10

Guides to Practical Bookselling

Loss Prevention & Security

Produced by the BA Loss Prevention Consortium

LOSS PREVENTION & SECURITY

This Guide has been written with extensive help from members of the BA Loss Prevention Consortium (BALPC). NB: The law is stated in general terms only as at the date below - professional legal advice may be required.

CONTENTS

INTRODUCTION

The total cost of crime to UK retailers is over £2 billion per annum (*British Retail Consortium: Retail Crime Survey*), with anywhere between one half and one third of this being spent on crime prevention measures. All of this cost comes directly off the bottom line, reducing profitability and exposing staff to danger, which could just be the tipping point that brings a business down.

By far the biggest loss is customer theft, though staff theft can also be very damaging as individuals working on the inside can steal more. There are also losses and costs involved in dealing with fraud, robberies, burglary and criminal damage. The other major cost for retailers in this area is in dealing with information security and the possible threat of terrorist action.

There are many ways of preventing and detecting crime and technology can help, but there is no substitute for staff vigilance and there are methods that can be used that don't necessarily have to cost the earth.

This guide to loss prevention and security will give some basic and advice in all the main areas, but it cannot cover everything and there are always new products and services coming onto the market. More information, which is updated on a regular basis, can be found on the BA's website. The BA's Loss Prevention Consortium (BALPC), consisting of senior managers from all the leading bookshop chains, is also there to help all members with free advice in the drive to reduce losses and ensure that bookshops remain a safe environment for everybody, staff and customers alike.

PERSONNEL

Your staff are your best asset in preventing loss and keeping your stock and premises secure, but remember that you also have a responsibility toward them not to put them at risk.

- Have a written policy and make sure all staff are trained in the security aspects of the business.
- Ensure adequate staffing levels - the presence and alertness of staff is by far the biggest deterrent to theft.
- Fit warning bells to enable staff to call for assistance from colleagues.
- Keep a security log and include - date & time of incident/brief details/action taken/person making the entry/managers comments.
- If staff are working alone or late at night, then you must carry out a risk assessment.
- Consider employing a keyholder service for out of hours alarm calls.
- Consider employing security guards - full-time or part-time/employed or from an agency.
- Check guards are registered with the Security Industry Authority (SIA).
- www.the-sia.org.uk
- Shop staff can also volunteer as Special Constables under the ShopWatch scheme:
- www.shopwatch.info

MANAGING THEFT

Managing Customer Theft

Shop & Stock Layout

- Before undertaking any major refurbishment, ask for advice on security aspects.
- To prevent the public gaining access to restricted areas, doors to off sales areas should be fitted with a lock or be alarmed if they are a fire escape route.
- Thieves like cover, so high shelving, spinners and quiet corners should be avoided.
- Make sure that lighting is adequate and there are no dark corners.
- Consider using convex mirrors for blind spots, but remember that thieves can use them too!
- Keep the shop tidy and free of clutter - do not provide camouflage for thieves.
- Keep shelves tidy and organised to help keep track of stock.
- Display high value and easily stolen merchandise near to a till point or in a location which staff can easily monitor.
- Minimise the number of copies on display.
- Consider empty display cases and a masterbag system for CD/DVD.
- Consider lockable display cases - ensure keys are kept handy but safe.
- Display notices stating which security equipment is being used and that thieves will be prosecuted.

Spotting The Non Shopper

What is the Non Shopper?

- Person or persons who enter your premises who at the time they enter the premises or after they have entered the premises form the intention to remove product from the store with out payment (ie theft).
- Until they have formed the intention and then selected the goods and some form of concealment/non payment they are not thieves they are **Non Shoppers**.
- Non Shoppers do not look any different from you and I.
- However, their body language and intentions are different from the genuine customer and this gives us the ability to spot them.
- Non shoppers are more worried about you than you are about them.
- On entry to your premises they are looking to see where you and the staff are.
- They are looking to see what security measures you have in place CCTV, EAS, guards, store detectives and staff & customer awareness of their presence.
- They have a secondary interest in the product.

Distraction Techniques:

- Non Shoppers often work in teams.
- One or more may act in an openly suspicious manner to deflect attention from the actions of another.
- Tricks may be used, such as picking up three products and replacing just two, while pocketing the third item.
- "Accidentally" knocking products off a shelf, then replacing some of the items with an apology, while pocketing the rest.
- Concealing product to be stolen, then purchasing one or two inexpensive items to deflect attention and reassure any casually suspicious observer.

Every staff member should take ten minutes and consciously watch their customers shopping. By understanding how your customer shops you will soon spot the Non Shopper:

- Watch how they enter the store.
- Their movements through the store.
- Their interest in the product.
- Their approach to staff and other customers.

