

Differences have however arisen. Those occasions where government believes that business activities contribute - directly or indirectly -to crime committed **outside** the workplace, or to unwarranted costs on the criminal justice system, are the most common source of friction. There have been a range of examples in the mid to late 80's. Attention has been drawn to practises by breweries and pub owners that have been held to contribute to drunken behaviour, particularly rowdism in city centres at night (Ramsay, 1982). Considerable pressure has been exerted on motor manufacturers to incorporate improved security devices into cars, and by this means hold in check increases in autocrime (Southall and Ekblom, 1985); indeed, an index of individual models' vulnerability y to autocrime has recently been published. And it has been suggested that the acceptability of some retail practises, which have seemed to present an open invitation to shoplift and have led to unnecessary demands on police time, should be a matter of public debate (Ekblom, 1986).

The growing realisation of the 'interdependence' of criminal activity, and crime prevention effort, in the private and public sectors has, in no small measure, been strengthened by the evidence from the third British Crime survey (Mayhew, Elliott and Dowds, 1989) - the first to enquire specifically into victimisation at work. While it has been widely recognised that those in employment are more at risk from crime than those that are not, much of this was shown to be because of crime at the workplace itself. The survey established, for example, that seven out of ten thefts of workers' property took place at work. These findings have served to underline the point that crime prevention in business cannot be solely treated as the concern of the corporate body affected. Much of the property crime commited against the individual takes place at work and indeed those in employment suffer a good deal of violent crime as a result of the work they do.

Something of this complex interrelationship was evident in the report on business crime prevention produced recently by the CBI/Crime Concern Working Party

(CBI/Crime Concern, 1990). The primary objective of this document was to enhance business efficiency by aiming at the business which has not recognised the losses they could be sustaining from crime, and by making the point that these problems are - like most other business difficulties - manageable. A secondary objective, however, was to promote the social responsibilities that businesses are believed to have to the wider community (albeit, by reminding business that self-interest, too, can be served by a commitment to prevention: that safer communities are a necessity for business to thrive). The latter message explicitly recognised that governments cannot afford to let businesses "go their own way" on crime issues: for, should they do so, corporate profitability will not be the only casualty.

Methods and constraints

The short timescale of this study precluded a systematic survey and instead a selection of major companies were approached directly - by phone or letter - and follow up meetings fixed, when appropriate, to gather details of initiatives.

By the same token, no formal sampling methods were used to dictate which companies should be approached: these were selected by informal contact. Larger companies, with correspondingly larger or more sophisticated risk management functions, predominated. Disproportionate attention was also paid to those sectors - such as the financial services, the retail sector, breweries and some public utilities - with crime problems that are certainly more highly publicised and which, from the evidence of one of the few business surveys carried out (by the Working Group on the Costs of Crime, 1988), are more sizeable. For obvious reasons, although some companies with a direct commercial interest in crime or loss prevention assisted the exercise, they were not invited to submit case studies. A list of the companies and public utilities who were able to assist is in the Appendix.

There were substantial constraints - anticipated from the outset - working against the achievement of the project objectives. Like many other organisations, those in the commercial or industrial sectors have a natural inclination to limit disclosure of non-essential information about their operations. In this exercise, their reluctance to do so was justified under one - or a number of - different explanations:

(i) **Companies voiced skepticism that openness about crime problems could achieve anything positive and corresponding concern that it could risk alerting potential criminals of their vulnerabilities, or earn the opprobrium of shareholders and the City.**

The latter concern - put simply, that those who sustain losses from crime believe this will be interpreted as a sign of mismanagement - is widely recognised: it emerges as the primary reason cited by financial services companies for not reporting fraud to the police (see Ernst & Young, 1989).

To the extent that many companies did show a readiness to disclose details of their crime losses (although generally after they have been tackled successfully) it is a welcome sign that this view was not universally held.

(ii) **Concerns were registered that publicizing the details of precautions taken against crime could render them invalid.** This is naturally quite legitimate particularly in the case of the more sophisticated or elaborate security controls.

(iii) **Some believed that disclosure could reduce the competitive edge they had achieved by effective precautions.** This argument is closely allied to that above. The few companies employing it believed they had achieved competitive advantage in overcoming problems faced by their sector by some effective defensive strategy or mechanism.

(iv) **Finally, and most obviously, many companies - though content with the impact of preventive actions they have taken - were unable to provide supportable evidence to this effect.** While management theory might advise that initiatives should be targetted at clearly defined problems, resources derived from approved budgets and attention paid to monitoring progress, the reality is that few actions (even against discrete problems) meet such textbook criteria. Moreover, determining precise cause and effect naturally becomes extremely difficult in cases where anti-crime actions form part of a broader strategic effort. It is also problematic when the risks faced have not been experienced in the past but are nonetheless serious in their implications (such as actions against terrorist attack, food contamination etc.).

These various impediments, and a tight timetable, should serve to underline the fact that the enquiry can make no claim to being either representative of business initiatives in general - or indeed of actions taken against crime by the businesses actually surveyed. It provides rather a commentary on some interesting developments in an area that has seldom been subjected to external scrutiny, and a few examples of actions that have been demonstrably successful.

Report layout

The commentary on company initiatives has been divided into four separate sections. Section 2 explores actions being taken to prevent theft - by outsiders or staff themselves - in and around the workplace. Section 3 focuses on the rather separate problems associated with preventing losses outside the confines of factory, office or shop. Section 4 deals with fraud and Section 5 with violence and threats to which workers are subjected. Observations on the wider lessons to be drawn from this exercise are drawn together in Section 6.

2. Managing crime at the workplace

Tackling crimes likely to result in a direct loss at the factory, office or building site itself - whether by the predation of outsiders, or the activities of employees themselves - constitutes the primary focus of most businesses' preventive strategy. The wide sphere of activities which can be involved (and the fact that individual elements of any general preventive strategy are difficult to separately evaluate) make it impossible to present examples that could lay claim to being representative. Instead, a commentary is provided on some of the main themes common to the anti-crime actions taken by the businesses that were consulted.

While there is no formal hierarchy in the way these themes have been presented, actions taken against external threat are presented first, followed by actions against internal threats.

Risk assessment

One of the distinctive features of several of the larger conglomerates was that they were able to provide operating companies with in-house crime audits undertaken by specialists in the parent or holding company. This presents the subsidiary company with a facility which their operational teams are frequently unable to provide because of the pressures of day-to-day work. At the same time, the use of in-house services is aimed at ensuring impartiality. It is also held that recommendations will be more likely to be cost effective and consistent with broader company objectives.

The mechanisms for initiating security audits vary widely. At one end of the spectrum, some conglomerates **require** that operating companies are subjected to audits: in Trafalgar House, for example, the security audit service is performed on an annually programmed basis, taking 3 years to complete the round. Once provided, a written report is required from the receiving party on all the recommendations made. At the other, the service is discretionary, and charged for in much the same way as an external consultancy. The audits performed by the Post Office Investigation Department (POID) fall into this mould: these are executed in a tightly structured manner derived from the days when Post Office operated as one company (all recommendations being formally classified according to the perceived risk, the urgency attached to implementation, and the associated cost) but the service is provided only to customers who pay for it through an inter-business contract.

Comprehensive security audits of existing sites - embracing internal procedures as well as external protection - are not of course the sole prerogative of such larger organisations. One of the more impressive signs that prevention is being taken seriously is that some (particularly amongst the multiple retailers surveyed) have now developed formal mechanisms for gauging the risks likely to arise at new sites. While consultation with prevention experts at, or shortly before, commencing

new business operations is quite commonplace, the critical factor here is that crime costs are being considered as an intrinsic element of whether or not to develop. One of the primary exponents of this form of assessment is Argos - where surveys of proposed sites (comprising analysis of police statistics, informal consultations with operators already there, assessment of detailed site criteria which may effect risk, etc.) are now an accepted part of the viability assessment for new stores. An unexpected byproduct of their experience with such surveys is that the company has scrapped the idea of common standards of security protection at all stores. This allows expenditure saved from minimal protection at low risk sites to be diverted to increased protection (well beyond former common standards) where risks are shown to be high.

Crime analysis

Risk audits, while obviously drawing on the evidence available from known incidents, dwell heavily on **theoretical** exposure: the vulnerabilities judged by the auditor likely to be exploited. This is essential, but equally many companies place weight on the global lessons which can be learnt from detailed analysis of reported incidents.

Crime analysis techniques were at their most sophisticated in several of the companies who have direct responsibilities for large field operations (such as BT) or who had developed sophisticated computerised systems to perform analysis on high volumes of incident records (see Burrows, 1988).

High reporting levels are a prerequisite for effective crime analysis - simply because unreported incidents may conceal factors material to the conclusions drawn. This renders burglary, which is generally reported simply to effect repairs and initiate audits, as a good subject. Quite sophisticated analysis of burglary patterns was not unusual, and the experience of several of the electrical retailers in this field has led them in new directions. A number of them have, over recent years, experienced a sharp upward surge in high-value burglaries at their out-of-town superstores, and have been monitoring such attacks to tailor their own preventive strategies with some precision. The common risk has also prompted the main players in the Electrical Retailers Security Association (ERSA) to initiate early warning arrangements which notify the others of all such instances, persuaded them to pool all of their information on break-in methods and on-going investigations, and even sponsor external enquiries by universities to help determine future preventive policy.

Integration of security hardware

Another common route being pursued by many of the companies consulted in this exercise was the integration of security systems and controls: both with each other (for example, merging CCTV, alarms and electronic article surveillance) or with

other trading systems. This trend is obviously made feasible by a range of technological developments. But it also has wider significance: separately operating security systems are to an extent, evidence to the effect that many crime control devices are 'built-on' afterthoughts. In contrast 'commonality' is a clear demonstration that security technicians are working in conjunction with their data processing counterparts in mainstream operations.

Although it did not prove possible to separate precise cost-benefit details, to many respondents these were self-evident. A number believed that simple rationalisation of contracts, service agreements and so forth with a range of hardware suppliers had achieved major savings. Others have refined their protective policy. Weaknesses arising from ageing alarm systems (including false alarms), for example have caused Standard Tyre and Exhaust to put a lifespan of 5 years on all their systems after which they are replaced. But the strongest examples were of developments when alarm systems had been converted to share other company communication channels and bought under in-house control. Retailers are amongst the front runners in this field: several of the major grocery chains (e.g. Gateway, Tescos, etc.) now have experience of running their own central stations over several years and use alarm communication channels to operate centrally facilities like branch lighting, refrigeration monitoring or store climate controls. Others are taking advantage of forthcoming company decisions to provide on-line electronic point of sale (EPoS) or funds transfer (EFTPoS), in place of night polling, to merge communication systems and effect major savings. It is also evident that CCTV systems linked directly with EPoS - that will display details of till transactions on CCTV monitors, or can select to record only specified high-risk transactions - are becoming commonplace.

Case study 2:1 provides an example of how the grocery chain Tesco has integrated much of its security hardware and the resultant payback.

Case study 2:1 Evaluating closed circuit television

Closed Circuit television (CCTV) is now in widespread use to broaden the range of management control and to act as a deterrent to crime. There have been spectacular developments in the sophistication of systems available. In particular, in response to users' concerns about the ability to monitor permanently 'live' systems, there have been innovations in the development of systems that trigger only when activated by alarm sensors or other signals. Few evaluations are however available.

