Retailers Crime Prevention Toolkit

Home Office

Secured by Design

Official Police Security Initiative

POLICE CPI

Police Crime Prevention Initiatives

Contents

Introduction

This Retailers Crime Prevention Toolkit has been designed at the request of the Home Office, through a collaboration between the National Business Crime Centre (NBCC) and Police Crime Prevention Initiatives (Police CPI) to provide useful information and guidance to support you in keeping your business safe from crime and to help you to prevent crime impacting both your staff and your business.

POLICE CPI
Police Crime Prevention Initiatives

Police Crime Prevention Initiatives (Police CPI) is a longstanding, not-for-profit, crime prevention organisation. Set up by the Police Service in 1989, Police CPI delivers a wide range of innovative and ground-breaking crime prevention and demand reduction initiatives to support the wider UK Police Service, as well as the Government and the general public, bringing organisations together to reduce crime and the fear of crime and create safer communities.

Part of the National Police Chiefs' Council (NPCC) Prevention Coordination Committee, senior police officers from England, Scotland, Wales and Northern Ireland control and direct the work Police CPI carries out on behalf of the Police Service, setting the strategic direction of Police CPI to ensure there are benefits for both the public and the Police Service.

NATIONAL BUSINESS CRIME CENTRE
Reducing crime through partnership and prevention

The National Business Crime Centre (NBCC) represents UK Police forces to work in partnership with the business community to tackle crimes against businesses.

Hosted in the City of London Police the primary role of the NBCC is to provide support, guidance, and training to businesses and organisations to help them prevent and respond to business crime effectively. This includes providing advice on crime prevention measures, sharing best practices, and helping businesses to report and investigate incidents of crime.

Our aim is to:

Improve partnership working with the business community and raise national police standards, to accurately understand and reduce the impact of crime

Enable businesses to target resources more efficiently, through effective intelligence and information exchange, disrupting crime against business at a national level

Prioritise prevention, enabling businesses to protect themselves from crime by being a conduit of best practice and a centre of excellence, supporting all businesses throughout the UK.

The NBCC also works closely with law enforcement agencies to ensure that they have the tools and resources they need to engage with the business community and prevent and investigate business crime effectively. In addition, the NBCC plays a key role in raising awareness of the risks of business crime and the impact it can have on businesses, their employees, and society as a whole.

Business crime is defined as:

Any criminal offence where a business, or person in the course of their employment, and because of that employment, is the victim.

www.nbcc.police.uk

Securing your business does not have to be a costly endeavour and many of the crime prevention measures outlined in the booklet may already be in place. The information provided should be used to support you in reviewing your current arrangements and subsequently identifying any areas for improvement over time.

Whilst following the information and guidance in this booklet is no guarantee to keep you free from all incidents, it will most definitely help you be better informed about preventing crime for your business.

Physical Security

Securing your property will help make your business safer

Security

Investing in security measures can seem daunting but it is a good investment, will last a long time and can add value to your property. Many security features can be multi-purpose and provide enhanced safety and security for you and your staff in a variety of situations. You do not need to apply for planning permission for certain security improvements, but there are planning regulations (laws) that affect many of the changes you can make to the outside of your business, including building walls and fences. Improving physical security at your premises can help you reduce your risks from all forms of crime.

What is physical security?

Criminals are observant and opportunistic and whether they are intent on committing burglary, theft, harm or damage, they are always on the lookout for vulnerable features to exploit. Almost all types of crime can be defended against by the implementation of physical security measures.

Criminals attempt to remain unseen, unheard and uninjured whilst committing their crimes. As a result, they look for properties with low levels of security that is easily overcome, where they are less likely to be seen by neighbours or passers-by.

Retailers should install physical measures to strengthen security, such as tested and accredited locks and bolts on doors and windows, to deter criminality and increase attack resistance.

Why improve physical security?

Commensurate security products and design features can provide a level of physical security that will defeat the abilities of the average criminal by deterring, detecting and delaying as follows:

DETER

Visible, appropriate physical security measures make it less likely for criminals to identify homes / property as easy targets.

DETECT

Physical security measures, such as CCTV, make it more difficult for criminals to successfully commit crime by assisting with verifying an attack and initiating an early response.

DELAY

Physical security measures, such as locks, make it more difficult to successfully commit crime by increasing the effort and delaying the actions of criminals

When looking to source security systems and products, the first port of call should be the Secured by Design website www.securedbydesign.com. This contains details of the many hundreds of companies and thousands of products that have met the exacting Police Preferred Specification. All of the companies have their website and full contact information listed, as well as a detailed list of all of their Secured by Design accredited products.

To help get you started on making your premises more secure

Security Standards Explained

Secured by Design is the official police security initiative that is owned by the UK Police Service with the specific aim to reduce crime and help people live more safely.

Combining the principles of **'designing out crime**' with Physical Security, SBD brings together Crime Prevention Through Environmental Design (CPTED) & Police approved products such as doors, windows, fencing and CCTV. The way CPTED works is to deter criminal and anti-social behaviour through the design, layout and specification of buildings and the spaces around and between them, that serve to reduce easy opportunities for crime to be committed. It is argued that more crimes are committed where a criminal feels more comfortable committing them, for instance where a physical environment offers easy unrestricted or at least uncontrolled access, where clear messages of ownership are absent, where either or natural and formal surveillance are absent or where wrong doers feel free to move within an area assured of their anonymity.

It is important that any security product used for physical security protection,
should be fit for purpose at its chosen location, giving assurance that it provides an appropriate level of protection in that application. Such assurance can be demonstrated where a security product has been tested and achieved an appropriate security standard supported by ongoing certification of the manufacturer's production processes.

Secured by Design (SBD) operates an accreditation scheme on behalf of the UK police for products or services that have met recognised security standards.

Such products or services must be capable of deterring or preventing crime and are known as being of a **'Police Preferred Specification'**.

Police Preferred Specification ensures that products have been:

- Independently **tested to a relevant security standard**
- **Fully certified** by an independent third-party, United Kingdom Accreditation Service (UKAS) certification body

Or

- Tested and certified by an approved body such as Sold Secure or Thatcham

Police Preferred Specification requires:

- Regular re-testing
- Annual inspection of the manufacturing facility to ensure quality and performance are maintained (by a UKAS body)

There are a wide range of security standards throughout the world, from a variety of sources for all manner of products.

For more information on Testing and Certification for security products see www.securedbydesign.com/guidance/standards-explained

When looking to source security systems and products, the first port of call should be the Secured by Design website www.securedbydesign.com. This contains details of the many hundreds of companies and thousands of products that have met the exacting Police Preferred Specification. All of the companies have their website and full contact information listed, as well as a detailed list of all of their Secured by Design accredited products.

Secured by Design

SBD

Official Police Security Initiative

Conducting a Premises Security Assessment

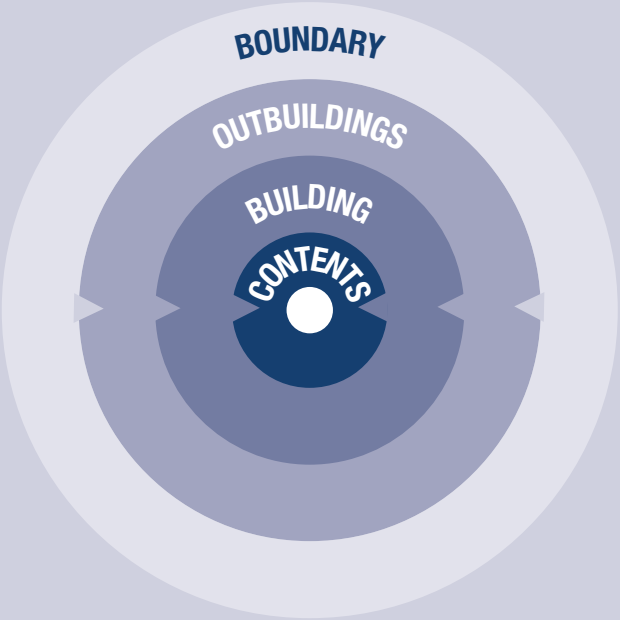
The best way to conduct a review of your own premises security is to approach it with the mindset of a potential criminal

This is referred to as the “onion peeling principle” and can be approached by starting with the boundaries and working inwards towards the centre.