Everybody given the right pressures and circumstances is capable of theft and violence.

Three reasons for theft:
- Need
- Greed
- Revenge

Three types of Non Shopper:
- Professional
- Addiction driven

- Personal consumption

We all have deep seated involuntary actions and reactions when committing theft.

- At the point of theft the main concern is “Am I going to get caught”.
- All the moral judgements have been made.
- All of the immediate consequences have been dismissed.
- The majority of Non Shoppers rely on anonymity.
- On most occasions when you spot a Non Shopper they will spot you.
- Many people who spot thieves do not believe what they are seeing.
- Rely on your instincts.

When you spot the non-shopper they will spot you.

- They need to prove that they are not a Non Shopper
- Extended eye contact
- Body to body reactions
- They will touch product

This is your opportunity to deal with the Non Shopper.

- “I see you are interested in “X”.
- “As you can see we have “X”.
- “What are you looking for?”
- Always ask open questions to avoid a Yes/No answer.
- Hand them a basket for the product.
- Escort them to the tills.
- Turn the potential theft into a sale (A Win/Win).

Studies in the USA and the UK have indicated that by engaging a Non Shopper in a conversation of greater than 30 seconds and more than three exchanges reduces the likelihood of theft by that non shopper that day by 90%.

After the Non Shopping incident, ensure that you collate all incidents to gauge your exposure to Non Shoppers.

- Are you being targeted by one or more from a particular group of thieves?
- What product is being targeted?

With thanks to Geoffrey Northcott, Head of Loss Prevention, Borders International

Managing Staff Theft

Typically within retail more than a third of all losses result from staff theft, although within bookshops it is probably much lower. However, even if the incidents are few, the amount of cash or goods stolen is usually much higher than losses from customer theft.

A study by the Centre for Retail Research identified wearing or carrying merchandise out of the store, bogus refunds, taking cash from the till and loyalty card fraud as major causes of loss. Collusion between staff and customers ('sweethearting') was also doing

substantial harm to the bottom line as it reduces the risks of detection associated with other types of staff theft.

New and temporary staff are more likely to be involved in theft, but a surprising number of managers and senior administrators - people with privileged access who can potentially steal over several years - are also routinely caught.

Clearly prevention is better than detection and there are several steps a retailer can take.

- Always undertake systematic background screening of job applicants. Do not take CVs at face value, not least since some of the most dishonest people are also some of the most plausible.
- Require new employees to undergo induction training to clarify their duties, responsibilities and procedures. It can be difficult - and potentially unfair - to act in some cases of malpractice if employees are unaware of the required standards or procedures they must follow.
- Let employees know where they stand through their contract of employment describing the clear consequences of theft and the employer's right to prevent it. For example, the right to search bags or the use of CCTV. (Note that the law sets strict rules for the use of surveillance technology in public places and employee consent is an important factor – see www.informationcommisioner.gov.uk
- Make it clear that all incidents of theft will be thoroughly investigated and reserve the right to take actions on an 'as needed' basis by including a provision in contracts of employment.
- A disciplinary policy to deal with theft is essential. Staff must be made thoroughly aware of the consequences that will follow if they are caught stealing. The policy should set clear limits by describing precisely where perks end (eg for staff purchases or discounts) and theft begins.
- Act to reduce opportunities and temptations for dishonesty. For example, try to ensure that at least two people close up at night and that keys held by employees are engraved 'Do Not Duplicate'.
- Till systems will provide exception reports. Make sure these are always examined and take time to question staff about any items highlighted. If staff know these will be taken up, far less errors will go missing.
- Be alert to warning signs. Although one of the most common reactions to catching a dishonest employee is 'I would never have suspected him/her', some common factors are usually present. This can include - employees who habitually violate rules, have a substance abuse or gambling problem or who feel aggrieved toward the employer.
- Provide employees with lockers or a secure area for their personal effects and then prohibit them from the shop floor.
- Consider deterring staff theft by initiating random searches of bags and packages leaving the premises. Take some time to ensure that the procedure is patently random and without basis.

A firm but fair policy to employer and staff alike should help reduce staff theft.