Problem: *Tescos, one of the country's largest retailers, are vulnerable to crime in various forms - not least from attacks on staff in the course of robbery, from shoplifting and from internal theft. They have become increasingly aware that incorporating 'piecemeal' security arrangements for their supermarkets (particularly larger superstores) provides less than comprehensive protection. Equally, their reliance on store detectives as a main element in their defensive strategy has been a costly drain on store revenues.*

Preventive *Strategy:* *Over recent years, a growing number of stores (both new and existing) have been fitted with an internally-developed security package, known to the company as the "Totally Integrated Security System" (TISS). This package incorporates changes in store design and procedures, but its central component is the provision of CCTV to ensure central monitoring of all vulnerable areas both within and outside the store.*

The areas covered by TISS can be broken down into three categories, and CCTV coverage at each is relayed both to a security control room and the manager's office:

— *Central cash handling areas have been modified into a suite of rooms comprising a cash room and a safe room - separated by a sterile, airlock area. This internal 'fortress' incorporates internal alarms, CCTV cameras and monitors, and hardened doors. Safes are only accessible when management and cash carriers unlock in tandem.*

— *To protect against cash snatches at the till, as well as staff theft and collusion, check-out lanes are all separately monitored by CCTV and cash lifts from the tills are carried out by the use of an air conveyancing system to the 'fortress'.*

— *Vulnerable internal and external areas like staff entrances, rear doors, waste disposal areas and where appropriate, petrol forecourts are under surveillance.*

In nearly every instance, monitoring is not continuous but is triggered by defined usage but with the capability of being 'driven' by the operator.

The capital cost of such sophisticated equipment, fully integrated, is high: some £150K for an average superstore. Running costs, in the form of security operatives, are some £15K to £20K per annum but they are not an additional cost, security managers being present at the stores anyway.

Impact: *The first two installations of TISS were at a new store and at an existing operation. At the new store, because of the lack of previous history, any measurement of the impact of TISS proved impossible. However in the second store an immediate impact was seen. Unknown losses dropped from some £12K a week to £5K a week.* ***In other words, the payback on the capital expenditure on TISS was realised within six months (£7K saving per week X 26) on this criteria alone. These were not*** **however** ***the only benefits: cash losses from the tills dropped from some £500 per week to £20 per week, and violent incidents in the store almost disappeared.*** *As a result of this initial success, the system was extended to other stores.*

The roll-out programme for TISS is still in its infancy and the company view is that it should be installed only in stores where there are major problems and an opportunity of getting a payback. Nonetheless similar success patterns have been

repeated at the eight stores currently operating complete systems: indicating that unknown losses can be reduced by between 40 and 60% at high loss stores. Incidents of violence and casual shop theft are reported to virtually disappear. There are also benefits in that the 'quality' of arrests of more professional thieves is improved and that taped evidence increases the likelihood of "guilty" pleas in the courts.

Contract services

Amongst the various objectives of those involved in the upgrade or modification of security hardware, several aim to reduce their dependency on manned services like guards. It was not uncommon for this cost to be reduced by straightforward technological development: the computer firm Digital, for example, has already realised significant savings in its guarding budget simply by networking alarms and CCTV installations so as to facilitate the monitoring of key functions at one central point. Savings in the first year of a roll-out programme, which has covered about 10 of its 50 sites, are already £165K and will rise to £142K in the following year when the capital outlay at these sites is past. More substantial savings will follow as the programme is extended nationally.

Savings in operating costs were however generally viewed as secondary to the greater efficiency, and deterrent value, of sophisticated equipment. Trafalgar House cited their experience in protecting the enormous ship buildings yards at Scott Lithgow as a case in point. In 1988/89 these yards were the regular target of those removing heavy gauge power cabling for its copper value: some - but by no means all - of these teams were detected by security patrols. But a decision taken in early 1990 to instal CCTV with infra-red lighting (operating by microwave link) had a dramatic impact and attacks are now nearly totally eliminated.

On a related issue, a number of companies also reported benefits from tightening contractual control over those providing guarding or store detective services. When such services are used there appear to be substantial differences in the extent to which the employing companies dictate their own special requirements or accept the guards' 'standard' methods of operation - and indeed in the attention devoted to monitoring compliance with agreed terms. One of the more sophisticated service users is Woolworth who collate a series of performance indicators - ranging from the numbers of staff searches conducted or arrests made, to the number of till checks carried out - on a Head Office database. These various indicators have been developed over time as those which appear to have the strongest bearing on store stock losses. The use of the system, coupled with a deliberate policy of employing several competing companies, serves to exert strong pressure towards maintaining guarding standards.

Internal procedures

One of the clearest signs of the seriousness with which companies treat crime issues is the extent to which their security, or crime risk managers, are seen as having an

open remit and responsibility to subject routine operating procedures to scrutiny. This proactive role is substantially different from the essentially "fire-brigade" function that many companies expect (and at odds with the view that the crime specialist has no contribution to make beyond that of providing security hardware). The more proactive model is of course a challenge to both the crime specialist and to the recipients of advice on prevention: in Dixons, for example, there is an expectation that security operatives should not only have a central troubleshooting role like this, but that they should occasionally perform 'live' tests of vulnerable systems (for example, by hijacking a container) to bring home to the business the seriousness of the risks faced (see Crime Concern, 1990).

In nearly all of the companies surveyed there was a ready acceptance that security direction and advice was appropriate on obvious matters such as cash handling: a point reinforced by some of the interesting initiatives reported to the CBI/Crime Concern Working Group. Scottish and Newcastle Breweries, for example, have followed the lead of companies more familiar with cash snatches by installing two-key safes (requiring simultaneous unlocking by their manager and the security company) in their pubs. Kwik-fit has tightened banking procedures by agreeing arrangements with banks that they will give notice of any takings not deposited by local Kwik-fit branches. Managers who for any reason are not able to bank takings on a specific day have to inform a 24 hour hotline to this effect (failure to do this constitutes a dismissible offence).

Most companies however are reluctant to allow free rein for crime specialists beyond such fairly well-defined boundaries. One example of security breaking these bounds was an initiative on cheque recovery taken by Tesco's Security Department (Case Study 2:2).

Case study 2:2 Automatic cheque recovery procedures

The methods used by companies to recover 'rubber' cheques rejected by banks are diverse. Some will go directly to debt collecting agencies to extract repayment but most initially respond by following internal procedures. The focus varies from concentrating on claims disputes with banks to liaising with the police about stolen cheques.

Tescos have subjected their procedures to detailed reappraisal and their experience suggests that there could be many who could make substantial improvement.

Problem: *Up until 1986, all rubber cheques handled by Tescos were dealt with by a small Cheque Recovery Group of four administrative staff. The Group's activities were bureaucratic and focused on resolving signature disputes with banks and - should these fail - attempting to trace customers. In 1986 the recovery rate of the team was 15% of cheques handled (approx £80K pa).*

Preventive ***action:*** *Critical analysis of this team's operation during 1986 led Tesco to decide to target primarily the* ***customer*** *passing a bounced cheque either by writing directly to his/her address (which are collected on all cheques not guaranteed by cheque card) or by passing letters to the customer directly through their banks. A decision was taken to computerize this operation. The improvements took place in two phases.*

The first phase involved the minor development of a software package and the purchase of computing equipment which enabled letters to customers to be generated automatically. By the same token the software was programmed to generate recalls to customers who failed to respond within a month. The cost of these changes was a modest £10K.

A second development phase took place in late 1987 when the limitations of operating three stand-alone PCs were apparent. To network the system, £34K was spent on purchasing two additional PCs (£4K) and the system net work itself (£30K). At this point, it was also decided to charge those customers who paid with cheques that were not honoured an administration fee of £5 to meet the cost of cheque recovery.

Impact: The immediate impact of Phase 1 of this minor programme was to increase the **recovery rate** ***from 15% to 35% per year, producing a very rapid payback. The recovery rate rose again with the introduction of the networked programme in 1988 and were of sufficient magnitude to fully meet the costs of the hardware and necessary soft ware after the first month's operation.***

Administration has not risen proportionately and despite the rise in the number of cheques handled (for example, doubling between 1988 and 1990) the costs have been offset by the income of an average £15K per annum levied from the administrative charges paid by customers who fail to respond to initial enquiries.

During 1990 some 66% of those cheques received by Tesco Stores which subsequently bounced have been recovered which equates to the sum of £2M in cash. The majority of these recoveries (87% in 1990) are made from customers where account funds were not, at the time of drawing, sufficient: not from attempted fraud. Apart from the clear financial case for the computerised recovery system itself, it has led to significant improvements in cashflow and enabled company investigators to concentrate on the remaining fraudulent cases.

Promoting awareness

It goes without saying that employee support is central to any successful preventive strategy. This is a message that none of those surveyed disputed, but of course

ensuring that each employee understands his or her personal responsibilities - and, still more, subscribes to the values and principles underlying the company policy - is by no means easy. It is moreover difficult to establish the payoff from investment in this general area.

Three principal themes emerged. First the majority of the companies surveyed had, in some published format, issued a mission statement on crime and how it should be dealt with. As the respondents tended to be large corporations, this is not surprising, but is nonetheless welcome. A number however admitted to some degree of company ambivalence in the execution of the written policy. But there were also signs of a good deal of thought being given to detail: at a mundane level, for example, Sony Music had installed random selection equipment to eliminate suspicions of victimisation by those subjected to staff searches. Others were, where appropriate, using metal detectors to eliminate the need for personal contact during searches.

Second, there were signs of the same kind of careful thought and advanced techniques going into training packages (with in-house videos, interactive presentations, etc widely used). One of the concentrated training programmes that could be shown to have yielded considerable benefits was that set up by the large DIY multiple B and Q (Case Study 2:3).

Case study 2:3 Enhancing awareness and accountability

One of the common messages to emerge from the retail sector was that increased "shrinkage" losses - coupled with recessionary pressures - have been effecting radical re-assessment of operating cultures: with managerial accountability, in particular displacing the predominance of the entrepreunerial sales-orientation of the recent past. DIY chain B and Q were among the companies who have been coming to grips with this issue.

Problem: *Despite robust improvements in sales and profitability throughout the late 80s, B and Q experienced significant increases in its stock losses, which by late 1990 rose to an unacceptable level.*

Preventive action: *The company set up a top-level working party, comprising representatives of all the main company functions (with - importantly - the robust support of the operations director serving to signal a major change of direction) to formulate a strategy to tackle these unacceptable losses. This team developed a comprehensive action plan - covering 95 action points - which were devolved to a wide number of directorates to implement. It also introduced a three-pronged programme aimed at educating branch staff and developing the accountability of individual branch managers. This comprised:*

— *Conducting an intensive training programme, under the name of "Storewatch" for all store management grades (managers and their two deputies). Over*

1100 staff attended these sessions which utilised sophisticated audience-response devices to ensure the full participation of all who attended. At them, management were set realisable targets for their stores and equipped with training material to continue to 'cascade' the message to their own staff.

— *Focussing management "hit" teams at the worst 25 stores in the chain. These teams - of six or seven staff (audit, security, personnel and training professionals) headed by a district manager from another region - spent a full week conducting in-depth enquiries. This then led to presentations of an action plan to the Operations Director. This in itself was a powerful message to all store managers.*

— *Increasing the audit and security coverage* in *the worst region. This was an experiment which went against a company trend (and indeed one apparent in many parts of retailing) to cut back on audit and security support. A regional auditor and security manager were appointed to agree a programme with the regional management team that carefully targetted their combined resources at the stores providing the greatest potential payback.*

The cost of this overall programme was reasonably modest, comprising the costs of training material and equipment, hotel accommodation for the hit team and marginal increases in audit and security staff for the second and third elements.