The 3 key areas where you can be most effective in reducing the likelihood of your premises being targeted are to:

DETER
DETECT
DELAY

Most criminals will not target your business premises if the risk of being seen, noticed and getting caught is too great.



1. Lighting

Lighting is an important part of any overall security plan.

Lighting at entrances and exits makes it safer for people coming and going after dark, can be a good deterrent and can help investigate an incident outside a property. It is important that lights are installed in the right places and are operated in the right way to maximise effectiveness against any type of crime.

Good security lighting should be energy efficient, distributing an appropriate amount of uniform light to maximise visibility and colour rendition, whilst minimising light pollution.

Secured by Design (SBD), recommends photo-electric cell lighting – lights that automatically switch on at dusk and off at dawn, typically referred to as ‘dusk to dawn lighting’. Research has proven that a constant level of illumination is more effective at reducing crime and the fear of crime by providing well-lit areas that prevent criminals and terrorists from operating covertly.

SBD also favour the use of good quality LED lighting and other energy efficient light sources and advise against the use of florescent lighting which is environmentally unsustainable.

2. Bollards for physical security

Subject to planning permissions, physical barriers, such as ‘anti-ram’ bollards, may be installed to protect vulnerable building elevations, doors, roller doors and shutters.

Where crime risks dictate that there is a realistic chance of a ram raid type attack, with the intent to aide theft of the contents, or penetrate the shell of the building, to carry out an act of terrorism, the following standards for secure bollards that will prevent such an attack should be specified:

- Fixed bollards tested and certified to PAS 68-1:2013

Bollards providing passive protection to areas of a building that either are not required to have protection against an attack by a vehicle e.g. to keep a fire door (opening outwards) clear of obstruction, or where there is no means by which a vehicle may have access but a substantial barrier is still required may be tested to BS 170-1.

PAS 69: 2013 provides guidance on the appropriate selection, installation and use of such bollards and should be referenced in the first instance.

3. Roller shutters and grilles

Grilles and shutters can provide additional protection to both internal and external doors and windows. The minimum standard for such products, when required, is certification to:

- LPS 1175: Issue 7 Security Rating 1 or
- STS 202: Issue 3, Burglary Rating 1

For roller shutters, the above minimum security ratings are generally sufficient where:

- a shutter is required to prevent minor criminal damage and glass breakage, or
- the shutter is alarmed and the building is located within a secure development with access control and security patrols, or
- the shutter or grille is intended to prevent access into a recess, or
- the door or window to be protected is of a high security standard in its own right.

Security ratings higher than the minimum may be required and will be dictated by one or more of the following security considerations

- Type of crime risk
- Level of crime risk
- Location of the building
- Security level of the door or window being protected

Roller shutters can be either manual or automatic. Roller shutters can be operated from control buttons, inside and outside the premises.

Shutters that can operated from inside premises are particularly effective as they can quickly provide a physical barrier and ‘cover from view’ in the event of a firearms or bladed weapons attack.

Property maintenance

You should check your premises regularly, at least once a week, to see if there are any obvious signs of an attempted break-in or damage. It is important that premises continue to be well-maintained to prevent any spiral of decline. This includes removing litter and graffiti as soon as possible and making sure that landscaping is cut back to assist with surveillance from passers-by and your CCTV system. Flammable and combustible materials and substances should be stored in a secure, lockable container, cage or room. Bins should be securely stored away from the building to prevent arson. Regular maintenance should form part of your ongoing site security assessment.

Make sure that any outbuildings or external stores are secure. Ensure none of your equipment is left outside for any criminal to use to attack your property.

Side and rear boundaries should be higher than those at the front – check with your local planning department for the permitted height in your area. Trellis on top of fences combined with spiky defensive plants can help deter intruders.

4. Doors and Windows

Where a property has been awarded Secured by Design (SBD) certification, the front door will already be an enhanced security doorset, which includes the door, frame, locking hardware, glazing and hinges.

An external door into any building should be capable of being closed and locked to prevent casual intrusion into the building. Doors can be made of many different materials, presented in a range of different styles, with a variety of locking features.

It is preferable that a doorset should be tested and certified against the requirements of BS 6375, which gives assurance of the doorset's fitness for purpose against normal mechanical uses of the doorset and it will stand up to everyday wear and tear over a prolonged period.

The following performance standards refer to both window and doorset units and should be included in specification of new or replacement units:

BS 4873	Aluminium performance standard	BS 7412	PVCu performance standard
BS 644	Timber performance standard	BS 6510	Steel performance standard
BS8529	Composite performance standard	BS 8213	Code of Practice re install of PVCu windows & doors

There are many door sets currently in use that do not meet a tested and independently certified security standard. If a timber door is installed and has not been security tested and rated, the door should be at least 44mm thick and made from solid wood, free from rot or damage and not manufactured from soft wood or constructed with a hollow core

It is recommended that glazing in and immediately beside any doorset should protect the locking systems, with a layer of laminated glazing to the security standard BS EN 356:2000 class P1A. Laminated glazing is resistant to forced intrusion and even when broken the units remain intact without creating large shards of flying glass which can cause injury.

A suitable alternative to laminated glass is Security Film that meets BS EN 356:2000 class P1A standard or higher, installed to the edge of the glass, under the window beading.

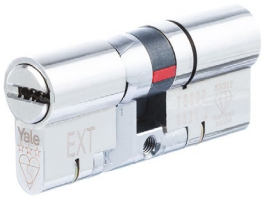
For more advice on other door profiles and locking systems, see the publication "The Police Crime Prevention Initiatives guide to Physical Security" at https://www.policecpi.com/about-us/login

A suitable alternative to laminated glass is Security Film that meets BS EN 356:2000 class P1A standard or higher, installed to the edge of the glass, under the window beading. For further advice, speak to a reputable, local glazier. Laminated glass and security film on glass can reduce the risk of forced entry by any attacker. This increased level of security can provide better protection during the 'Hide' phase of RUN HIDE TELL. Furthermore, it can reduce the risks of flying glass during a criminal or terrorist attack.

Improving management of physical security at your premises can help you reduce your risks from all forms of crime, including terrorism. Doors that lock securely, can provide a very good layer of physical security.

5. Locks

To secure doors, gates and other security barriers, it is recommended that a 'fit for purpose' lock is used, one which is tested and certified to an appropriate security standard.



DHF TS007 and SS312 Diamond are recommended security standards for cylinder locks. Those standards protect against lock snapping, lock picking, lock bumping and lock burning attack methodologies for Oval and Euro profile cylinder locks.

Padlocks

BS 12320, LPS1654 along with 'Sold Secure' Bronze, Silver, Gold or Diamond are all appropriate standards to recommend for padlocks used in security applications.