Tackling The Thief

- Arresting a thief is fraught with problems and can be extremely dangerous. The aim should **ALWAYS** be to **PREVENT** a theft rather than make an arrest.
- Every company and organisation should also have a written policy in this area to ensure that correct procedures are always followed.
- Never leave the premises and pursue a thief out of the store. Staff and customer welfare is more important than property.
- The suspected shop thief may pose a physical threat to employees or customers and one or more elements required to make an apprehension can often be missing.
- Take a description and contact the police.
- Build up a picture of any problems you may have and use prevention techniques to avoid similar occurrences.
- A free booklet, *Making Arrests: A Good Practice Guide For Retailers*, is available from the Home Office, but training and/or the use of professional help is preferable and is recommended.
- If you do suspect a theft – use deterrence rather than attempting an arrest.
- If there is a security tagging system and the alarm goes off, always assume that the store has made an error.
- Approach the customer and identify yourself, politely requesting that they return to the cash desk, as it is possible a tag on a purchase may still be active.
- Ask the customer to produce their purchases for checking, thank them for their co-operation and apologise for any inconvenience.
- Check that the customer has not paid at another cash desk.
- If the customer makes an excuse and produces goods which have not been paid for, payment should normally be accepted and the transaction completed.
- If the customer refuses to return to the cash desk, stay polite, professional and calm and refrain from any accusations.
- Contact security personnel and/or a supervisor/manager/second employee to act as a witness.
- Under no circumstances should the person ever be searched or physically touched.
- After the event, make a note of everything, including anything said by you and/or the suspect, then date and sign the note.
- Make a photocopy of all stock identification stickers and, if possible, take a photograph of the merchandise.
- When the police arrive, tell them exactly what occurred and no more.
- If the police officer takes the product as evidence, obtain a receipt.

Fixed Penalty Notices

In some cases, police may issue a Fixed Penalty Notice, the main points of this are:

- Penalty notices for theft apply to retail and commercial theft only.
- Only police officers and special constables can issue penalty notices for theft.
- Notices may be used for “*low-level, anti-social and nuisance offending*" and should not be used in cases that are “*too serious*” or have aggravating circumstances.

- Notices can only be used for thefts up to a value of £100 or criminal damage up to £300 (police officers judgment as to the value). Notices can be issued for the higher sums of £200 and £500 for the respective offences but only in "*exceptional"* circumstances.
- Notices for theft would usually only be used where goods have been recovered.
- Penalty notices for these offences carry a fine of £80 and as long as they are paid within 21 days do not result in a criminal record.
- Notices are intended for low level, usually first time offending and "*will not be appropriate for those who repeatedly offend*".
- The victims' views will be taken into account and notices "*will not be appropriate where the victim is not compliant*". This phrasing should place a veto in the hands of the retailer.

Exclusion Orders & Civil Recovery

Booksellers experiencing particular difficulties with persistent shoplifters may wish to take advantage of the opportunity to ban such persons from the premises. Similar arrangement used by local councils of the issuing an *exclusion order* or *banning notice*, which acts like a form of trespass. Civil recovery is another technique for dealing with thieves and is a process by which retailers can use the civil law to recover legitimate costs from people who steal from them. Both these methods require careful administration to ensure that businesses remain within the letter of the law. More information can be obtained from the BA.

ROBBERY

Prevention

- Keep your front doors and windows clear of signs and posters to allow good, two way visibility. Employees can see suspicious persons outside. Passers-by and police can see inside.
- Keep the outside of your business well lit at night.
- Make sure your cash register area is clearly visible to outside observers.
- Practice good cash control. Keep a minimum amount in your cash drawer and make regular drops into a safe.
- Advertise outside that you keep a minimal amount of cash in the register.
- Don't keep large bills under the cash drawer. If you don't have a safe, find a less obvious place to hide your extra cash until you go to the bank.
- Use a safe that the clerk cannot open alone or that requires two keys. Post that fact conspicuously, including on the safe itself.
- Use video camera surveillance and make it well known.
- Vary your banking routine. Carry cash in a variety of ways - a lunch sack, attaché case, flight bag, pocket, etc. Money bags are pretty obvious.
- Vary the times and routes that you use to go to the bank and have an escort, who should walk a few yards behind.
- Make deposits as often as possible.
- Be alert for "customers" who seem to be loitering or glancing around the store while appearing to shop or browse through a magazine.

- Watch for suspicious persons outside the business - especially in parked cars and around telephone boxes.
- If you see someone who is acting suspicious inside or outside, call the police to have them checked out.
- Two persons should be on hand at opening and closing times.
- Before closing, one person should check the office, back rooms and rest rooms to make sure no one is hiding inside.
- Keep side and back doors locked. Have employees use the main entrance, if possible.
- Place markers at the main entrance that employees can use to help gauge the height of a robber as he leaves.

Conduct during a robbery

- Try to stay calm. Don't make any sudden movements to upset the robber.
- Do exactly as you are told. **DO NOT RESIST!**
- Activate your alarm **ONLY** if you can do so secretly.
- Tell the robber about anything that might surprise him, such as someone who is expected to arrive soon.
- If you have to move or reach, tell the robber what you are going to do and why.
- Try to get a good look at the robber so you can describe him later.
- Don't be a hero. It's better to lose your money than your life.
- Give the robber time to leave.
- Note his direction of travel when he leaves. Try to get a description of his vehicle **ONLY** if you can do so without exposing yourself to harm.