Impact: The overall effect of this package of measures in their first full year (Feb 90 - Feb 91) was to reduce Band Q's stock losses by 25%. The original investment in the programme was returned twentyfold within the first year.

While the concentration of these various countermeasures in the space of one financial year does reasonably enable a direct causal connection to be drawn, it is more difficult to seperate the success of the individual components. In isolation, the targetting of the worst stores (where losses fell by 40%) and increasing the audit and security support (which transformed the 'worst' region in '90 to the 'best' in '91), were successful: but staff at these stores were also subjected to the same training programme.

Needless to say, given these manifest successes, B and Q are now intent to make further inroads on their stock losses and are targetting further training initiatives at identifiable groups within the stores; providing increased audit and security support for the rest of the company; and continuing to develop their "worst 25" store initiative.

The third point was that a good many companies have been investing some effort in persuading employees to bring suspected cases of malpractice or crime to their attention. The 'neighbourhood watch' message about the significant potential in activating the "eyes and ears" of the community is now commonplace and its import has not been entirely lost within corporate organisations. But, for some

respondents, it has been reinforced by their own analyses of how internal detections for crime typically come to light: invariably these show staff themselves as the main "whistle blowers" (see Winfield, 1990). The response has been to try to increase the alternative reporting routes available to those suspicious of their colleagues - with some companies now providing confidential hotlines direct to internal security.

Devolving responsibility

A more specific and tangible aspect of general crime awareness is the task of promoting clear understanding of the direct responsibilities each individual bears for prevention. Again, evaluation of particular initiatives in this sphere proved well nigh impossible, but two important themes seemed to be gaining ground.

Several of the organisations intent on ensuring the full accountability of local management for prevention, and with penalising them for their losses, were coming to terms with the inadequacy of the accounting procedures and systems necessary to support this objective. This was in some instances apparent in the realisation that the convention of allocating security expenditure from central budgets does not foster any accountability: under these accounting conventions there can be little surprise that local management may not be particularly committed to regulating another departments' expenditure. In other cases it has proved difficult to foster local management control because of the lack of accessible management information held at warehouse, branch or unit level - or simply because audits had not been performed at manager changeover. In other words, the shortcomings of management information are proving, to some, a major hurdle in establishing local accountability.

Despite these difficulties, the majority of organisations were strongly committed to the principle of local autonomy. This, for example, is the main principle underlying policy in Marks and Spencer (where each store manager is ultimately entirely responsible for his or her own operation). Many others - within retailing and beyond - were working to ensure their individual operations could be judged as entirely independent profit centres: bearing the responsibility, and cost, for preventive actions and being judged - and often paid - on outcome.

Organisations well advanced in the implementation of this philosophy have not seen their central security/risk management functions 'wither away' but adapt to a new - more discriminating - role. In many respects their changed role is akin to that of a consultancy service, where they act to encourage and evaluate ideas from local management, identify new technologies, and so fourth - but do not attempt to provide any semblance of 'ground cover' across the organisation. Practitioners see it as a major step back from the unrealistic and impractical view that a small central team could somehow police the whole organisation. The parallels with trends in modern policing are unmistakable.

3. Protecting assets in transit

Cash or product 'on the move' often proves most vulnerable to theft - and for obvious reasons. It is difficult to achieve the same standards of physical protection that might be taken for granted at fixed premises; goods are changing hands between different people (frequently third parties), which can lead to disputes over accountability, and of course logistical and commercial exigencies will often work to the detriment of prevention. It is not surprising, therefore, that one of the common characteristics of those business sectors found by the Working Group on the Costs of Crime (1988) to bear the heaviest crime losses was that their operations hinged on the movement of cash or consumables (as against, for example, sectors like manufacturing and engineering).

This section provides some examples of actions taken by business to deal with the risks inherent in the physical movement of cash and cheques and to combat the problem of cheques or credit being intercepted in the post. It then provides a short account of some 'industry responses' to crimes arising from general product movement in the tobacco industry, the breweries, and the wines and spirits sector.

Cash and cheques

Cash must be the most attractive target for theft, and there are commentators who have drawn attention to the fact that, despite major steps made towards the "cashless society", British firms still pay a higher proportion of their workers in cash than their European counterparts (see CBI/Crime Concern, 1990). This, coupled with the predictability of pay day routines, means that the wages snatch is still not uncommon.

There are however few companies routinely involved in cash handling that are not well versed in the risks. The cash holding of the single retail or bank till has been reducing and the security of collection methods between individual till and the safe (whether by secure cans or air passage) has been improved. It is also now widely accepted that large cash holdings should be made inaccessible to those who may be coerced during a robbery: notices to this effect area familiar sight - from those on taxis or milk floats through to security vans.

Cash carrying services offered by security companies have also mushroomed, and it is pertinant that the risks associated with cash or cheque movements have not been the only incentive. It has been the experience of a number of multi-outlet companies that the actual frequency of robberies committed against staff carrying takings to the bank - although invariably worrying - has not been sufficiently frequent (or the outcome serious enough) to warrant the cost of extending security collections to all trading locations. However the recognition of associated financial dividends alongside the security merits of these arrangements can radically reverse this equation. Several companies have found that by utilising security collections

they can arrange for money to be deposited in bullion centres and so achieve same or next day credit rather than the normal 3 to 4 day bank clearance on cheques. In short: additional interest accrued from bullion centre deposits can go a considerable way, and sometimes exceed, the cost of fees to security carriers.

Failure of postal deliveries

Financial service companies are showing increased concern about the loss of valuable documents and credit instruments in the post (see Ernst & Young, 1989). Not all of these losses arise from robbery or theft of mail - some losses originate from senders themselves (for example by misaddressing mail) or occur at the receiving location (when mail can be intercepted before the receiver collects it). But the general concern about all these factors is reflected in the emphasis that the Post Office itself - through its investigation department (POID) - is giving to sharpening its efforts to minimise the risks.

Improved analysis and cooperation is serving to enhance investigations after attacks on postal delivery workers. These establish patterns or linkages between attacks and in particular - through rapid links with the DHSS'S records of Giro benefit payments - pinpoint when post offices may be used to cash stolen items.

Beyond this, there are renewed efforts aimed at identifying when credit cards, sent through the post, go missing. Until recently the mainstay of the Post Office strategy was an arrangement where credit providers contributed to POID'S 'Canberra' system. This uses all participants' reports of non-receipt, and subsequent fraud, on credit cards to identify high risk post offices and routes, and to target POID investigators accordingly.

This service is now being supplemented by a commercial scheme, launched by the Post Office and others, entitled the Fraud Risk Management (FRM) initiative. This shifts the focus to one of prevention by aiming to provide a more proactive and direct service which can - within the terms of the legislation on date protection - identify high risk addresses for a far wider range of frauds: enabling contributors to take appropriate action when risks require it. The arrangement draws directly on details of fraud suffered by many credit providers - whether application frauds, insurance or mortgage frauds or plastic - and reconciles these with address records held and updated by TV licencing.

It remains to be seen whether this broad based initiative (launched in late 1989) will attract sufficient support from the financial services sector to make it a viable and comprehensive industry service. Clearly the stakes for the Post Office, as for the direct loser, are high, as Case Study 3:1 illustrates by drawing on the experience of one credit provider - Barclays Bank - who sought to tackle the risks inherent in credit card intercepts. Their lead in turning to the selected use of special courier services has been followed by others.

Case study 3:1 Thefts of credit cards sent by the post

A significant problem faced by all credit card providers is the 'interception' of cards in the post, or shortly after their delivery, and their subsequent misuse. The preventive action taken by Barclays Bank broke new ground, and has been followed by several other card issuers.

Problem: *In 1989 'intercepts' of Barclays' Visa and other cards were estimated to have constituted 45% of all fraud losses - some £14M. Conventional methods of control had significant drawbacks: the use of registered mail for all deliveries was prohibitively expensive, and any claims could only meet the cost of card replacement (not the fraudulent transactions that often followed). Equally, requiring clients to collect their cards from banks was expensive and - during trials - met with significant customer resistance.*

Preventive action: *The route chosen by Barclays was to establish high risk areas for card intercepts and employ special courier services - initially private contractors, but later a POID service - to deliver in these locales (approx 5000 per day). This use of contract services enabled Barclays to impose criteria on when deliveries should* ***not*** *be made (i.e. to obviously empty properties, or to houses with multiple occupants where the customer could not be contacted), which could not be permitted under normal Post Office guidelines. If deliveries had to be aborted, the customer would then be advised to collect from their local Barclays Bank.*

The cost of this service is approximately £30K a week, or £1.6M per annum. Additional administrative costs sustained by Barclays increase the total running cost to £2M per annum.

Impact: *Since the introduction of these arrangements in July 1990, 'intercept' frauds have dropped from 45% to 25% of total fraud losses. The improvements have however driven fraudsters to use stolen cards more excessively, and the average fraud loss per intercepted card has almost doubled.*

Despite this, after the running costs of this initiative have been taken into account, the current estimate is that there will be a reduction of fraud loss of some £5.0M per annum effected by the selective use of courier services.

Product movement

The experience of industry wide initiatives may be chequered but the preventive actions effected through the Tobacco Advisory Council (TAC) have achieved substantial success. A security council was formed in 1969 to tackle the major crime losses being sustained by the tobacco industry - and had an immediate advantage in that it developed as an additional service of a trade association with a history

running back to the second world war. The most significant mark of their success is that gross recorded losses sustained by the industry, when adjusted to 1969 prices, have only once exceeded those sustained in its year of origin.

One of the apparently unique characteristics of this group, compared with many other anti-crime associations in business, was its early decision to **pool all reports of UK crime incidents experienced by the industry** at the TAC and to fund a separate group to plot company and industry statistics and trends (including criminal intelligence). This enabled the security council to monitor the performance of distribution companies, providers of alarms and other security equipment, police forces and indeed company anti-crime strategies. It put the group in a remarkably powerful position, albeit only advisory to the individual tobacco operator, in establishing shortfalls in crime prevention.

Their experience in tackling vehicle hijacks during the 1980s illustrates the way this function operates. In 1983 an increased number of vehicle hijacks prompted the security council to commission the development and evaluation of anti-hijack devices. A security technology group was approached and developed an on-board computer which could provide different levels of physical protection (from back door digital locks to vehicle immobilising devices) and incorporate radio connections that alerted distribution control in the event of hijack. These devices were fitted to vehicles operated by one of the largest independent carriers for the industry and attacks were rapidly displaced to other fleets. A 'domino effect' was then plotted through the industry which showed that in the initial years, although fleets with anti-hijack devices were afforded high protection, the extent of displacement was such that there was little impact on overall industry losses.

This pattern only changed in 1988, with the development and industry adoption of Datatrak (a device which actually pinpoints with extreme accuracy the location of any hijack) which has reduced the number of attacks across the board. Hijacks of tobacco, which typically net a loss of at least £80K per incident, have reduced from 22 in 1988, to 14 in 1989, 4 in 1990 and 1 in the first quarter of 1991.

Another striking example of an effective industry response, not related to one specific form of theft but to the broader issue of accountability of product in transit, was furnished by the Brewers' Society. This provides a convincing financial case in support of an initiative they took to reduce the theft of aluminium beer kegs: see Case Study 3:2.