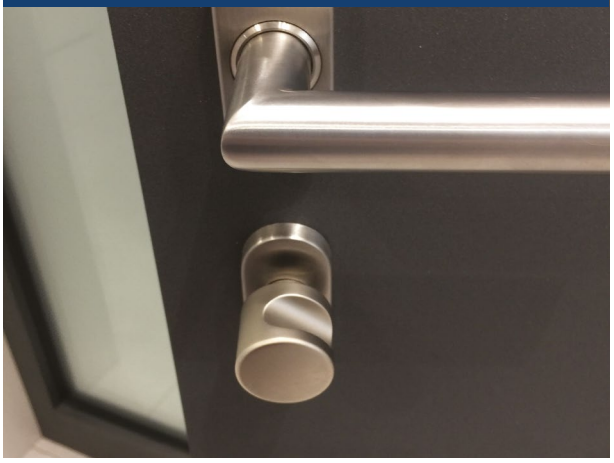
Guard Plates

Fitting a mortice deadlock, or sashlock involves removing wood and this leaves a very weakened area around the mortice lock. Lock Guard plates can be bolted together through the door - to resist a 'kick-in' attack and so help avoid a burglary.

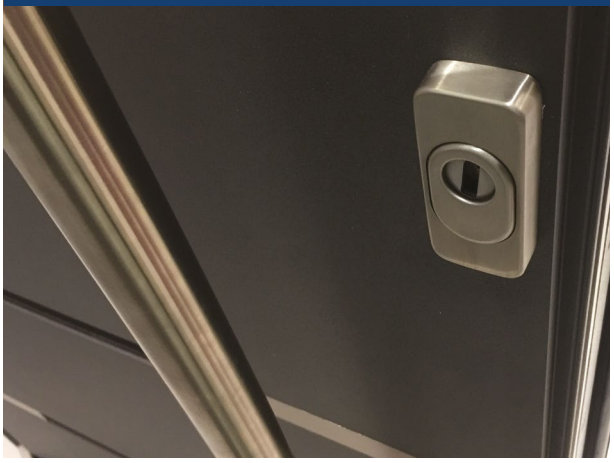
Anti-Thrust Devices

Anti-thrust plate is locksmith terminology for a flat device that is fitted to the external face of a door, overlapping the edge and covering the gap between the door and frame. Most often used for outward opening doors. It is intended to prevent someone using an implement to tamper with the latch or bolt.

INSIDE: No key required to open



OUTSIDE: Opens with a key



BS 8621 Lock

A thumb turn, operated lock is recommended for internal doors. It is recommended that your staff room/kitchen/safe place door should lock by a thumb turn so staff can quickly secure themselves in the event that a shopper becomes aggressive/violent or a terrorist incident happens in or near your premises.

Master Locksmiths Association

Seek advice from a registered Master Locksmith, in respect of locks for doors and windows, safes, along with other security furniture.

Practice good key management.

- Ensure you know who holds keys to your premises, stock rooms and safes by conducting a key audit
- A key audit will enable you to track, check and account for all your keys and stress the importance of keeping keys secure. Update this regularly
- Label keys with a bespoke code that can be explained to employees, but others would not understand
- Keys should never be hidden around the premises. Keep duplicates to a minimum
- For additional security consider specialised or patented security keys produced by a locksmith

A Master Locksmith can advise on a range of options.

www.locksmiths.co.uk

6. CCTV

CCTV is a cost-effective way of protecting your organisation's assets. Together with appropriate signage, it can deter criminals and provide surveillance. It can also record events and aid access control. CCTV can be used to observe suspicious criminal and terrorist behaviour.

CCTV cameras should provide quality images in which people can be recognised. Cameras should be positioned and set in such a way that changing weather and lighting conditions do not interfere with picture quality.

If the CCTV system is intended for evidential purposes, it should have a recording and storage capability of 31 days, using a format that is acceptable to the police for evidential purposes. The recording device should be stored in a locked and secure location or cabinet.

Security standards recommended in respect of CCTV / Security Surveillance Systems are:

- **BS 7958** - CCTV Management and Operation Code of Practice
- **BS 62676** - British Standard for the minimum requirements for CCTV Surveillance in security applications

CCTV systems should be registered with the Information Commissioner's Office (ICO) to comply with Data Protection legislation. You can find further information at: www.ico.org.uk . Clear signage should be posted to inform people that CCTV is being recorded in the area.

The CCTV cameras and their covers should be cleaned often, to ensure views are kept clear. This could be the removal of a spider's web or dust.

And lastly, it is good practice that CCTV security systems are fitted by a service provider who is a registered member of the NSI www.nsi.org.uk or SSAIB www.ssaib.org certification schemes.

For more useful advice about CCTV & VSS (Video Surveillance Systems) see the Secured by Design website page:

www.securedbydesign.com/guidance/crime-prevention-advice/vehicle-crime/cctv-security-advice

7. Intruder Alarm System

It is important to understand the importance of having an alarm system in your store or business. When criminals are looking at committing a crime, they will choose locations that are easily accessible and will avoid properties that have effective security.

To achieve a police response to an alarm activation, your alarm should be a professionally fitted and monitored alarm. Alarms are professionally fitted by a service provider who is a registered member of the NSI www.nsi.org.uk or SSAIB www.ssaib.org certification schemes.

BS EN 50131 is the security standard recommended in respect of intruder alarm systems. This standard includes 4 ratings from low risk to high risk to address site specific needs.

By installing an alarm, this can protect the property against unauthorised access when the business is closed.

It is also good practice for businesses for the alarm to provide a "Hold-Up/ Panic" alarm protection for you and your staff when the business is open, especially if they are on their own in case there is ever a hold up situation.

For more useful advice about Intruder Alarm Systems see the National Police Chiefs' Council website page:

www.policesecuritysystems.com/choose-an-alarm

8. Internal

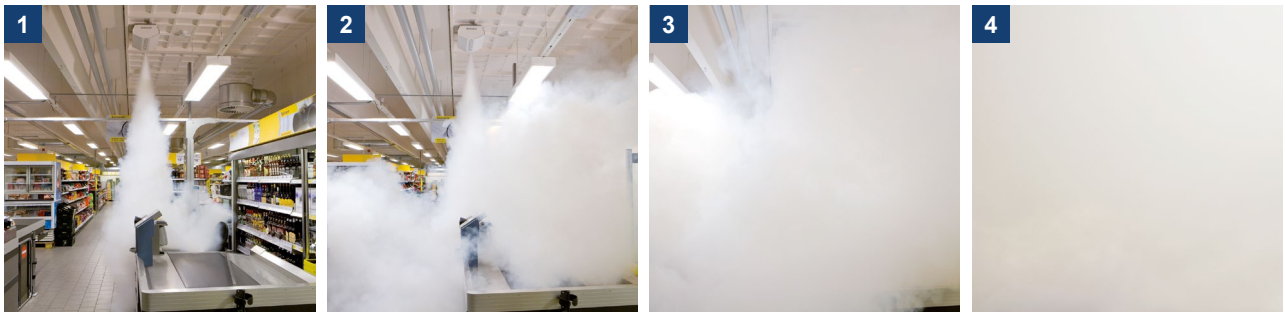
Security Fogging System

A security fogging system is triggered by an alarm sensor or switch and will instantly fill the area you are trying to protect with a dense, harmless fog that reduces visibility, making it virtually impossible for an intruder to access the items they want to steal. If you already have such a system, check with your supplier that it is still in good working order.

Smoke screens could provide ‘cover from view’ for staff and customers in the event of a firearms or bladed weapons attack.