After a robbery

- Call the police immediately, even if you have already activated the alarm.
- Close the business and lock the door(s) if you have a key.
- Do not discuss the details of the robbery with witnesses or fellow employees.
- Ask any witnesses to stay until police arrive. If they can't, get their names, phone numbers and addresses.
- Do not touch anything that the robber may have touched. Block off areas where the robber was, if necessary.
- Try to recall as much as you can about the robber's appearance, speech and mannerisms. Make notes.
- Step outside the store when the police arrive so that they'll know the robber is gone and you are safe.
- Let the police answer inquiries from the news media.
- Do not discuss the amount of money taken with anyone other than police.

The above advice may assist in keeping you, your staff and your property safe. Please use common sense if involved in a robbery.

With thanks to PC Holland of the Westminster Division of The Metropolitan Police

FRAUD

Credit & Debit Cards – Chip & PIN

To combat the huge rise in plastic card fraud, banks have moved from magnetic stripe cards to the Chip & PIN system. The system combats fraud by holding secure data in the chip so it cannot be copied or altered and transactions are also authorised by a PIN number to establish the identity of the holder. Liability for fraudulent transactions which could have been prevented by Chip & PIN technology is now with the retailer.

There will be some instances when a signature can still be accepted and staff should follow the prompts on the terminal, as follows:

- Customers will still sign if they have old style cards.
- Customers from other countries that may not have upgraded to Chip & PIN cards will continue to sign.
- Some disabled cardholders will have been issued with a Chip and signature card and can continue to sign.
- If there is a technical problem with the Chip & PIN equipment, the retailer can choose to accept a signature - but if the problem persists they should contact the bank or supplier straight away.

If there are any concerns, businesses should contact their acquiring bank on the usual customer service number. For more information see the Chip & PIN Programme Management Organisation (PMO) website at: www.chipandpin.co.uk.

Credit & Debit Cards – Card Not Present (CNP)

The following is a combination of tips and tricks to reduce credit card fraud from various sources (listed at the end of this section). This advice is primarily aimed at the e-commerce sector, but may be equally valid for certain situations in mail order and/or telephone orders where the cardholder is not present (CNP).

- Your merchant acquirer should be your first port of call for help and advice. Remember that authorisation for a card-not-present transaction is not a payment guarantee. It just confirms that the card is not reported stolen or lost, and there are sufficient funds in the account. Retailers are liable for chargebacks. So make sure you understand the details of your contract with your merchant acquirer and follow their guidelines at all times.
- Your merchant acquirer will also hold details of stolen cards and may also have Address Verification Service (AVS) or Card Security Code (CSC) or other knowledge-based systems based on the sending patterns of their customer.
- Add a message to your website stating that you check all transactions for possible fraud (even if you don't it may put off some thieves from trying).
- Set an upper limit for transactions (£100 sounds reasonable, but preferably base it on your own experience). Telephone all UK buyers over the limit and run extensive checks on all international orders over the limit.
- You will find that certain UK Post Codes and countries are far worse for fraud than others. It is hard to predict, but many countries in Africa, Asia and Eastern

Europe are notorious for fraud on the Internet. It may be wise to wait until you are sure funds have been cleared or simply reject all orders emanating from these countries.

- Don't accept an order unless complete information is provided. The British Retail Consortium's Code of Best Working Practice for CNP transactions recommends that retailers should capture the following information:
- Customer/Cardholder name & statement billing address (including Postcode which can be checked online or via a database available from Royal Mail).
- Length of time at address & previous address (if moved within last year).
- Delivery address (if different) & name of intended recipient.
- Card number & expiry date.
- Card issuer (for comparison with BIN ranges supplied by acquirer).
- Customer email address & land line telephone number (Telephone numbers can be checked online or via a database available from BT and possibly include a fax number if it's a company).
- Be extra careful where the delivery address is different to billing address, especially if it is a non-permanent address (eg a hotel). Ask for a fax confirmation with a signature and copy of the bank billing address. If you have time, send a paper 'receipt/thank you' card to the billing address including instructions to call you if there is a problem.
- Never release goods to a third party allegedly sent by the customer (eg a taxi driver).
- Obviously, do not accept orders where the return email address is undeliverable and also be wary of orders from free email services (you can check if it is a free service by typing www in front of the domain name of the email address) and mobile phones.
- Check the origination of the email using the IP number to see if it is from the country claimed in the email - go to www.arin.net/whois/ .
- Be especially careful of very large orders (value and/or quantity) and where the customer appears unconcerned about shipping costs.
- Contact the customer and ask them to confirm details of the order and ask for additional information or repetition of part of their details. For instance there is a Card Security Code, which is the last three or four digit number on the security strip. Or, ask for a check on the bank issuing the card or the expiry date.
- You don't want to lose the order, but in suspicious circumstances, if at all possible delay delivery until you are certain the funds will be paid.
- Make sure you have some form of proof of delivery and understand if you can claim insurance for lost parcels, especially for overseas orders. Banks will also chargeback if the customer claims not to have received the order ('denial of service').
- Keep a log of all fraudulent transactions and analyse them for patterns, eg value, geographical location, type of card, multiple cards at the same address etc.
- Consider using the Verified by Visa or MasterCard SecureCode services for online payment security, which can protect retailers from chargebacks for certain fraudulent transactions.
- Consider using a specialist software service that checks for fraudulent orders - no system is perfect, but they can screen out suspect orders automatically for checking.