Case study 3:2 Targetting keg theft: joint action by the brewers

One striking example of a collaborative venture taken by industry competitors to tackle a common external threat is the brewers' initiative against the theft of aluminium kegs.

Problem: *During the 1950's most major brewers started to replace the traditional wooden beer keg with light, tough aluminium substitutes. The security of these kegs was not at this point an issue: they were moved only between individual breweries and their tied houses, and unique identifying numbers were recorded on delivery and collection. These controls however evaporated during the next two decades. The hegemony of the tied houses was challenged and the increasing number of kegs being passed to wholesale operators made it impractical to continue monitoring individual keg movement.*

These reduced controls - and indeed the vulnerability of kegs stacked outside pubs and distribution depots - was then exploited for the high scrap value of aluminium. In the early 80's, industry representatives became alarmed and sought to take action. Comprehensive estimates of the industry loss were difficult, being based on 'snapshots' in time, but in 1987 it was estimated that the loss of kegs (based on an average £50 replacement value) had risen to £23M per annum.

Preventive Action: *Individual brewers, once alerted to this problem, quickly realized that independent action would be limited in effect. The same constraints that gave rise to the initial problem served to restrict the scope for developing any internal audit trail for kegs. In view of this the seven major brewers, under the aegis of the Brewers' Society, embarked on a campaign aimed at restricting the organised teams who were operating to steal and smelt kegs.*

There were four main elements to this campaign, launched in 1985:

— *to alert police forces to this new form of criminal activity: by funding posters for police station noticeboards, advertisements in police publications and developing a training video which advised police on how to identify and liaise with brewers in relation to this crime.*

— *to heighten awareness amongst metal dealers who could inadvertently handle the stolen metal: achieved by advertising in appropriate trade magazines.*

— *to advise pub staff and the wider public, of the problem and the part they could play in reducing the risk - by articles in brewers' publications and the national press.*

— *to increase the likelihood of detection. To do this an information hotline was set up (and advertised in police and trade journals) offering rewards of up to £10K for the arrest and conviction of those involved in the theft and smelting of kegs.*

The total cost of this campaign over the first four years of its operation (1987-90) has been £195K. This figure is based on an estimated shared running charge of £145K over the period: to cover reward payments, advertising and the employment of consultants to coordinate publicity. During 1990 the seven brewers have also

instructed solicitors who will liaise with the Crown Prosecution Service on case law and presentation, or advise on civil actions. The 'hotline' is operated as an adjunct of an existing 24-hour guard service, and has not given rise to additional costs. The creation of two training videos involved a one-off expenditure of £50K.

Impact: A snapshot of losses in 1990, similar to that taken in 1987 now suggests that the industry cost has fallen to £10M per annum: a reduction of £13M over three years with a relatively minor investment in prevention.

While this reduction is very significant, the scale of loss remains large and more radical preventive strategies continue to be examined. A number of breweries have been looking into alternatives to aluminium: several have turned to stainless steel and plastic substitutes have been subjected to continued scrutiny. Paints which will colour smelted aluminium are being explored. Deposit schemes ('sale or return') remain under review, despite the difficulties in handling wholesale sales. Finally, one of the brewers has started bar coding kegs after development of codes that promise to be sufficiently resilient to the heavy handling and high pressure cleaning to which kegs are subjected. This development follows from a joint initiative to identify a common, compatible, barcode (essential if wholesalers are to be involved).

A third 'industry initiative' looked at in the course of this review was the anti-crime work of the Wine and Spirits Security Liaison. This has very strong parallels with the Security Council of the TAC (and has similar longevity, dating back to 1971). Transport and warehouse protection were its original goals, but these have been supplemented with an increasing role in tackling credit frauds sustained by the industry. While it cannot lay claim to quite the same blanket coverage in its field as the TAC (largely because of the wider spread of independents among the wine and spirits producers and distillers), it has a clear mandate from the majority. It also has the allied advantage of being able to indicate to potential members that subscription levels can be more than fully met by the reduction in insurance premiums (in addition to any reduction in loss by fraud) enjoyed by those who participate and follow recommended procedures.

Industry responses are difficult to organise and sustain and may in many cases be inappropriate. It may not be coincidental that the examples outlined in this chapter emerge from sectors where relatively small numbers of very large players dominate the market. Equally the incentives for them to act are considerable: because of the high value of their product coupled with high duties (for taxes - some 60% of the value of tobacco, for example - are still payable on stolen items!) and the vulnerabilities they face in distributing through so many diverse outlets. Nonetheless they effectively illustrate that cooperative efforts can work.

4. Designing out fraud

Much has been made in recent years of the spiralling costs of fraud which, despite many shortcomings in official statistics, clearly far outweigh the financial costs of all other forms of crime. Indeed, fraud is now frequently presented by commentators (although with little supporting evidence) as the 'easy pickings' to which professional criminals have been diverted (away from more violent forms of crime), and as the predicted growth industry when the European border controls are relaxed in 1992 (see, for example, Campbell, 1991).

The statistics are confusing because the number of regulatory authorities who are involved and keep separate records are numerous - from Customs and Excise and DTI through to the Treasury (which estimated in 1980 that its lost revenue from tax was between 7 and 7.5% of GDP). But analysis of those frauds dealt with by UK police fraud squads (Levi, 1987) has indicated that, revenue fraud apart, fully 96% arose from the private sector (two thirds from the financial services sector and one third elsewhere) and only 4% from public sector bodies and individual victims. On the basis of these statistics, in other words, businesses bear the brunt of all fraud losses.

Much fraud against business, too, goes unreported and while the stigma attached to admitting fraud is one reason this occurs, successive surveys by Ernst and Young have also indicated that this is a sign of companies' belief that the police can do little to either retrieve funds or deter. This attitude towards reporting fraud, by implication, throws some light on companies' views on prevention itself namely that the police have a limited role to play in such a complex arena. In the 1989 survey, for example, no financial services company - and only a third of others - expressed confidence that the police could deal satisfactorily with a £10K fraud against them. Even less believed that the police could assist in coping with computer fraud (although there was, at the other extreme, much more confidence that a fraud involving £1 million could be handled).

It seems, therefore, that it is only when considerable police time, and presumably the time of more professional officers in squads, can be attached to major frauds that companies perceive much payback. The implication from this, which is strongly supported by the contacts made during this review, is that day-to-day limitations on police time, and the complexity of so many business systems, preclude any real role for the police in fraud prevention.

Recognising crime opportunities

The belief that opportunities to commit fraud will, in time, be exploited - and that this principle is in many cases overlooked by those designing systems and procedures ~~ was widely accepted by all approached.

Respondents provided many telling examples of this, but one of the most striking was furnished by British Telecom about a case that received considerable publicity when it was first uncovered. The example relates to the time when premium rate service lines - using the 0898 prefix - were first set up. The higher charge rates on these lines are split between BT and the service provider, but in establishing the system BT agreed to pay service provider revenues (gauged from metering systems on the **incoming** line to the service provider) on a monthly basis.

It was soon realised that the mismatch between this payment period and the traditional quarterly bill to the customer could be exploited. BT subsequently discovered that a team had set up a premium rate service, ordered multiple phone lines at rented accommodation, and paid people to flood the service line with calls. This allowed them to reap revenues from BT for the first two months, and then to vacate the accommodation before being faced with the quarterly dial-out charges. The publicity surrounding the trial of the first team arrested for this crime prompted many more attempts which were only detected by improved controls from BT.

Case study 4:1, which draws on the experience of a major fraud faced by National Savings, provides another example of this same point - that system frailties are invariably abused - and illustrates the precautions that had to be taken in response.

Case study 4:1 Combating National Savings fraud

The National Savings Ordinary account improbably unique amongst savings options. The main advantage to the 15 million account holders is undoubtedly accessibility - afforded through nearly 21,000 post office branches nationally, most of which are open throughout normal shopping hours. Transaction volumes are significant, running at some 23 million in 1990. *The simplicity and convenience offered to customers has however had its drawbacks for National Savings, when accounts became increasingly prey to fraud.*

Problem: *The passbooks conventionally issued with most building society or bank savings accounts are simply a customer reference, for savings balances are accessed against a central computer record on each occasion transactions are performed. This is not the case with the NS Ordinary account: the bank book provided with this popular account gives direct access to the savers' funds. This difference was increasingly exploited by fraudsters during the late 70s and early 80s, when many books were operated fraudulently. False deposits were being entered against bogus post office stamps and worthless cheques would be deposited. By 1984, annual fraud levels had risen to £3.98M.*

Preventive Action: *In the face of these rising losses, in mid-84 National Savings initiated a multi-pronged campaign with Post Office Counters and the Post Office Investigation Department which continues to the present time. The lynchpin of this campaign was the establishment of an Account Validation Service (AVS) at National*

Savings in Glasgow. By ringing a freephone hotline post office staff could speedily check account balances on occasions when their suspicions were aroused. This was accompanied by an extensive training programme (combining local presentations and the circulation of a fraud prevention video) which advised post office staff of common methods of fraud and the characteristics of known fraudsters. The third component was to introduce a reward scheme which pays out for fraudulent books impounded by post office staff. The reports completed by those claiming rewards are used to assist the subsequent identification of offenders.

The "set up" costs of this campaign - comprising the capital and software developments required to operate AVS and the cost of the training video and roadshow material - totalled about £55K. The direct running costs of manning the validation service, call charges, supporting an on-going training programme and the payment of rewards (nearly 15,000 since introduction) totalled around £140K p.a. The gross cost over the six years of the programme has been £900K.

Impact: *The cost of fraud sustained by National Savings was cut by nearly two-thirds in the first year of this campaign from £3.98M to £1.35M) and nearly halved again the following year (to £770K). Improvement continued throughout the late 80s - albeit at a less dramatic rate - and annual fraud losses are now some £400K per annum.*

Over the full six years of this campaign (1985-90), the total loss from frauds against National Savings was £3.91M: less, in fact, than the single 1984 total. The rate of loss was rising sharply in the years preceding 1984, but even if annual losses had stabilised in 1984, the predicted six year loss would have been of the order of £24M, and would have called the viability of the service into question.

Finally, as well as the major improvement in fraud losses, the information gleaned through the operation of the reward system has contributed to the detection of 5,000 offenders over the duration of the campaign.

Procedural and systems audits

Every company, as a matter of course, builds checks and defences against fraud into everyday procedures, and indeed surveys indicate that internal checking routines are by far the most common means of detecting fraud (see Ernst & Young, 1989).

There are moreover few companies prepared to let the lessons of a major fraud pass by without remedial action. But one more proactive development noted during this survey was that some companies are seeking to initiate the same preventive assessments after more commonplace, and minor, frauds.

Actions taken by Dixons, the electrical retailing group, against till frauds are illustrative. Their security team, like many of their counterparts elsewhere in the

retail sector, have frequently produced catalogues of 'till scams' committed by staff, but primarily to assist investigators and management to identify perpetraters. In 1988 this focus was consciously redirected so as to design out the scams at source. A computer consultant was commissioned to work alongside security investigators, initially in order to familiarise himself with the 100 or more fiddles with which they were familiar. He then estimated the losses inflicted by these fiddles, and recommended changes in electronic point of sale (EPoS) software that could close the loopholes **without** prejudicing the speed and efficiency of operations at the tills.

This exercise was by no means successful in eliminating all fraud opportunities and the resulting changes were spread across too many different transactions to be separately costed. Nonetheless, it represents an innovative approach to tackling crime problems at source: at the vulnerable procedure or operation, rather than against the individual(s) who exploit them.