Security Fogging Machines can be integrated with the intruder alarm system or act as a standalone feature.

BS EN 50131 is the security standard recommended in respect of Security Fogging Machines.



Forensic Intruder Sprays

- The system is linked to the premises intruder alarm system for out-of-hours protection
- The spray head can be mounted in an overt or covert position
- Warning signage should always be displayed as a deterrent to criminals
- The system is armed by wired or wireless PA, and only fires when movement is detected by the PIR
- The forensic spray links the criminal to the premise

Accessible gaming and vending machines

Gaming and vending machines should be emptied of all stock and cash with visible external facing signage displayed to advertise this fact and deter a potential intruder.

Safe storage of valuables, assets and stock

Valuables, assets and stock should be either removed from the premises or stored in a secure, lockable container, cage or room and the keys stored in a secure key cabinet or removed entirely. It is advisable to check the continued performance of essential equipment and services, such as fridge freezers, electrical and water supplies, including central heating pipework.

Protect your Wi-Fi and other smart devices by changing the default passwords.

Remove and destroy any correspondence with your name and address on before disposing of it.

Further Security Considerations

What is Cyber Crime?

As technology rapidly evolves and continues to bring business opportunities this also opens new opportunities for criminality and terrorism. So, it is important that businesses understand and recognise the threats they could face from cyber criminals including terrorists and what they can do about protecting themselves from it.

Cyber Crime is an umbrella term for two linked but distinct categories of cyber crime.

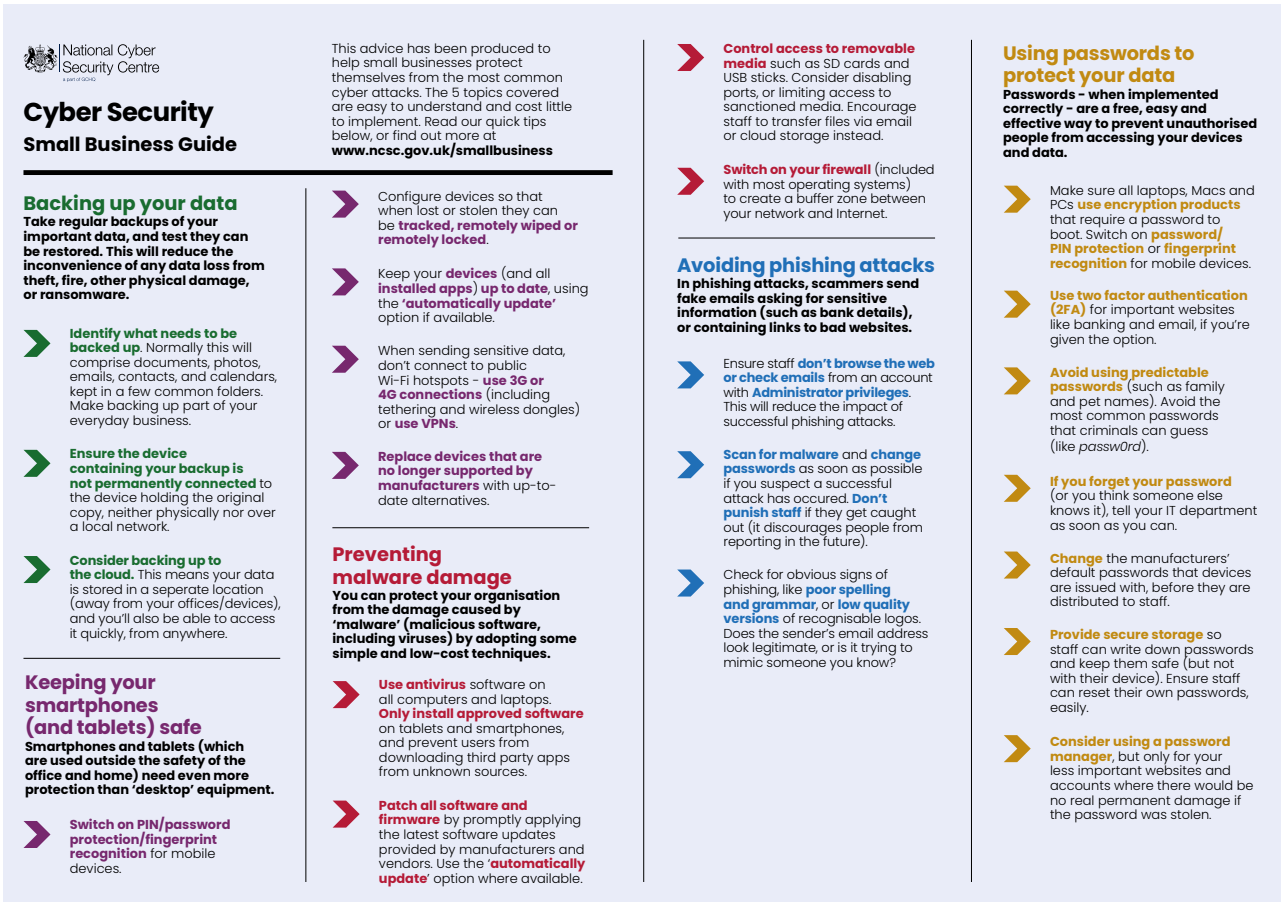
- Cyber dependant
- Cyber enabled

Cyber dependant crimes are carried out against computers, computer networks, data storage or other devices. They involve unlawful access to a computer system or making a system unusable.

Cyber enabled are traditional type crimes which can be increased in scale or reach using computers or other mobile data devices. This could be by using a false or stolen credit card to buy items online or a person sending funds to a criminal after recovering a fraudulent email.

Cyber security need not be daunting for small businesses – here is a quick explanation of the main threats and quick guide highlighting how to prevent them. For more detailed information go to the National Cyber Security Centre website

www.ncsc.gov.uk



National Cyber Security Centre

Cyber Security
Small Business Guide

This advice has been produced to help small businesses protect themselves from the most common cyber attacks. The 5 topics covered are easy to understand and cost little to implement. Read our quick tips below, or find out more at **www.ncsc.gov.uk/smallbusiness**

Backing up your data

Take regular backups of your important data, and test they can be restored. This will reduce the inconvenience of any data loss from theft, fire, other physical damage, or ransomware.

- **Identify what needs to be backed up**. Normally this will comprise documents, photos, emails, contacts, and calendars, kept in a few common folders. Make backing up part of your everyday business.
- **Ensure the device containing your backup is not permanently connected** to the device holding the original copy, neither physically nor over a local network.
- **Consider backing up to the cloud.** This means your data is stored in a seperate location (away from your offices/devices), and you'll also be able to access it quickly, from anywhere.

Keeping your smartphones (and tablets) safe

Smartphones and tablets (which are used outside the safety of the office and home) need even more protection than 'desktop' equipment.

- **Switch on PIN/password protection/fingerprint recognition** for mobile devices.
- Configure devices so that when lost or stolen they can be **tracked, remotely wiped or remotely locked**.
- Keep your **devices** (and all **installed apps**) **up to date**, using the **'automatically update'** option if available.
- When sending sensitive data, don't connect to public Wi-Fi hotspots - **use 3G or 4G connections** (including tethering and wireless dongles) or **use VPNs**.
- **Replace devices that are no longer supported by manufacturers** with up-to-date alternatives.

Preventing malware damage

You can protect your organisation from the damage caused by 'malware' (malicious software, including viruses) by adopting some simple and low-cost techniques.