More information:
Card Watch - www.cardwatch.org.uk
CyberSource - www.cybersource.com
ClearCommerce - www.clearcommerce.com
Experian - www.experian.com
WorldPay - www.worldpay.com

Scams

Scams can take many forms and are mostly aimed at consumers. However, in some cases businesses can also be targeted and the following is a list of some of the most common scams.

West Africa Advanced Fee Fraud

The 'West African' scam (sometimes known as the '419 advance fee fraud') although originating in West Africa, can also come from other countries. The scam is based on the premise that some major event (eg the overthrow of a government), has resulted in a large sum of money being held by someone who is seeking help in transferring it overseas with a proportion of the money being offered for helping arranging this. Victims may be approached by letter or fax, but now more often by email. Respondents receive a further communication asking for some money up front or for bank account details and the victim is then defrauded of the cash or finds their bank account emptied. For more information see: www.met.police.uk/fraudalert/index.htm

Premium Rate Telephone Numbers

Fraudsters use the high cost of premium rate telephone or fax numbers by tempting victims into bogus competitions, prizes, holiday offers, 'surveys' etc. The aim is to seek a response and keep the line open as long as possible (eg a long sales message or series of questions) while being charged at a premium rate. For more information see: www.icstis.org.uk

Unsolicited Directory Entry

Companies are sent a form for an entry in a directory (eg an international fax directory), but hidden away in the small print is a charge for entry and perhaps a commitment to an ongoing charge in future years.

Unsolicited Orders or Gifts

Some companies may send unordered products or 'gifts' and then demand payment. This is a criminal offence. For more information see: www.oft.gov.uk

Charity Promotions

Check all charity promotions with the Charity Commission to ensure they are registered, are genuine promotions and meet the legal standards required. For more information see: www.charity-commission.gov.uk

Trading Schemes

Trading schemes (sometimes known as direct selling or network marketing) are a legitimate form of business. However, if the main aim is to generate money by recruiting new participants rather than selling the goods or service, then it may be an illegal 'pyramid selling' scheme. For more information see: www.tradingstandards.gov.uk

Business Help
Companies are targeted by unscrupulous 'business experts' who claim that there is a need to comply with some legislation (eg business names, data protection, health & safety, fire precautions etc) or they offer an opportunity to evaluate the business for rates reduction or help to patent an invention etc. Inflated fees are charged, but in the vast majority of cases there is no legal compulsion. In reality free government help is usually available and often very little is done to help the business. Contact the BA Business Support Helpline to check your legal obligations.

Further sources of advice:
www.consumerdirect.gov.uk
www.ripofftipoff.net
www.scambusters.org

SECURITY EQUIPMENT

Buying a Security Appliance

- With so much consolidation and a number of new entrants to the security appliance market, the following top 10 tips should help to clearly evaluate their options.

- Innovation - is the appliance supplier considered to be innovative by third party analysts? If the supplier is not on the radar of any analysts, then this should start alarm bells ringing.

- Operating systems - are built for any number of purposes and trying to be all things to all men fundamentally makes them poor. What's needed is a small, slim piece of code built from the ground-up and specifically designed to manage a particular application.

- Hardware - pay attention to the application the hardware is running on. This may involve asking who the hardware provider is. Use a well-known, recognised manufacturer whose hardware runs on a reliable platform. Question the reliability of the components and how often they need to be replaced.

- Components - similar to how it works with a car, if components go wrong, it's vital to know that the hardware manufacturer has plenty of spare parts that can get your appliance back up and running quickly. Any good supplier should sign-up to the Return Merchandise Authorisation (RMA) - it's important to check that they do before making a purchase.

- Redundancy of components - it's vital that any appliance has multiple redundant components so that the loss of any single piece, such as a disk or network card, doesn't prevent the entire box from working.