Actions against cheque and credit card fraud

Another obvious area - where though the amount lost from individual fraud incidents may be low, the volume is high - is cheque and credit card fraud. The costs borne by the banking sector last year are estimated to be £120M: some £90M from lost or stolen cards, £20M from fraudulent account applications and £10M attributable to retailer collusion or other fraud (Security Management Today, 1991).

These figures represent a major increase on previous years, and are now leading to much more co-operation between banks and other credit providers. While the first review of cheque and credit card fraud in the UK has recently been completed, which will provide a far more comprehensive summary of preventive activity on this fraud (Levi *et al*, forthcoming), two interesting examples of cost effective measures are given below.

The first - case study 4:2 - summarises the actions taken by 17 banks and building societies to provide an on-line service to retailers when they entertain suspicions about cheque books or guarantee cards presented in payment to them.

Case study 4:2 Check card referral service

Frauds perpetrated by the use of stolen cheque and cheque guarantee cards cause major financial losses to issuing banks, and indeed to retailers who choose to accept such cheques over the guarantee limit.

An initiative taken by Midland Bank against such frauds in 1986, to which many other banks subsequently subscribed, has had a significant payback.

Problem: The losses sustained by all banks from cheque card fraud rose significantly in the early 80s and by 1986 are estimated by the Association for Payment Clearance Services (APACS) to have been of the order of £26.5M.

Midland were not alone in recognising that many of their retail customers were prepared to refer suspicious cases to them: if provided with a fast - and free - service. The advent of British Telecom's 0800 freephone service in mid-86 made this possible and the bank were quick to take advantage.

Preventive Action: *The check card referral service was established in July 1986. All Midland branches were instructed to telephone the service as soon as they were advised by customers of cards, together with cheques, which had been lost or stolen. These details were recorded on a stand-alone PC which could be accessed 24 hours a day, 7 days a week - by staff manning a freephone hotline.*

The service was then publicized at retail outlets. If suspicious card transactions were made and cards were ***not*** *reported as stolen, retailers were also enabled to check further by being provided with other non-sensitive information only the true account holder would be aware of.*

The set-up costs for the 1986 trial system - covering lost or stolen Midland cards only - was £10K (comprising costs of PC and software, BT lines and basic publicity). During late 1986/87 a further 16 banks and financial institutions joined the scheme, and shared additional costs. At this stage further computer enhancements were made totalling £20K. Running costs (primarily manning) between mid 1986 and the end of 1990 *have totalled £120K. In summary, the total cost for all participants has been some £150K.*

Impact: The payback on this comparatively minor investment - estimated by multiplying the maximum guaranteed value of each cheque (£50) by the average number of cheques left in retained cheque books (10) - has been £2.46M. This has grown year on year and is at least 16 times more than the investment in prevention.

There have moreover been 'spin-off' savings for retailers who accept cheques above card guarantee levels. Although these are impossible to quantify, Marks and Spencer were sufficiently impressed by the payback to arrange with Midlands to place the referral service data on hand-held organizers at M and S point-of-sale.

This scheme has not, of course, eliminated cheque card frauds, for not all retailers take advantage. Nor is it the only scheme in operation: others have followed Midland's lead rather than joining a single central scheme. For subscribers, however its benefits is clear.

In the case of credit card frauds - which experienced an increase of 126% between 1988 and 1990 (Levi *et al, op cit)* - most banks see the principal long term means of prevention as on-line authorisation. This will enable any sale to be authorised electronically with the issuer through the retailer point of sale. But the cost of achieving this - even against current fraud losses - are prohibitive. Such control will not moreover inhibit frauds that are committed with cards **before** they are reported lost or stolen. The second case study (4:3) describes an interesting computer application designed to tackle this particular problem.

Case study 4:3 Identifying unreported credit card fraud

A common feature of many credit card frauds is that they occur before the cardholder notices his or her card is missing and before the card issuer can put a block on the account. An initiative taken by Barclaycard has succeeded in effecting early identification of many such accounts by monitoring unusual usage.

Problem: *During 1989 and previous years, some two-thirds of the fraud losses sustained by Barclaycard took place before notification that the card in question was lost or stolen. Indeed, in cases where cards have been intercepted in the post, the customer has no means of being able to forewarn Barclaycard.*

The potential pay-off from earlier identification has long been known: if it can be established fraudulent transactions have occurred, a block can be put on the account which will trigger when transactions are made requiring authorisation (but not, of course, on all purchases). Equally, the number of the card can be incorporated into 'hotcard' files relayed to dealers. Both precautions increase the likelihood of the fraudster being identified: the tendency for the bulk of spending on stolen cards to occur in the first 10 days indicates that fraudsters realize this.

Preventive action: *In conjunction with the Knowledge-Based System (KBS) Centre at Touche Ross, a system was developed which lists accounts with potentially fraudulent spending patterns. Customers are then contacted to establish if indeed they have lost their cards.*

The system operates at two broad levels. A first process selects potentially fraudulent accounts, utilizing general parameters relating to the amount and frequency of 'normal' transactions and the level of activity on new or previously dormant accounts. These accounts are then separately assessed against models of previously-established fraudulent behaviour and indeed the cardholder's individual spending patterns.

Suspect accounts which have been selected through these screening processes are reported to an administrative team daily, who attempt to telephone the cardholder at home or work. If no contact can be made, a telemessage is sent through the post to the cardholder's address, asking them to contact Barclaycard. Should this method fail to achieve contact by the end of the second day a cautionary block is put on the account - which will enable a check to be made on the next occasion an authorisation call is made.

The full development costs for this sophisticated system have totalled £400K. This is not the actual cost to fall to Barclaycard, for three-quarters of the sum (an estimated £300K consulting from Touche Ross) were met by the Commission of the European Community (ESPRIT project). The actual cost borne was the remaining £100K (about £50K end-user computing by Barclays Bank and £50K 'tuning' of the

parameters by Barclaycard, and some CPU time which proved difficult to separate from other computing costs). In addition, the back-up staffing and administrative costs (of the team who contact cardholders) has totalled £100K pa.

Impact: *The full system only went 'live' across all Barclaycard classic Visa accounts in December 1990, but* ***extensive trials in September 90 (against the pattern of transactions on undetected frauds) indicate that the system will prevent some £500K frauds per annum across all card products. This is the equivalent of the true complete development cost and the associated administration for the first year of operation. If sustained, the system will effect a net saving of approaching £350K per annum from 1991 onwards, when running costs will be £150K (£70K administration; £50K continued refinement of the system).***

It is also worth noting that the estimated benefit from this system has been significantly reduced by the effect of Barclay's marked success in reducing the theft of cards in the post (see page 17). Both initiatives targeted this problem, and an earlier trial of the knowledge-based system, prior to use of contracted courier services, had suggested its impact in reducing fraud would be closer to £2M per annum.

Major threats

While few contacts were established with organisations dealing with major money or credit transactions, the message from these was that the higher risks were generally sufficient to justify more rigorous control mechanisms.

Mortgage providers, for example, seem to operate stringent checks and counter-check, designed to ensure that oversights by one department (deliberate or not) will come to light at another point.

Although resource intensive, these controls and strict mandates - covering all the components of a mortgage application, from the evidence presented by solicitors, valuers, the borrower and, ultimately, underwriters - are seldom disputed. This is because the high stakes at risk from even a single fraud are indisputable, and indeed because lenders need to meet the requirements set by their bankers.

One interesting addition recently made to the controls exercised by the National Home Loans Corporation (NHLC) is the use of a "coincidence recognition" programme. This system has strong parallels with applications utilised by the police for major crime enquiries, and is directed at spotting similarities in applications: for example, in names, telephone numbers, dates of birth or postcodes - whether those of applicants, solicitors or valuers.

Its logic (which has similar knowledge-based derivatives to the Barclaycard application described in 4:3) is that any series of fraudulent applications are bound

to show common characteristics, or even mistakes, overlooked by the fraudster himself. Over 100 items are checked. The actual benefit that will derived from this system (which has cost some £100,000 to develop) are not yet known but the view from NHLC is that - at the equivalent to only two frauds on an average-value mortgage - this can hardly be in dispute.

Collaborative action in the credit industry

The control of fraud within the credit industry has in the past been treated primarily as an internal management issue, despite strong informal networks and the activities conducted by the Association of Payment Clearing Services (APACS) against cheque card fraud. There have however been clear signs during the last year that these barriers are rapidly dissipating. Indeed, Levi *et al (op cit)* argue that, were their enquiry carried out even one year ago they would have concluded that the industry was "riven with organisational conflict". By contrast, they currently report so many initiatives that they "are difficult to list adequately".

The very marked increase in fraud losses experienced in 1990 (see above) has been the principal incentive to act. According to a number of those approached this has arisen not only because of increased criminality, but as an unanticipated consequence of fierce industry competition which has sacrificed preventive controls - such as lower authorisation limits -in the bid to secure retail business. The other crucial incentive has been declining profitability.

One sign of the new spirit of cooperation is the willingness of so many to join the Credit Industry Fraud Avoidance System (CIFAS). This pools the information held by its 52 members on a range of vulnerabilities such as applicants who have impersonated another individual, or addresses where fraudulent information has been given in the past. The register is proving its worth to many participants; Levi *et al* (who provide a more detailed account of the CIFAS operation) report that one major card issuer has already achieved a net benefit of over a million pounds from their participation.

Another indication is that both the issuers of plastic cards and banks are now setting up additional, more formal, mechanisms in order to air and resolve their differences. The establishment of the Plastic Fraud Preventive Forum (PFPF) represents a common response to the problem of plastic fraud and is in addition to the work already being done by APACS with regard to cheque card fraud. PFPF was set up in mid-1990 as an umbrella group designed to tackle the fraud problems faced by the finance industry and to initiate projects which will present remedies to common problems. It has now been supplemented (in early '91) by an equivalent banking group operating under the aegis of the Committee of London and Scottish Bankers - the Central Fraud Liaison Unit (CFLU). This unit has been created to coordinate a more formal and consistent exchange of information between the banks about non-plastic fraud and will serve to improve criminal intelligence amongst financial institutions and identify new fraud trends at an early stage. The logic behind this

is the realisation that cooperation is essential if the banks are to confront organised fraudsters, and to ensure that if fraudsters are successfully diverted from plastic fraud they do not turn their attention to other banking crime. Additionally the two initiatives should ensure a common approach to the police whereas at present related enquiries are often duplicated. Coordination should reap benefits for all and enhance the likelihood of successful prosecutions.

Although the type of crimes dealt with are clearly much more complex, this arrangement is in many ways similar in principle to such highly publicised schemes as shop or office "early warning" arrangements (the main component of most business watch). The belief is however that the more formal arrangements adopted (the banks have agreed to fund and staff CFLU as a separate entity for a one year trial) should promise a much more substantial likelihood of success.

5. Responding to violence

The 1988 British Crime Survey (BCS) found that just over a fifth of all assaults against those in employment took place at work and nearly a third of threats (Mayhew, Elliott and Dowds, 1989). To the extent that these threats and assaults arise from the nature of the work undertaken by workers - generally labelled "job related" incidents - government has been keen to stress that, as well as obvious social responsibilities to act, employers have obligations under Health & Safety regulations to take all necessary steps to reduce risk.

Of course a good deal of the violence and threats experienced at work are not specifically job related: workers spend a sizeable proportion of their working hours at their place of employment and disputes inevitably arise with colleagues and co-workers. Workers interviewed for the BCS nonetheless blamed their jobs for about one quarter of violent incidents, and more than a third of threats: and, when they did so, primarily blamed the public rather than their co-workers.