- **Use antivirus** software on all computers and laptops. **Only install approved software** on tablets and smartphones, and prevent users from downloading third party apps from unknown sources.
- **Patch all software and firmware** by promptly applying the latest software updates provided by manufacturers and vendors. Use the **'automatically update'** option where available.
- **Control access to removable media** such as SD cards and USB sticks. Consider disabling ports, or limiting access to sanctioned media. Encourage staff to transfer files via email or cloud storage instead.
- **Switch on your firewall** (included with most operating systems) to create a buffer zone between your network and Internet.

Avoiding phishing attacks

In phishing attacks, scammers send fake emails asking for sensitive information (such as bank details), or containing links to bad websites.

- Ensure staff **don't browse the web or check emails** from an account with **Administrator privileges**. This will reduce the impact of successful phishing attacks.
- **Scan for malware** and **change passwords** as soon as possible if you suspect a successful attack has occured. **Don't punish staff** if they get caught out (it discourages people from reporting in the future).
- Check for obvious signs of phishing, like **poor spelling and grammar**, or **low quality versions** of recognisable logos. Does the sender's email address look legitimate, or is it trying to mimic someone you know?

Using passwords to protect your data

Passwords - when implemented correctly - are a free, easy and effective way to prevent unauthorised people from accessing your devices and data.

- Make sure all laptops, Macs and PCs **use encryption products** that require a password to boot. Switch on **password/ PIN protection** or **fingerprint recognition** for mobile devices.
- **Use two factor authentication (2FA)** for important websites like banking and email, if you're given the option.
- **Avoid using predictable passwords** (such as family and pet names). Avoid the most common passwords that criminals can guess (like *passw0rd*).
- **If you forget your password** (or you think someone else knows it), tell your IT department as soon as you can.
- **Change** the manufacturers' default passwords that devices are issued with, before they are distributed to staff.
- **Provide secure storage** so staff can write down passwords and keep them safe (but not with their device). Ensure staff can reset their own passwords, easily.
- **Consider using a password manager**, but only for your less important websites and accounts where there would be no real permanent damage if the password was stolen.

Preparing for cyber incidents

Should your business be a victim of cyber-crime there is help and support available at:

www.ncsc.gov.uk/collection/small-business-guidance--response-and-recovery/resources

Visit the website and watch the short "Preparing for cyber incidents" video resource.

Safety and Security

Security Awareness

We all have a responsibility to minimise potential security risks at work. The following actions can help keep your organisation secure:

Entering and Exiting your Workplace:

- Look alert and be vigilant when entering or leaving a site – your behaviour can deter someone with hostile intent from committing a crime
- Report anything unusual or suspicious immediately to a manager or the police
- Follow the correct entry and exit procedures for passing through gates, vehicle barriers, doors and so forth (e.g. swiping your pass or signing in and out as appropriate. Rule Setting, Access Control and Surveillance are key principles of good crime prevention)

In and Around your Workplace:

- Wear your security pass in the workplace as appropriate, ensuring it is clearly visible
- Deal with sensitive information appropriately, for example by using a shredder for paper documents or locking it away
- Lead by example and demonstrate good security practice in front of colleagues, visitors, and the public

Suspicious Behaviour

Criminals need to plan and prepare. Look out for unusual behaviour whilst at work and when you are out and about to help deter crime.

Suspicious activity could include:

- Observing or photographing entrances
- Loitering in restricted or non-public areas
- Asking unusual questions
- Hiding their faces or in disguise
- Unattended items that are hidden, suspicious or not typical of the given environment

Vehicles are also often used by criminals. Be aware of vehicles parked out of place or left abandoned, or a vehicle retracing the same route.

Your actions could save lives. In an emergency call the police on 999.

It's OK to Say

Sometimes colleagues (including managers) might do things or talk in ways that are worrying. Everyone has their 'off' days – this need not be cause for concern.

However, you could be best placed to identify an issue before it becomes a problem.

A colleague behaving like this might need support from within the workplace. Any number of things might be happening with the individual, they could have problems at home, personal issues to deal with, or the problem could lie in the workplace.

There are various ways that you could intervene to help them receive this support, perhaps by talking to the individual, mentioning it to your manager or you may choose to report the issue.

In some cases, if the individual doesn't get the support they need, or the situation is not otherwise dealt with – it might become an **insider threat.**

The insider threat is the risk that legitimate access is misused, to cause damage or harm to an organisation.

Misuse of access could be:

- Deliberate or accidental
- Carried out by an employee or third parties

Insiders tend to behave in ways that give cause for concern:

- Signs of a vulnerability/ risk
- Unusual/ suspicious work activities
- Unauthorised work activities

This behaviour does not automatically mean the individual is a risk but if you see any suspicious activity or concerning behaviours, report it to the appropriate person within your organisation. If you have a gut instinct where you feel something is wrong – we urge you to trust it.

Delivery & Vehicle Security

Your vehicles and deliveries are vital assets for your business.

Of all the business and delivery vehicles stolen every year more than half of all those are stolen from the business' own premises. .

Some simple and but effective measures will help you stop or avoid vehicle theft and avoid your vehicle being used in other criminal activity and some simple procedures will also ensure your deliveries and supplies are more secure to help prevent theft and other crime.

The key message is to take the security of your deliveries and vehicles seriously.

Good security = Good business

Vehicle security:

- When you leave your vehicle always lock it and take your keys with you
- Never leave keys in the vehicle
- Always check that all security devices (if fitted) on the vehicle are working
- Never leave the vehicle with the engine running
- Always make sure whenever possible that your cab (if a lorry) and the load compartment of your vehicle are secure
- When loading or unloading, always lock the cab
- When driving, where appropriate, lock the load compartment

If you keep the vehicle keys when you are not at work:

- Make sure they cannot be identified – don't leave anything on the key ring that identifies who they belong to or which vehicle they fit
- Never leave the keys where others can see them; and always keep them somewhere safe and secure

If you keep your vehicle keys at work:

- Make sure they are in a lockable location and out of sight
- Never use a 'hiding place', for example, inside the front bumper

Delivery and site security:

- All physical barriers around the property such as walls and fences should be in good repair and maintained
- Access to any delivery point or location should be controlled, if possible, with appropriate demarcation and security arrangements i.e. fences, gates, doors, shutters and signage etc. This allows for any non-authorised access to be challenged
- All access points to the delivery area should be kept closed and secure, particularly those leading to non-public areas
- All delivery vehicles should be parked as securely as possible and any gates, doors or shutters should be secured while any delivery takes place – this will help prevent 'tailgating' and opportunist theft
- Security measures should be put in place to ensure that during any delivery access to the area is controlled and any unauthorised access is prevented

- Consideration should be given to introducing security measures to protect vehicles and deliveries including CCTV cameras to monitor any authorised access
- Wherever possible vehicles, trailers and other material should not be parked/placed against any fence, gates or walls as they could be used as climbing aids or cover from view
- Delivery drivers should be encouraged to report any concerns about security or unusual behaviour that occurs around their vehicle or the delivery point

Deliveries: Park Safely & Securely

- Park your vehicle within sight and where you can return to it quickly.
- When you leave your vehicle always lock it and take your keys with you
- Never leave keys in the vehicle
- Never leave the vehicle with the engine running
- When loading or unloading, always lock the cab
- Hide all personal property from view
- When returning to the vehicle, check all round the vehicle for signs of interference, including any load security seals
- Remember: If you make your deliveries more secure and reduce the risk of theft of your vehicles you will also reduce the opportunity for your vehicles to be used by terrorists as a weapon
- If you witness any suspicious activity, report it to the Police immediately by dialling 999 or the non-emergency number 101
- If you suspect any terrorist involvement call the Anti-Terrorist Hotline on 0800 789 321
- Call Crimestoppers on 0800 555 111 if you have any information about vehicle or any other crime. Your call is free. You do not have to give your name. You may receive a reward

Lone Working

A lone worker is a person who works in an environment by themselves or without direct supervision. They can find themselves working for a business in an array of surroundings such as rural, residential streets, factories, large or small buildings or within a vehicle.