- Level and quality of support provided by vendor - expect any potential supplier to offer 24/7 support and quick response times as part of a service level agreement.

The only way to really assess the quality of support is by testing the product before buying it - make this one of the key assessment points.

- Interoperability - it's important that the appliance has the ability to integrate with the most popular customer applications and networks to ensure that it doesn't limit future purchasing decisions.

- Integration of best of breed layers - look out for appliances that have taken solutions from other best-of-breed suppliers to further enhance the solution.

- Estimated ROI for product - consider how easy it is to extract data from the box to demonstrate real return on investment and justify spend.

- Future proof - don't just consider what you need today, consider whether the appliance has the ability to meet future needs.

Advances in security equipment continue on a daily basis, so this section can only be a general guide to the type of equipment available. The website www.securitypark.net is a useful source of new information.

Security Tagging

Security tagging (also known as Electronic Article Surveillance - EAS) is commonplace in many bookshops. Tags inserted into books are usually either acousto-magnetic (AM) or radio frequency (RF) and systems also require deactivators and detection barriers at the exit. There are a variety of options to choose from and the details of the two biggest suppliers can be found below. In addition, systems can be integrated with EPOS and linked to CCTV to trigger video recording. However, no system is perfect and determined thieves will find a way around. Their main purpose is to deter the casual thief and there is ample evidence of their effectiveness in this aspect.

Tagging Books

Tagging every book is probably out of the question. The cost and labour involved would be unlikely to pay dividends. The trick is to tag only those books most likely to be stolen and this requires some thought. Use stock audits to determine which titles and which parts of the store are suffering most losses and target these areas. Other alternatives are to tag a percentage of books across the board or all books above a certain price. Keeping the thief guessing is all part of the game.

Source Tagging

In some industries, retailers are able to demand source tagged goods from their suppliers, ie a tag inserted at the point of manufacture, embedded in the product. However, the book industry uses a wide variety of tags. The technology of the near future will be RFID. This is a combined security tag *and* bar code, a so-called 'intelligent tag' incorporating a chip and a transmitter to identify the product and act a security device. This will have many uses throughout the supply chain for publishers, distributors, booksellers and libraries (which are already leading the way). However, universal RFID at item level is a technology that will take some time to come to fruition; EAS is readily available now and can give a return on investment. EAS will continue to be a useful loss prevention tool even after RFID is introduced.

Further information:
www.bic.org.uk
www.adt.co.uk
www.bluerocksecurity.com
www.checkpointsystems.com
www.intrepidsecurity.com

CCTV

Closed Circuit Television (CCTV) is another useful tool in the fight against theft. But before considering purchase, a full evaluation should be carried out. Questions that should be addressed include:

- Is the system intended to deter public theft, staff theft, or both?
- Is the system to be monitored when in operation and, if so, by whom?
- Are the monitors on public view or covert?
- Is there any benefit in having dummy cameras also?
- Does the system log date and time?
- Will the tapes be examined as a matter of routine or only to view particular incidents?
- What is the system for changing tapes?
- How often will old tapes be replaced?
- Will the data be transmitted over the internet for remote access?

The CCTV system is covered by the Data Protection Act and therefore advice should be sought in its use and extent. CCTV suppliers are often not the best source of advice, as they do not operate systems. For more information see:
www.informationcommissioner.gov.uk

Static camera systems are the least expensive; often several static cameras can be installed for the cost of a single camera capable of pan, tilt & zoom (moveable cameras).

Cameras are most effective when the public realise a working system is in place but cannot tell what is being monitored. A camera at the entrance to the store plainly indicates the presence of an active system and every a sign stating that CCTV is in operation is an extra deterrent.

The use of smoked or mirrored glass domes prevents the casual observer knowing the direction the camera is pointing. Lighting is crucial to success; common errors include lighting too low at night and installing too many lights close to cameras.

Where possible the camera system should cover the whole floor area to give continuity of evidence, where the video is to be used for a court case. More modest installations provide cover for the points of risk, such as high value stock or blind corners, preferably supported by a camera at the entrance to show the individual leaving the area.

The VCR is no longer the preferred choice of recording medium. The Digital Video Recorder (DVR) is now used extensively. Smaller businesses would be well advised to use a DVR which is widely accepted and used in the industry, to ensure long service and maintenance life. Much more latitude exists with the selection of camera and monitor manufacturer.

The service and maintenance contract should offer the option of a comprehensive service. The repair and replacement cost of the average DVR is likely to be a considerable percentage of the total installation cost.

Always seek three quotes. Always seek the advice and recommendation of a surveyor, using their experience to guide your thinking. If their recommendations are not consistent once the specifications have been submitted ask at least two to re-quote according to the specification you think most appropriate to your business needs.