Some of the most vulnerable occupational categories are in the public sector (such as welfare workers and female nurses) which fall outside the sphere of this review. The BCS occupational breakdown was of necessity rather broad (given the small respondent samples in specific occupations), but it did distinguish entertainment managers and security men as suffering more than three times the average risk of violence and threats (and women office managers, too, facing the same risks, but from violence only). It also identified that retail and wholesale male managers face at least twice the average risk of violence and threats. Companies in these general areas of employment-as well as the banks and building societies, where incidents (although perhaps not as frequent) may be more serious - were therefore approached.

The initiatives that came to light took many forms and are best described under three headings: those aimed at establishing risk (as a prelude to other actions); those aimed at reducing the incidence of violence or threatening behaviour; and those aimed at improving the support given to victims.

Assessing risk

Much violent crime goes unreported and a number of the companies approached - principally multiples in the retail sector - have sought to estimate the extent and characteristics of unreported incidents. This has been done for a number of reasons.

In some, there was concern that failure to report might be an indication that employees believed that the company could either do little to avoid repetition or, worse still, did not care (which can have obvious implications for staff morale and retention). Others undertook the exercise as means of establishing a more comprehensive picture of **why** incidents occur, so as to address the root causes.

Finally some took this route to ensure that the company could pinpoint accurately **where** incidents occur, and to avoid any possible bias inherent in the statistics of recorded offences (which may not be uniformly reported simply because, in some areas, incidents are commonplace).

The method typically adopted has been akin to a crude victimisation survey: asking the staff. In the Argos chain, for example, estimates derived from the returns completed by representatives of the staff in each store (the Manager and his/her deputy, a full time and a part time employee) suggested that in 1990 over 200 incidents involving actual physical violence occurred, and many more threats, but only 35 were reported. This serious under-recording, however, was mainly accounted for by regular non-reporting in a small number of high risk stores. These findings are quite consistent with those revealed by Dixons Stores Group (comprising of the Dixons and Currys chains) who used a similar methodology but incorporated their victim surveys into training sessions on identifying and defusing violence (completed by all staff). Both companies also investigated staff perceptions- which, although by no means definitive (because the surveys aimed to elicit group responses, rather than the views of individuals) seemed to suggest that most staff were not particularly fearful and were sanguine that the risks they faced were part and parcel of modern retailing.

Reducing the likelihood of attack

Developing policy which will avert attacks on staff requires clear understanding both of the issues that trigger incidents, and something of the interplay between protagonists. In many cases the precipitating circumstances are difficult to avoid: Marks & Spencer, for example, noted that fully 95% of incidents reported to them arise from the handling of shoplifters, whereas in Argos - with a radically different merchandising style - shoplifting took second place to refund procedures as the primary trigger of violence or threats (45% of all incidents). But even if the roots of violent or threatening encounters prove to be largely unavoidable prior analysis is necessary to establish if steps can be taken to reduce the likelihood of repetition.

One of the less welcome, but pertinant, facts which can emerge from prior analysis ~ unwelcome because it seems to cloud an otherwise clear distinction between 'victim' and 'offender' - is that some staff are less well able to cope with threatening situations than others (see Walmsley, 1986 for general review). There are several instances where research conveying this message has met with fierce resistance from employees' representatives - and indeed employers themselves. But the benefit is that it can point to ways in which employers can exercise some control over circumstances.

Case study 5:1, describing an enquiry commissioned by the brewers Whitbread, provides an example from a company who took up the various challenges presented to them in a consultant's report on violence - and, in consequence, achieved a significant reduction in violent incidents.

Case study 5:1 Reducing violence in public houses

The risk of violence faced by publicans is widely recognised: indeed, the 1988 British Crime Survey indicated the very high job-related risks (from both violence and threats) faced by "entertainment managers" (see above). Action taken by Whitbread Inns has sought both to prevent outbreaks of violence, and to support staff when such incidents do occur. This case study indicates that, simply in terms of reduced staff turnover, the investment was well-justified.

Problem: *In the latter half of 1986, Whitbread Inns received a comprehensive - and critical - analysis of violence in its pubs, commissioned from an outside consultant. Among its many findings this alerted them to the inability of some managers to defuse potentially violent disputes; to the financial penalties incurred when pubs become tarnished with a violent image, and to managers' perceptions that the company was not sufficiently supportive of them after attacks had occurred.*

One of the first responses was to derive a company code of practice in dealing with violent incidents, and to establish proper reporting procedures. Data derived for 1987 lent much credence to the consultants' analysis: some 900 reports detailing actual physical attacks were filed, with over 70% of these deriving from houses where managers were in their first year of service. Moreover 'exit' interviews showed that violence was a major reason for management couples leaving employment with the company.

Preventive actions: *The actions taken in support of the 1987 Code of Practice have been wide-ranging. One of the first steps was to establish a central management post tasked to develop and implement the company strategy.*

This initially focussed on preventing attacks - primarily by the screening of staff who were to assume management posts, by social skills and role play training (especially for the new manager), and by work on the design and layout of high risks sites. Latterly there has been a growing emphasis on the support of staff when incidents do occur (developing basic counselling skills in area managers, improving insurance protection etc.).

Over the four years of this developing programme, the annual cost has been £150K. This includes the cost of the initial consultant's report, for maintaining a training programme (and accommodation/videos) and funding the post of Security/Safety Manager to coordinate the strategy.

Impact: *There are a range of criteria which could be used to justify this substantial outlay. The absolute number of reported incidents has declined to 600 in 1990: a drop of one-third (moreover those involving houses with managers in their first year of service has declined from over 70% to 23% of the total). In view of the increased incentive to report incidents (by a more 'caring' company image, more generous*

terms for claiming injury compensation etc.), this is highly significant. It can be reasonably expected to have been accompanied by lower costs incurred from pub damage, less time off work after attacks and a reduced loss of custom which often accompanies violent incidents.

Benefits can also be measured in terms of reduced staff turnover ***Over the years of the programme, house management turnover has improved from 38% to 25%: the equivalent of some 120 fewer couples each year. On a conservative estimate that only 10% of this improvement might be attributable to the policy (and by 1989, only 2% of couples mentioned violence as their reason for leaving in 'exit' interviews), the company cost of recruiting and fully training 12 couples would be of the order of £240K per annum. This alone is substantially more than the cost of the programme.***

Supporting victims

Of course not all violent or threatening incidents are avoidable. One of the more forthright messages to emerge from this enquiry was that many companies now recognise that there can be substantial hidden costs if they fail to adequately support staff who are subjected to violence or threats.

The experience of Abbey National, one of the first organisations to grasp this increasingly familiar message, is illustrative. In 1988 it came to the building society's (as it was then) notice- from both union representatives and those in their personnel department monitoring sickness absences - that their follow-up procedures after armed raids were failing them. Responsibility for follow-up had long rested with area general management, but as the frequency of attacks increased there had been a tendency to delegate downwards to lower management - who were perceived to be well-meaning but insensitive in their dealings with victims.

A preliminary assessment of the problem was commissioned from an occupational psychologist. This confirmed that it was not unusual for employees' perceptions of the organisation to take a sharp knock after such incidents. The evidence was sufficient for Abbey National to persuade five other building societies (most of whom had, at about that time, been assisting a Home Office enquiry into the building societys' high vulnerability to robbery: see Austin, 1988) to join forces with them. They commissioned the Roehampton Institute to carry out a more extensive, sector-based, analysis. This subsequently revealed the difficulties were not unique to Abbey National.

The policy of going outside the host organisation for advice has merit in that it ensures some impartiality in assessment: important when 'in-house' enquiries can be tainted with the same company image that may have been generated after an incident. It has been followed elsewhere. In 1989 the Dixons Group, for example, commissioned an external report from Leicester University on this same subject ~ which reported not dissimilar reactions from staff.

Those companies who have identified difficulties of this nature have tended to follow one of two courses. Abbey National, even before receipt of the final Roehampton report, initiated a new policy towards both the prevention of violence and post-raid support. The launch was backed by a training video based on a simulated branch raid which, among its various components, introduced staff to new touch-button screens which can be instantaneously activated by those under attack. More stringent follow-up procedures which were initiated also ensured that staff from the company's occupational health department attend every branch. This is initially done on the second or third day after a raid ("after the dust has settled") with all staff present at the time, including the manager (who many tend to assume 'will cope'). Staff are privately interviewed and offered counselling and the procedure is repeated - whatever respondents' reactions initially - about six weeks after the event. These sessions are in total confidence - and this principle is categorically recognised by all in the company.

While Abbey National has chosen to provide counselling from an internal department (except in extreme cases where this is plainly insufficient), some other companies have opted to employ external services. In 1989 Midland Bank, for example, chose to enlist the services of independent counsellors who are now advised of all reported bank raids. They attend each to offer - but not, of course, pressurise - all involved access to their services. When appropriate they will include customers. This approach obviously reinforces the important theme of confidentiality.

All of the companies involved in providing these support services expressed the view that the primary benefit was intended for the individual victim - and for this reason few attempts had been made to assess **corporate** benefits. At the same time they firmly believed that these did materialise in various forms - such as in the reduction of staff absences after raids or in minimizing the inefficiencies which trauma can cause. The only organisation surveyed where even rudimentary attempts had been made to assess the corporate spin-off was Northern Ireland Electricity: see Case Study 5:2.

Case study 5:2 Justifying support for staff after violent incidents

Few employers challenge the view that they have an inescapable responsibility to support their staff who are upset or traumatised as a result of job-related violence. But evidence that, by so doing, they can achieve actual cost savings has dividends. It can transform a purely reactive response to reported cases to a far more proactive and exhaustive programme aimed at identifying cases and responding speedily. While the evaluation of counselling or similar support activities is inevitably problematical, some general estimates of the impact of Northern Ireland Electricity's support programme can be derived.

Problem: *Electricity employees not only share the risks of instrumental violence - perpetrated by those seeking to steal cash or electrical merchandise - common to retail operations, but also a good deal of the sort of violence meted out against those in positions of authority (such as benefits officers, social workers, etc). The latter will arise, say, in circumstances when customers are advised that their supply will be cut off because of the non-payment of bills, or in conducting preliminary enquiries into cases when meters have been tampered with. To supplement these 'industry' problems, many employees of Northern Ireland Electricity face increased exposure to attack and stress arising from the social and political tensions in the province (such as in a recent case when workers on a cabling crew innocently become witnesses to sectarian killings).*

Costs arising from inaction: *NIE has a long tradition of providing comprehensive support for staff who become victims of violence, but their experience of a minority of cases where they* ***fail to get early notification*** *(often because of the outward air of normality initially displayed by victims) serves as a constant reminder of the consequent costs.*

These costs, for example, can comprise pay for absenteeism following an incident (the sick pay scheme is generous, with most cases qualifying for full pay for the first six months); overtime required to be paid to others who have to cover the duties of the absent individual (especially important for shift workers at power stations or cabling teams); the need for consequential actions like transfers or early retraining, or superannuation and insurance paid to those rendered permanently ill or indeed killed (as has happened in two cases in the past year).