It's important to recognise the potential for a situation to quickly develop and increase a lone worker's vulnerabilities; some useful points to consider when lone working are listed below.

Keep Safe

- Remain aware of your surroundings at all times and avoid using devices which may distract you such as head or ear phones
- Don't take unnecessary risks
- Trust your instincts. If you feel uncomfortable, leave the location
- Take note of your surrounding and especially note alternative exit routes
- Keep to well lit or busy streets and avoid danger spots as much as possible
- Never underestimate a threat

For further advice on Lone Working visit www.suzylamplugh.org

Your actions affect whether a safety situation escalates or not.
As soon as you identify a possible risk, act to reduce it or avoid it completely.

Are you PROTECTED?

THRIVE assessment

All calls to the police undergo a THRIVE assessment against the following considerations, the results of this assessment will determine what action is taken by the police:

T Threat	**A threat is a communicated or perceived intent to inflict harm or loss against another person.**
H Harm	**Harm is to do or cause harm. E.g. to injure, damage, hurt ¬– physical or psychological. What harm taken place?**
R Risk	**Risk is the likelihood of the event occurring i.e. is the offender still at the scene or nearby?**
I Investigation	**Investigation is the act or process of examining a crime, problem or situation and considering what action is required.**
V Vulnerability	**Vulnerability is defined for the purposes of incident management as "a person is vulnerable if as a result of their situation or circumstances, they are unable to take care or protect themselves, or others, from harm or exploitation".**
E Engagement	**Engagement is where organisations and individuals build a positive relationship for the benefit of all parties.**

Below are a number of areas where retailers can take action to prevent crime and protect employees from violence and the business impact of crime.

Prevention	**Do you have a prevention strategy?**
Reporting	**Do your staff know when and how to report a crime?**
Offender Management	**What is your process for managing offenders?**
Training	**What staff training do you have in place to reduce crime?**
Employee Support	**What support is there for staff who are victims of crime?**
Corporate Support	**Do you have the right resources to deliver your strategy?**
Technology	**How are you using technology to protect your staff?**
Engagement	**How do you engage with the police and other groups?**
Data	**How is data used to influence your strategy?**

Prevention

Strategy

Having a well-designed prevention strategy sets the organisation's tone in respect of preventing crime, which in turn helps retailers to minimise losses from criminal activities, which can have a significant impact on the bottom line of their business. A strong strategy can also help retailers to create a safe and secure shopping environment, for their staff and customers, leading to increased staff retention, customer satisfaction and loyalty.

In addition, the strategy can help retailers provide transparency when complying with legal requirements and regulations related to security and data protection. By implementing a strategy that includes measures such as CCTV, security personnel, crime reporting and advanced technological solutions, retailers can also reduce the risk of data breaches and ensure that they are protecting the privacy of their customers.

Reporting

Why Reporting Crime Is Important

Crimes against businesses are under reported to the police, the 2024 British Retail Consortium Crime Survey suggested that retailers experienced almost 16.7 million shop thefts. However in the 12 months to June 2024, the police received reports just short of 470,000 shop thefts.

It's vitally important that all crimes are reported to the police as this allows the police to fully understand what is happening where, when, how, and who are committing the offences so that crime prevention plans can be developed and the appropriate resources allocated accordingly.

What To Report

The Retail Crime Action Plan sets out how reporting should be prioritised with the following types of incident:

- Where there are incidents involving violence or threats of immediate violence
- Hate related crimes
- Offences committed by prolific/persistent or juvenile offenders
- Offences where there is evidence of organised crime
- Offences committed with a significant value or commodity type (e.g., corrosive liquid etc) or where there are reasonable lines of enquiry to pursue

The NBCC regularly see examples where the shop theft has been reported but the assault or violence hasn't. It is important that the ongoing threat is reported to the police to ensure that you get the right response.

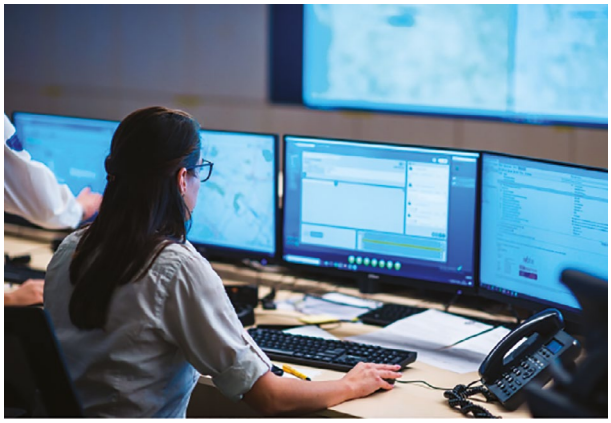
Attendance at the scene for retail crime will be prioritised in the following circumstances:

1. Where violence has been used or threatened.
2. Where an offender has been detained (for example, by store security) police will attend the scene with urgency and repeat / prolific or juvenile offenders will be treated with elevated priority. All police attendance will be subject to a THRIVE risk assessment (see next page).
3. Where evidence needs to be promptly secured which can only be done in person by police personnel e.g., securing forensic evidence.

How To Report

The NBCC have produced a guide of how to report a crime.

Reporting a Crime



Reporting a Hate crime

The guide includes the different ways that crimes can be reported and what information should be shared with the police to ensure you get the right response.

Internal Reporting Systems

Having an effective incident reporting platform helps the business develop their own threat assessment i.e. where and when are the crimes taking place, what is being taken along with who is committing the crime and by what method. Knowing this information allows the business to develop plans to protect the business and employees through deploying strategies such as additional guarding, issuing banning notices against offenders, target hardening products, store layout, product placement, providing training and sharing information with other partners and the police.

Does your business follow the ASCONE model to report crime? This approach used by many retailers ensures that only those shop theft offences that reach a certain standard are reported.

A	**Approach**	**Observation of the person approaching the product.**
S	**Selection**	**The person been seen to select the product.**
C	**Concealment**	**Efforts have been made to conceal the item.**
O	**Observation**	**There has been unbroken observation of the offence.**
N	**Non-payment**	**There has been no effort to pay for the item.**
E	**Exit**	**The person has left the store with the unpaid item.**

Statements

Having reported a crime, it is critical that when requested, the person reporting and/or the key witness is available to make a formal written statement to officers at the time of attendance. The person making such a statement should do so with the full authority of the company.

- A witness statement is required from the staff member reporting and from the staff member who witnessed the offence, including stock loss details and other offences
- A statement to produce the CCTV as evidence to be made by the relevant staff member
- Also consider completing an Impact Statement for Business (ISB) which is a written statement and is intended to provide businesses that have been victims of crime with a voice in the criminal justice process

Offender Management

Does your company have a policy/procedure to deter offending? Do your staff know what is expected of them if they see a crime taking place? The best approach to reduce crime is to deter the offender; offenders don't like to be seen/recognised so by offering a service such as a basket, or help them to find an item, can go a long way to stop the crime happening.