With thanks to Brian Cottrell, Crime Prevention & Store Facilities Manager, W H Smith

INFORMATION SECURITY

The security of business has never been more important. As the numbers of websites, emails and electronic files increase, and the ways to access them become more flexible, the threat to information mounts. The following are quick and effective ways of dealing with the issues and can be thought of as 'good housekeeping'.

Work out what's valuable

Consider the effect of losing the following:

- Your VAT return (the day before you have to file it)
- Your accounts
- Your customer contact list

Consider the effect of someone stealing:

- All your customer credit card numbers
- Details of the new product or service you've just designed

Consider the effect of being unable to use your computer because:

- Power cuts
- Theft
- Mystery technical glitches (at 5.30pm on a Friday when there is no service engineer available)

The following practices will help counteract the most common threats:

Backups

- Take backup copies of important information
- Think about how much information you are prepared to lose and decide on an appropriate backup cycle - daily, weekly, etc
- Store backup media away from the originals, ideally off-site
- If information cannot be backed up (for example, valuable documents, such as deeds or share certificates), store them in a fire proof safe or similar

Software

- Keep software applications and operating systems up to date with latest patches - if in doubt, ask your vendor
- Ensure that suitable virus defence software is installed throughout your system

- Consider other security measures such as firewalls and intrusion detection systems as appropriate

Physical security

- Keep your premises physically secure
- Always try and make sure you know who's in the building
- Prevent visitors casually wandering your premises - if appropriate, fit an alarm
- Lock valuable assets such as laptops, mobiles and file servers in a secure room
- Keep valuable items out of direct public view

Education

- Let everyone know what is expected of them
- Ensure people know about the value of the information they handle
- Ensure people know any procedures for handling threats
- If you have a formal policy, ensure people know where it is, and their responsibilities

Access control

- If you run a multi-user computer system, use appropriate access control software to keep those without permission away from information held on your computer systems
- Ensure everyone who needs access has their own ID and password
- Adopt a clear screen policy - never leave computers logged in when people are away from them
- Ensure people can access only what they need to for their job

Clear desks

- Establish a practice of clearing desks at the end of each day
- Make sure people have a lockable drawer or cupboard they can put their work in
- Make sure they're actually locked, and the keys removed

Destruction

- If you handle sensitive information, you don't want the wrong people reading it - destroy any copies you don't need
- If you have a lot of paper copies, modern shredders are inexpensive and effective
- Some organisations use specialist destruction companies - this is normally only required if you have a lot of highly sensitive material

Further sources of advice:
www.itsafe.gov.uk
www.businesslink.gov.uk
DTI Information Security Health Check Tool:
www.dti-bestpractice-tools.org/healthcheck/
The Business Continuity Institute (BCI): www.thebci.org
www.microsoft.com/security

With thanks to: www.is4profit.com

TERRORISM

Security at Work

Simple preventative steps

- Be alert and observant and report any unusual or suspicious activity to the appropriate people or departments. Encourage your staff to do so, too.
- Have a good look around your workplace and establish an awareness of what should and should not be there. This will be very important if you need to search your premises at any time (for example, if there were a bomb threat).
- Develop links with neighbouring businesses and share information so that, together, you are able to cover a wider area.
- Trust your instincts; if you feel something is wrong, ring the police.
- If you have information about possible bomb threats or other immediate threats, call **999**.
- If you have tip-offs or confidential information about possible terrorist activity, call the police anti-terrorist hotline: **0800 789 321**.

Think about terrorism

All terrorists have to plan and prepare for an attack, which can make them vulnerable to discovery. They may seek anonymity, or other identities, in making these preparations. Be aware of the companies and the people who come and go in the delivery of goods or services in your workplace. If anyone or anything causes you serious concern, report the incident to your managers or to the police.

Terrorists need money to finance their operations. They get it by both legal and illegal means. Make sure you are not funding terrorists:

- Take good care of your credit cards, financial facilities and records
- Do not adopt trading practices that effectively launder money; know your customers and have proper audit trails, so that you can make sure that your customers are who they say they are.

Sensible precautions

Know your business:

- Are you alert to unusual transactions that raise questions about their purpose or intent?
- Would your accounting practice pick up anomalies?
- Could your business unwittingly support terrorist activity?
- Are your computer systems and access to them secure?

Know your staff:

- Can you be reasonably certain they are who they say they are?
- Have you checked references and employment records?
- Would you be aware of any behaviour or changes in behaviour that might give cause for concern?

- Are managers aware of how they should handle such instances?
- Are you confident that similar standards are applied to agency, contract or consultant staff working within your organisation?