Most of these cost are extremely difficult to separate. Absenteeism is the most finite: NIE calculate the average cost borne by the organisation for any absent individual is £12K per month. Applying these general costing conventions to violent incidents which go unreported (although naturally cases differ widely) NIE indicate that conservative estimates might be:

— *absenteeism after serious cases of direct assault is typically about six months, or some £7.5K per case;*

— *absenteeism after less serious cases involving threats is typically about four months, or some £5K per case;*

On the basis of the actual number of individuals receiving counselling by NIE last year the corporate "exposure" can be crudely calculated. Some 15 victims of direct assault were dealt with (15 x £7.5K = £110K approx) and 20 victims of major threats (20 x £5K = £100K). On the basis of these reported cases alone, therefore, the corporate exposure for absenteeism could be estimated to be some £210K.

Preventive actions: *The policy of NIE is that local management are required to inform the Health and Welfare department immediately following the occurence*

of incidents (local management themselves are instructed to deal only with practical issues like basic legal advice, claims, sick pay details etc). On notification, Occupational Health nurses visit all involved (at home, work or hospital) to provide a first-line assessment of their medical condition. This is followed by an interview with the NIE Medical Officer who carries out a more comprehensive analysis of the incident and its aftermath with the victim. He then schedules further appointments or decides to refer to external specialists (in most cases specialists in post-traumatic stress disorder).

Cost of preventive programme: *As the service to crime victims provided by the Health and Welfare Department of NIE forms only one part of their workload a reasonable estimate of their involvement can be provided by referring back to their caseload in the last full financial year. The combined cost - in terms of staff time, transport and administration - of responding to the 35 victims given counselling support (referred to above) was 15K in internal costs and £2.8K in external medical services: or a total of about £8K (including staff time). On top of this the 35 victims obviously had to receive additional, purely financial, support for the time they were actually absent from work. The sickness absence for these actual cases was 95 months in total, or a cost of £114K to NIE.*

In total, therefore, the cost of responding positively to these 35 cases and meeting their absenteeism was around £122K, compared to the estimated company exposure of £210K from absenteeism alone: a financial dividend.

While this analysis is by necessity crude, it is also a minimum estimate and overlooks many of the less tangible benefits - such as minimising overtime paid to others, retraining and so forth - which are also likely to have accrued.

Notwithstanding the inability of other principal respondents (Abbey National, Lloyds and Midland Banks) to cost their actions precisely, all perceived that hoped-for benefits had been realised. These operated at two levels. First, and most obviously, feedback from staff themselves has proved to be extremely positive. Second, and less expected, they reported that follow-up interviews and counselling have been instrumental in identifying shortfalls in security procedures, or training in these, that have required remedy.

More general lessons have also been learnt about past practices that have confirmed companies' commitment to their new policies. For example, the common reaction of sending people home to get over incidents is now viewed as inappropriate inmost cases: the ability to turn to work colleagues who shared the same experience to talk through events is invaluable. Visits from the "top brass" of the company are recognised a imposing additional pressures. And indeed individual rewards are distributed with care - for they can heighten feelings of guilt among those who believed they could perhaps have done something to avoid attack. To professionals like Victim Support - who obviously welcome signs that businesses are now

recognising victims' needs - these sort of lessons are crucial. They do however have some reservations that companies may turn too readily to stress counsellors who may apply "disease" models of treatment - addressing a victim's "problem" - and overlook some of the unique characteristics of the **crime** victim.

Some occupations are clearly more prone to job-related violence than others. From the evidence assembled in this cursory overview, the signs are that the financial services sector are leading the way in their response to violence, and that the retail sector is following in the same direction. Oil companies, too, are now attempting to grapple with the same issues - in early 1991 setting up three working parties into violence on petrol forecourt (looking closely at design and planning; physical security and training) under the aegis of the British Oil Industry Service Station Committee. This appears to be one of the first concrete signs of industry cooperation and may be indicative of future trends.

6. Summary and discussion

In attempting to draw together some of the wider implications of this commentary on business initiatives, the exploratory and random nature of the enquiry deserves restatement. It was limited in scope and range and thus provides little more than an initial excursion into the extremely wide ranging and diffuse effort business has invested into crime prevention.

This should invite caution: but there are nonetheless several themes that emerged - not only from the initiatives described by businesses, but also from the broader discussions of approaches taken by business respondents.

Observations are presented under four headings. The first comments on the nature of business perspectives of crime problems, and their perception of risk. The next three headings deal more directly with prevention: with problem identification; with investigating alternative remedies and their implementation, and finally with evaluation.

How crime is perceived

Crime risk management, which has been the central focus of this report, is not firmly established. It is however a concept that can be more readily grasped in the boardroom, for managerial perceptions of crime problem are quite different to those of the police.

The police service is tasked to prevent and detect crime, and while it is under unmistakable pressure to do so more efficiently and selectively than in the past, these objectives remain paramount. In contrast, businesses facing crime problems have no such direct responsibility and will often choose (perhaps more than the individual victim) **not** to respond in any way. Appeals to companies' social responsibilities invariably cut little ice. Their primary objectives are profitability - and survival. To the extent they subject their options to rational assessment, their inaction suggests they have not being able to successfully identify remedies that will justify additional expenditure on resources.

But while the realities of business can drive commercial managers to exercise the principles of 'crime risk management' in a way that traditional law enforcement agencies can seldom grasp, successful execution depends - in the first instance - on comprehensive assessment of the losses being sustained from crime, of how these occur, and of emerging vulnerabilities. These **functions are underdeveloped in nearly all companies.**

One clear message emerging from this enquiry was that where crime risks are undeniable and controllable - such as at warehouses or factories, holding valuable

assets, in the transportation of large sums of money, or in the handling of major financial transactions - few companies will dispute the necessity of making substantial sums available for protection.

The payoff from prevention is however clearly more tenuous in operations involving **high volumes** of transactions - retail operations, day-to-day payments by cheque or credit cards, and so on - where unimaginative solutions invariably prejudice operational functionality with little certainty of compensating payback.

But even in these difficult conditions, the review offers evidence that, once alerted to shared risks and persuaded that there are surmountable, many positive industry initiatives have been mounted and proved their worth. The common hallmarks of the more successful are that they have been targetted at quite specific problems - nearly all emanating from external threats - and joint action has been supported by all the principal losers. This is a marked contrast to some of the more broad-ranging and perhaps over-ambitious schemes that are occasionally embarked upon. For example, a recent enquiry into the joint actions against crime and nuisance taken by companies tenanting industrial estates (Johnston et al, forthcoming) attributes most failures to the absence of adequate shared information about risks, consequent misdirection of effort and only partial support for the actions taken.

There is also some evidence from this enquiry that the criminal 'grapevine' - initially amongst company employees, but quickly spreading to outside the business - is fairly rapidly alerted to the vulnerabilities of these high volume operations.

Unless quickly identified and removed, the exploitation that follows can be extremely damaging. Good examples from this report include the 'run' on National Savings frauds experienced in the early 80's (which threatened the future viability of this account), the growing prevalence of credit card intercepts in the post or - for more professional teams - the hijacking of cigarette lorries and thefts of aluminium casks. This mushrooming of offences against one target has no parallel in theft-related offences against the individual, and early warning can seldom be extricated from police statistics. Yet the threat they can pose to the unaware business is substantial.

Problem identification and costing exposure

There has been an inclination in the recent debate about business crime to dissasociate the **investigative** function performed by internal security departments from a more desirable focus on **prevention.** This has served to remind companies that favour the investigative model that the detection and prosecution of offenders are - in isolation - unlikely to have significant impact on overall loss: a point that was reinforced in the 1989 shrinkage survey undertaken by Touche Ross (Touche Ross/APTS, 1989): this showed companies arresting high numbers were no more effective in controlling shrinkage than others.

It should not however obscure the fact that detections are an invaluable source of information about current vulnerabilities. Indeed in a number of the case studies reviewed investigators have uncovered vulnerabilities and sources of substantial loss that have hitherto to been completely overlooked. The lesson is to focus attention on the methods used by detected offenders in order to transform operating procedures and so deny others similar opportunities.

Feedback from known crimes are not the only route to identifying vulnerabilities. Nor, indeed (given the limitations that businesses face in establishing where losses occur) can stock or other routine audit procedures be the sole guide. One of the most consistent messages of recent crime prevention literature is that crime owes much to the opportunities presented to the potential criminal, and the case studies here suggest that system or procedural loopholes quickly come to be apparent to company staff operating them on a day-to-day basis. These vulnerabilities can be recognised by "risk audits" which can usefully draw on the experience of selected staff operating each procedure. Risk audits should not however be purely theoretical, for the case for prevention is much stronger if they can go on to establish whether opportunities are actually being exploited.

As a final, but essential, stage of establishing the need for anti-crime actions, the full impact of the criminal activity noted by these various processes need to be established. One of the more innovative developments coming to the notice of this enquiry has been the move some companies have made to looking beyond the superficial costs associated with a particular crime incident, to more comprehensive costing. The "cost of security failure" project currently being undertaken by BT's Security and Investigation Directorate, which aims to fully document the costs of 105 routine security failures borne by the company, is the best example: Case Study 5:1 gives details about just one of the crimes.

Case study 5:1 Establishing full crime costs: BT van break-ins

A striking example arising from BT's "cost of security failure" initiative was a detailed examination of the losses sustained from thefts of and from engineers' vans.

'Traditional' Costing: *The accepted wisdom within BT (as with most other businesses) was that the value to be attached to this form of crime comprised simply the loss of any equipment (primarily tools and telephones), and the associated costs of damage sustained to vehicles themselves. These should be expressed at 'rate book' values (ie. cost price) as this constituted the actual cost of replacement borne by the business.*

In 1989 there were 4,500 attacks on parked BT vans, leading to £1M loss of equipment expressed at these "rate book" values.

'Comprehensive' Costing: *BT's current initiative attempts to provide a more complete analysis of the actual loss sustained by their business by this form of crime — and involves both re-assessment of direct costs, and enquiries into a range of indirect consequences. The dimensions include:*

— *expressing the loss of telephone equipment at market value (i.e. cost inclusive of margin, VAT etc.) as an indication of* ***revenue lost;***

— *assessing the lost 'down time' of engineers who are unable to perform their duties because they have to wait to have tools or equipment replaced, or vehicles re-instated;*

— *estimating the damage to vehicles:*

— *above all, estimating the detrimental effect on morale of a continuous problem of break-ins.*

These full costs are not all easily quantifiable, but the costing of those elements where this is possible has caused BT to **upgrade their estimates of their 1989 losses from vehicle attacks substantially. These are now estimated to have been £2.5M, or 250% more than was calculated using "traditional" methods of costing.**

Lesson: *The major implication of this particular analysis has been to cast the costs of preventive action taken to protect vehicles themselves (or the premises in which they are housed overnight) in a more favourable light. In 1989 selected BT vehicles in high risk areas were fitted with inner grilles with slam locking mechanisms (easily operable even by engineers who are loaded with equipment and tools). The cost of these devices was modest and the outlay has been more than justified by a reduction in successful attacks and in the associated loss of equipment.*

Others are pursuing the same logic. The hidden costs of crime have been considered in some detail by the Royal Mail letters business of the Post Office. For example, burglaries of sorting offices between 1988 and 1990 have had an average **visible** loss figure of about £1500 per incident. Against this, the average **invisible** loss - in compensation paid for registered letter thefts, for reconstituting violated mail, repairing physical damage, audits and the cost of keyholder attendance - has been calculated to be about £5K per incident. In other words, leaving aside the inconvenience borne by customers, and the consequential damage to the reputation of the Post Office, 'knock on' costs are some three times the value of property stolen. Recognition of these more meaningful costing conventions has played a significant part in justifying major investments to improve the alarming and physical protection of premises (measures which have effected a reduction in the **visible** losses from £258K in 1988/9, to £186K in 1989/90 and £20K in 1990/91).