Evidence has shown that the majority of offending is carried out by a small number of prolific offenders, most shopworkers will know who these are. What is your organisation's approach to managing prolific offenders, do you know who they are, do you operate a banning scheme, how is this enforced and monitored?

The NBCC is developing guidance around civil recovery, which allows the retailer to recover costs lost due to the crime; the guidance will include when you can request details of the offender from the police to start the legal process.

Knowing your offenders motivations and how they commit crime along with other trigger points helps you to design solutions to mitigate the risks e.g. issuing banning notices, reviewing your refund policy, involving partners to support homelessness.

What is Being Done to Tackle Prolific Offending

The NBCC is producing guidance on banning individuals, this includes a suggested process along with considerations.

When looking for solutions consider other partners such as your BID, BCRP or local authority. In Hampshire, a Business Crime Navigator has been employed through partnership grants to support the local homeless population in Portsmouth who commit crimes against businesses; this approach has seen a reduction in offending from this group.

Anti Social Behaviour (ASB)

ASB takes many forms and includes a range of nuisance and criminal behaviours which cause distress to others, and we know through engagement that it is becoming an increasing issue.

It can also impact the customers of the business and local community because of the price in increased costs of goods, higher insurance premiums and potential loss of investment by businesses in the local area.

The NBCC has produced a range of resources to help businesses understand ASB and what tools are available to help them prevent and combat it.

Anti Social Behaviour (ASB)

Training

We know that training around de-escalation and good customer service can go a long way to reducing incidents of theft and violence. The NBCC has identified the main causes for violence and abuse and addressed them through the development of four short videos to help and support shopworkers. The videos deal with issues such as disruptive and anti-social behaviour, personal safety and de-escalation, saying no, and dealing and interacting with suspected thieves.

The NBCC has developed a booklet for those in the retail environment to help them identify the key drivers of violence against staff and provide guidance on how to prevent or mitigate the associated threat of violence and abuse of staff. We recognise that violence and abuse can take place in many forms and in a wide range of businesses, small or large.

The Guidance covers the three main triggers of violence – challenging shoplifting, age restricted sales and offenders under the influence of drink or drugs.

https://nbcc.police.uk/images/Reducing_Violence_Against_Staff_Online.pdf

Shop worker videos

Lone workers are described by the Health and Safety Executive (HSE) as 'those who work by themselves without close or direct supervision' and that can encompass many different job roles in a wide variety of industries. Location with lone workers or low levels of staffing can make them more attractive targets for offending.

As an employer you have specific duties to protect lone workers within your employment. This also applies if they are working for you as a contractor, a freelancer or are self-employed.

The NBCC, in collaboration with the Metropolitan Police Business Crime Hub and their Designing Out Crime Officers have created a short film as a guide to lone worker safety. There is also a link the HSE website proving further guidance.

Loan Worker Safety Guide

Training is a big investment for any organisation so the challenge is to ensure that colleagues follow the procedures and that they are not ignored or that 'work arounds' are not created. Examples would include refund policies, locking of doors, where keys to sales cabinets are kept etc.

Given the incidents of knife crime there has been an increased focus by the police and Trading Standards to ensure that retailers follow the law in terms knife storage, age restrictions etc. The NBCC provides some free bespoke training for retailers who sell knives.

Knife Guidance

Employee Support

Being a victim of crime can have a devastating effect on staff members, therefore, it is important that the right support is in place. The NBCC has created a framework for employers, which signposts sources of guidance and advice and how retail employers can help to prevent violence and abuse in retail settings and protect the wellbeing of their employees.

Framework for Employers

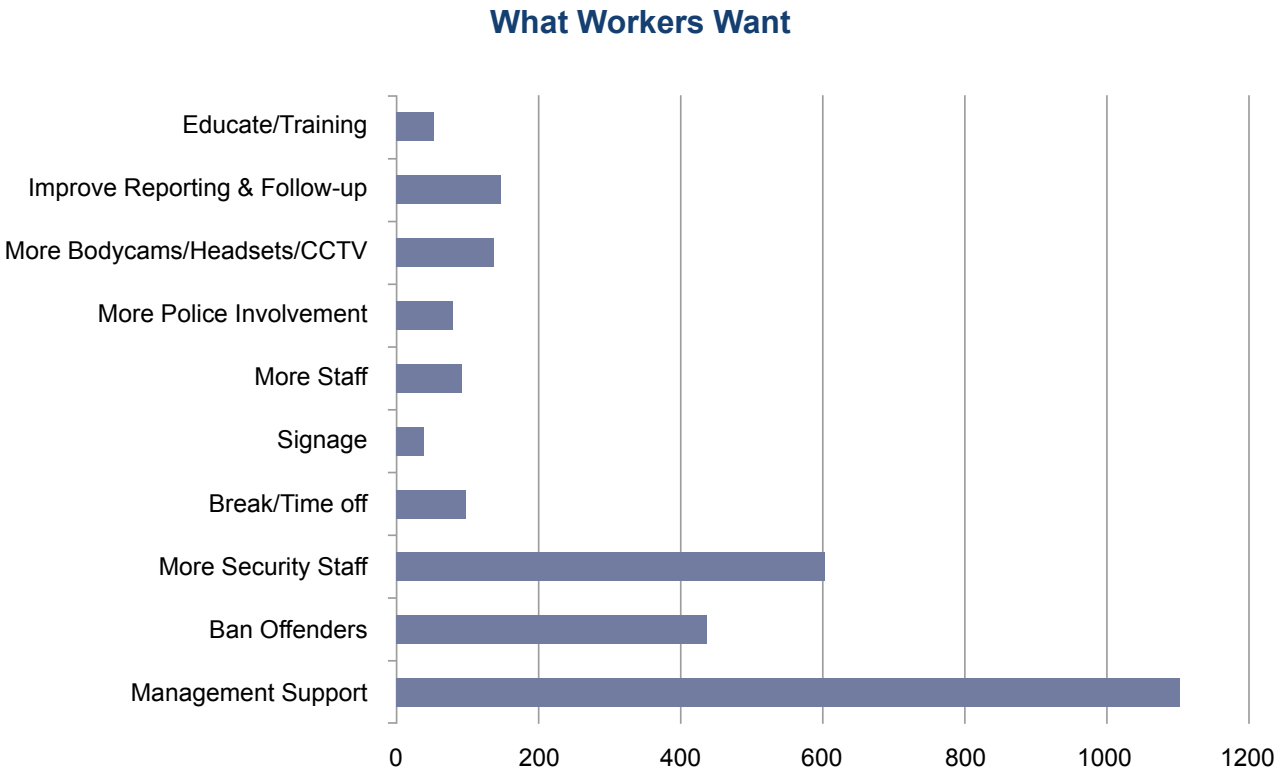
Another opportunity to support staff is through an Impact Statement for Business (ISBs). The statement gives you the opportunity to explain and document the effect the crime has placed on the business and its employees. This statement is used as part of the evidence and taken into consideration by the court when sentencing.

The NBCC regularly receives feedback about the positive impact that ISBs have made at court and the ISBs are strongly supported by the CPS.

More information on ISBs can be found here.