Know or develop appropriate contingency plans:

- Does your business have suitable contingency plans if your office is not accessible?
- Is there a way for staff to contact the office to check the current situation?
- Do you work with the police and the fire brigade to ensure your standard emergency plans, such as fire evacuation drills, are up-to-date and regularly exercised?
- Do your staff know the procedures?

Invest in security measures:

Before you invest in additional measures, review what is already in place.

- Do your existing measures form a cohesive security package that provides overall assurance?
- Does someone have specific responsibility for security?

Existing measures are often adequate if properly maintained, but attention to them may have become lax. Staff may not be aware of them or may have developed habits to circumvent them. Simply reinstating good basic security practices and regularly addressing them brings benefits at negligible cost.

Protect against electronic attack ('hacking')

The National Infrastructure Security Co-ordination Centre (NISCC) offers the following advice to companies and organisations to protect against electronic attack:

- Consider if changes in your business circumstances or relationships might increase the threat of electronic attack to your organisation
- Check that protective security measures are properly implemented and up-to-date
- Anti-virus software should be updated regularly
- Patches should be applied to eliminate known vulnerabilities
- Internal security policies should provide appropriate protection from inside attack

More information about how to protect against electronic attack, and details on the latest vulnerabilities and patches, can be found on the NISCC website, www.niscc.gov.uk.

Suspicious Packages

The Government has also published a list of some of the warning signs that should alert mail room staff to suspicious packages. They include:

- Discolouration, crystals on surface, strange odours or oily stains
- Envelope with powder or powder-like residue
- Excessive tape or string
- Unusual size or weight given size
- Lopsided or oddly-shaped envelope

- Postmark that does not match return address
- Restrictive endorsements such as 'Personal' or 'Confidential'
- Excessive postage
- Handwritten, block-printed or poorly typed addresses
- Misspellings of common words

Where to go for more advice

Protective security advice for businesses, organisations and anyone with responsibility for the safety of others can be found on the Security Service website (MI5), www.mi5.gov.uk.

Contact your local police and arrange a visit from your local Crime Prevention Officer or your local Police Counter-Terrorism Security Adviser. Both will help you assess any problems and offer advice.

The manuals *Business as Usual* and *Protecting Against Terrorism* help businesses form contingency plans and prepare for emergencies.

The booklet *Expecting the Unexpected* on the London Prepared website www.londonprepared.gov.uk is another useful resource for business continuity.

For more information see:
www.homeoffice.gov.uk – www.preparingforemergencies.gov.uk

CRIME PREVENTION

The BA Loss Prevention Consortium (BALPC)

BALPC's main objective is to drive down losses within bookshops by focusing on current problem areas affecting all members and working collectively on long term measures. This may include - reporting on organised theft and initiating prosecutions; reviewing legislation and consultative documents from Government; working with other organisations on initiatives (such as the Retail Crime Survey produced by the British Retail Consortium) and exchanging information on new products and services.

BALPC members also offer a **free** email advice line on any subject to do with loss prevention or security issues. Some examples are:

- Customer & Staff Theft
- Guarding & Shop Detectives
- Security Marking & Tagging
- Security Equipment
- Fraud & Scams
- Contingency Planning

All requests for advice will be handled through the BA and will remain confidential. To ask a question, simply email it to sydney.davies@booksellers.org.uk and it will be forwarded (anonymously) to the experts for their comments.

Home Office & Police Service

This guide covers many aspects of loss prevention and security, but there are areas, eg security of premises, that require specialist advice. Local police stations have crime prevention officers who can offer free advice and publications. The Metropolitan Police and the Home Office have a number of free general guides on crime reduction, plus some specialist advice for retailers. www.police.uk
www.met.police.uk
www.crimereduction.gov.uk
www.crimecheck.co.uk

Other Retail Crime Advice

The British Retail Consortium conducts an annual Retail Crime Survey and holds seminars on retail crime. Action Against Business Crime (AABC) is the national organisation for business crime reduction partnerships (BCRPs) and is a partnership between the BRC and the Home Office to expand the work and impact of BCRPs. It provides a national focus for efforts of business crime partnerships working to reduce crime against business across the country. For more information see: www.brc.org.uk

Design Against Crime has case studies on how good design can reduce crime.
www.designagainstcrime.org

HSE Books publish guides on risk assessment and preventing violence to staff. Companies also have a duty of care towards their staff under Health & Safety legislation.
www.hsebooks.co.uk

Crimestoppers is an independent UK charity working to stop crime.
Tel: 0800 555 111
www.crimestoppers-uk.org

Victim Support is the charity which helps people cope with the effects of crime.
www.victimsupport.org

Sydney Davies
Booksellers Association of the UK & Ireland Ltd
June 2006