Identifying means of prevention and implementation

Crime prevention practitioners in business need a wide knowledge base: about crime itself, investigation and the criminal justice system - but also about all of the particular business operations with which they deal. There is naturally enough no formal training package that can adequately equip anyone for so wide a brief (although a number of universities are developing courses to deal with specific areas). All the evidence - from this survey and elsewhere (see, for example, Elder, 1989) - is that businesses themselves are divided in their views of whether those responsible for their crime management should possess formal police or business experience. When they opt for the former it is commonplace for something of a divide to exist between the crime manager and their business counterparts - with the commercial arm believing that practitioners do not fully grasp the complexities and exigencies of business operations (a point similar to that made by business about the police handling of fraud) or that solutions are impractical.

While this problem relates largely to reaching agreement with business managers on strategy, those responsible for fostering crime prevention in business also face another problem entirely familiar to the police: the job of 'selling' prevention to those responsible for day-to-day operation of controls. The familiar message to emerge from this exercise is that preventive procedures or operations which do not originate from those responsible for implementation - or which are at least not properly 'sold' to this group - face an uphill struggle. This is one reason that practitioners in business, like the police, expend great effort in trying to ensure that security devices or disciplines are involuntary, or effected automatically.

Amongst practitioners, many see the source of both difficulties (reaching agreement on directions and everyday operational support) as inescapably rooted in the organisational framework of the corporations of which they are part. In the main these locate risk management departments as standard **cost** centres - with budgets borne from corporate resources but with no means of benefiting from cost effective activities. There are however alternative administrative arrangements. On a continuum, these can be characterised as **charging** centres (where charges are at least levied on service receivers), which are not uncommon; **business** centres (where security, while remaining an internal non-profit making. operation, enters into contractual arrangements with its various customers - who are given the option to buy similar services elsewhere); and **profit** centres (where, in addition to competing for in-house business, the function can operate outside organisational boundaries and profit from this).

While commercial 'profit centre' operations fell outside the remit of this survey, one example of the business centre model is the Post Office Investigation Department (POID). This department, which functions as part of Post Office Headquarters, attained this status as a consequence of the Post Office division into three seperate operating companies. These companies call on POID services - whether for one-off investigations, routine surveys or protection - on a strictly

contractual basis (which is reflected in the fact that some will buy services similar to those offered by POID from outside the Post Office, or indeed meet the same needs from in-house resource). While POID is constrained by the provisions of the Post Office Act from operating as a fully fledged profit centre (ie. selling its services on the open market), nonetheless its entire budget and manning levels are dictated by its revenue.

In principle one of the casualties of such an arrangement could be the loss of skilled resources, familiar with the host businesses' operations, that can often prove to be the 'whistle-blowers' on undiscovered crime. In an attempt to overcome this weakness, POID also operates arrangements which allows them - with the agreement of operating companies -to conduct speculative enquiries on what are called "windfall" charges. These cater for circumstances where, while operating companies may not be fully persuaded to buy services direct, they are content to allow special enquiries - funded at POID'S **own** expense - which can be paid for by an agreed percentage of any consequent savings. A well publicised enquiry completed recently on this basis was an investigation for the Royal Mail into the fraudulent recycling of postage stamps: an enquiry which led to the identification and prosecution of a large scale, and sophisticated, team which had defrauded the Royal Mail of something of the order of £10m in stamp revenues.

There are many factors dictating how and why each company operates its internal security function in the way that it does. The models described here are not universally transferable. But the benefits of the various alternatives to the standard cost centre are not simply related to image. The idea of injecting 'market' realities into this area can meet important criticisms: ensuring that service users truly need and will fully utilise the services provided for them - and that service providers adequately recognise and strive to meet the wider objectives of the businesses they serve.

Evaluation

The case for monitoring and evaluating crime prevention measures is largely self-evident: without this discipline there is no way of developing initiatives to full effect, of tuning them to respond to inevitable adjustments in criminal methods - or indeed of justifying their continuation. These arguments are not diminished by the indisputable difficulties associated with evaluating anti-crime activity.

While this loose overview has provided a range of instances where within reasonable bounds, crime prevention measures can be reported to have been evaluated **and** justified, it should not be taken as indication that the evaluation of such initiatives is routine practise throughout the business sector. **In the majority of cases this is not done.** But the rigours of operating within a business environment do provide some impetus and it is probably true to say the situation is on balance better than that prevailing in the public sector (Home Office, forthcoming).

All the signs are that businesses with in-house crime management services - and the practitioners within them - would do well to develop these evaluative disciplines. The move to business or profit-centre models is - in its own way - a means of imposing this: obliging practitioners to prove their worth in straight business terms. No doubt any such moves would spark fierce debate about evaluative criteria to be applied. But within the business environment there can be no stronger justification for the continuation of crime prevention practise.

Appendix: Organisations contributing

Companies

— Abbey National
— Argos
— B and Q
— Barclays Bank
— Barclaycard
— BAT
— British Telecom
— Cogitare Ltd
— Courage Brewing Ltd
— Digital Equipment
— Dixons Group
— Group 4 Securitas
— Hanson
— Kingfisher Group
— Legal and General Assurance Society
— Lloyds Bank
— National Home Loans Corporation
— National Savings
— Northern Ireland Electricity
— Marks and Spencer Plc
— Midland Bank
— P and O Containers Ltd
— Post Office
— Royal Mail Letters
— Sainsburys
— Securicor
— Shell
— Sony Music
— Standard Tyre and Exhaust Ltd
— Tesco Stores Ltd
— Touche Ross Management Consultants
— Trafalgar House
— Whitbread
— Woolworth

Representative organisations, etc.

— Association for Payment Clearance Services (APACS)
— British Oil Industry Service Station Committee
— Brewers' Society
— CBI
— Credit Industry Fraud Avoidance System (CIFAS)

— Crime Concern
— Electrical Retailers Security Association
— Loss Prevention Council
— Tobacco Advisory Council
— Victim Support
— Wine and Spirits Security Liaison Ltd

References

Austin, C (1988). *The prevention of robbery at building society brunches.* Home Office Crime Prevention Unit Paper No 14. London: Home Office.

Burrows, J. (1988). *Retail Crime: prevention through crime analysis.* Home Office Crime Prevention Unit Paper No 11. London: Home Office.

Campbell, D. (1991) *That was business, this is personal: the changing face of professional crime.* London: Mandarin.

CBI/Crime Concern (1990) *Crime: Managing the business risk.* London: CBI.

Crime Concern (1990) Safer *Communities - Making Them Happen.* Report of proceedings at the 1990 AGM conference. Swindon: Crime Concern.

Ernst and Young (1989) *Fraud '89: the extent of fraud against large companies and executive views on what should be done about it.* London: Ernst and Young.

Elder, A. (1989). *Shrinkage in UK multiple retailing.* University of Stirling: Institute of Retail Studies.

Ekblom, P. (1986). *The prevention of shop theft: an approach through crime analysis.* Home Office Crime Prevention Unit Paper No 5. London: Home Office.

Home Office (1988) *Report of the Working Group on the Costs of Crime.* Home Office Standing Conference on Crime Prevention. London: Home Office.

Home Office (forthcoming). *Report of the Working Party on the local delivery of Crime Prevention.* London: Home Office.

Johnston, V., Leek, M., Shapland J., and Wiles, P. (forthcoming) *Crimes and other problems on industrial estates.* Home Office Crime Prevention Unit Paper. London: Home Office.

Levi, M. (1987) *Regulating Fraud* London: Tavistock/Routledge.

Levi, M, Brissel, P. and Richardson T. (forthcoming) *The Prevention of Cheque and Credit Card Fraud.* Home Office Crime Prevention Paper 26. London: Home Office.

Mayhew, P., Elliott, D. and Dowds, L. (1989) *The 1988 British Crime Survey.* Home Office Research Study no 111 London: HMSO.

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

Security Management Today (1991) *Credit card fraud 'set to explode': banks warn* item appearing in Vol 1 No. 4.

Southall, D. and Ekblom, P. (1985). *Designing for car security: towards a crime-free car.* Home Office Crime Prevention Unit Paper No 4. London: Home Office.

Touche Ross / APTS (1989). *Survey of retail shrinkage and other stock losses.* London: Touche Ross Management Consultants.

Walmsley, R. (1986). *Personal Violence.* Home Office Research Study 89. London: HMSO.

Winfield, M. (1990). *Minding your own business: self regulation and whistle-blowing in British companies.* London: Social Audit.

Crime Prevention Unit Papers

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

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

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

4. **Designing for Car Security: towards a crime free car.**
   Dean Southall and Paul Ekblom. 1986. v+25pp. (0 86252 222 6).

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

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

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

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

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

10. **Getting the Best Out of Crime Analysis.**
    Paul Ekblom. 1988. v+38pp. (0 86252 307 8).

11. **Retail Crime: Prevention through Crime Analysis.**
    John Burrows. 1988. v+30pp. (0 86252 313 3).

12. **Neighbourhood Watch in England and Wales: a locational analysis.**
    Sohail Husain. 1988. v+63pp. (0 86252 314 1).

13. **The Kirkholt Burglary Prevention Project, Rochdale.** David Forrester, Mike Chatterton and Ken Pease with the assistance of Robin Brown. 1988. v+34pp. (0 86252 333 8).

14. **The Prevention of Robbery at Building Society Branches.** Claire Austin. 1988. v+18pp. (0 86252 337 0).

15. **Crime and Racial Harassment in Asian-run Small Shops: the scope for prevention.** Paul Ekblom and Frances Simon with the assistance of Sneh Birdi. 1988. v+54pp. (0 86252 348 6).

16. **Crime and Nuisance in the Shopping Centre: a case study in crime prevention.** Susan Phillips and Raymond Cochrane. 1988. v+32pp. (0 86252 358 3).

17. **The Prevention of Fraud.** Michael Levi. 1988. v+19pp. (0 86252 359 1).

18. **An Evaluation of Domestic Security Surveys.** Gloria Laycock. 1989. v+33pp. (0 86252 408 3).

19. **Downtown Drinkers: the perceptions and fears of the public in a city centre.** Malcolm Ramsay. 1989. v+23pp. (0 86252 419 9).

20. **The Management and Prevention of Juvenile Crime Problems.** Barrymore Cooper. 1989. v+63pp. (0 86252 420 2).

21. **Victim Support and Crime Prevention in an Inner-City Setting.** Alice Sampson and Graham Farrell. 1990. v+27pp. (0 86252 504 7).

22. **Lagerland Lost? An experiment in keeping drinkers off the street in central coventry and elsewhere** Malcolm Ramsay. 1990. v+38pp. (0 86252 520 9).

23. **The Kirkholt Burglary Prevention Project: Phase II.** David Forrester, Samantha Frenz, Martin O'Connell and Ken Pease. 1990. v+51pp. (0 86252)

24. **Probation Practice in Crime Prevention.** Jane Geraghty. 1991. v+45pp. (0 86252 605 1)

25. **Lessons from a Victim Support Crime Prevention Project.** Alice Sampson. 1991. v+41pp. (0 86252 616 7)

26. **The Prevention of Cheque and Credit Card Fraud.** Michael Levi, Paul Bissell and Tony Richardson. 1991. v+52pp. (0 86252 633 7)