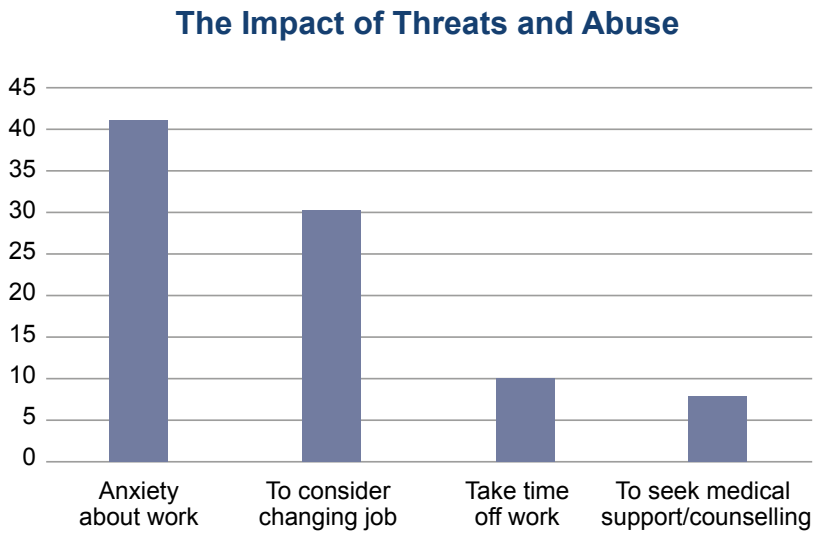
Impact Statement for Business

In the USDAW, Campaign To End Violence And Abuse Against Retail Workers survey (2023) employees were asked what support they wanted to tackle the violence and abuse they experienced at work, by far the biggest request was for management support, demonstrating the value that comes with the correct employee support.



FFF Survey Results Report 2023

The following table from the same survey shows the impact that threats and abuse have on employees, with 30% saying they considered looking for a new job.



On occasions employees who are a witness to a crime will be required to attend court, do you support your employees who are a victim of crime and give them time to attend court to support prosecutions? In the year 2023/24 over 10% of crime reports of shop theft were not supported by the retailer, meaning that the crime was closed with no further action taken against the offender.

The NBCC recognises the role that many employers play in supporting employees in other areas of their life such as those that are subject to domestic violence. The following webpage offers a host of materials around hate crime, recognising modern slavery and supporting employees who are affected by domestic abuse.

Crime Prevention: Safeguarding

Op Portum

We know that when people feel vulnerable, they will look for places where they will feel safe, in our towns and cities this will often be recognisable shops or restaurants etc, irrespective if they are shown as a safe space or not. When this happens, we want to ensure that the colleagues who offer support are prepared to deal with the situation and understand what they should and shouldn't do, which may put them, or your organisation, at risk. The NBCC has developed specific guidance, based upon best practice, of what should be done to support those who feel vulnerable.

Creating Safe Spaces in Retail
Operation Portum

The guidance is supported by a range of products including a video, training slides, in-store staff posters and marketing materials.

The scheme offers over 15,000 safe space locations across the country and is supported by a number of well know high street brands from retail and hospitality. A number of shopping centres and Business Improvement Districts also support the scheme as do some of our largest private security providers, which takes the scheme into other public space locations such as transport hubs, sport grounds and music venues.

The guidance and a full list of supporters is available on our website here.

Corporate Support

The Right Level of Investment

According to the British Retail Consortium almost £1 billion was lost through crime, yet the corporate support in place to manage the processes to prevent loss doesn't always exist with sufficient support to make a positive difference. All businesses have a responsibility to prevent crime, protect themselves and their employees from harm and therefore need to invest in the appropriate resources. We know that loss prevention can be an easy area to reduce costs to save money, the NBCC is keen to support businesses to highlight areas for improvement so as to secure investment.

Private Security

When considering buying private security services the NBCC works closely with the Security Industry Authority (SIA) and we have produced some signposting to help guide you through the process.

Buying Private Security Services - SIA Support

Technology

The use of technology is playing an increasingly important role in fighting crime. Technology such as body worn video has been shown to not only reduce instances of violence but also makes employees feel safer with one retailer seeing a **34% reduction** in violent incidents. Likewise, connected headsets create a feeling of reassurance in the face of reduced staff on the shopfloor.

The vast majority of police forces now use a Digital Evidence Management System (DEMS), which allows CCTV footage to be shared electronically. The NBCC has mapped UK police forces to show which system they use, as well as created guidance on how it can accessed.

Digital Evidence Management System (DEMS)

CCTV Witness statement

The NBCC have worked with the Crown Prosecution Service (CPS) and police forces to develop a standard witness statement which retailers can use when submitting CCTV evidence to the police using a Digital Evidence Management Systems (DEMS).

The standardised statement will ensure retailers provide all of the information the police need to process the CCTV as evidence in a criminal case.

The new witness statement is available as a download on the website and will be accepted by all police forces across England and Wales: **Video Witness Statement**

Facial Recognition

Facial recognition is another area in which the technology has greatly improved, the Information Commissioners Office has recently published some guidance around the use of facial recognition in a retail environment.

Facial Recognition

Other technology to consider includes:

- Using Automatic Number Plate Recognition (ANPR) to create alert for OCGs
- Behavioural analytics
- Real time video analytics for self-checkout

Engagement

Local partnerships such as Business Improvement Districts (BIDs) and Business Crime Reduction Partnerships (BCRPs) play a critical role in our towns and cities to prevent crime. There are in excess of 330 BIDs across the UK generating around £345m from levies.

Business Improvement Districts (BIDS)

Business Crime Reduction Partnerships (BCRP)

If your business pays a BID levy establish what that BID is doing to support to prevent crime, considerations would include:

- Do they operate a BCRP?
- If so, is that BCRP accredited or working towards an accreditation?
- If there an information sharing platform, if so do you as an organisation allow the sharing of data to help raise the awareness of prolific offenders?

Often the NBCC hear accounts of poorly attended BCRP/shop watch meetings by retailers who are reluctant to release their staff, consequently they miss out on key pieces of intelligence around the activity of prolific offenders so making their role that much harder. How do you ensure that local staff are able to support these meetings?

Business Crime Reduction Partnership Accredited

BCRP National Standards

The National BCRP standards were developed as a collaborative effort between BCRPs, businesses, police forces and other stakeholders. The BCRP National Standards provide a single reference for “what good looks like” in order to give reassurance to business members, police and other stakeholders.

Nationally, businesses invest considerable amounts into BCRPs and the NBCC wants to encourage continued and further investment. The NBCC is the national stakeholder for the standards as well as providing an independent secretariat that owns and publishes the standards on behalf of the board.

Visit the NBCC to find out more about the accreditation and the value that BCRPs offer to its members and the local community.

Business Crime Reduction Partnerships (BCRP)

Getting involved with initiatives such as Safer Business Action (SaBA) Days and the ShopKind campaign really helps to bring businesses and police together. More information regarding SaBA Days and ShopKind can be found on the NBCC website.

SaBA Days

There are a number of business forums and membership groups where retailers can share learning and ideas e.g. BRC ops groups, Oris Forums, NBCS etc. The NBCC can also provide advice and contacts should you wish to connect with the local police or Police and Crime Commissioner (PCC).

Many PCCs now have business crime as part of their Police and Crime Plan. Does your PCC have business crime as part of their Police and Crime Plan?

Data

The use of data should be the golden thread through your prevention strategy, here are some examples of how data can support you to prevent crime:

Identifying Patterns

Data analysis can reveal patterns and trends in business crime. By examining historical data, businesses can identify common types of crimes, their frequency, and the locations where they occur most frequently to create crime maps. This information helps in understanding the modus operandi of criminals and allows businesses to take preventive measures.

Deterrence

Knowing that a business has robust data-driven security measures in place can act as a deterrent to potential criminals. Using the data to determine store layout, product placement, location of CCTV cameras, or increased staff surveillance demonstrates that the business takes security seriously and is prepared to respond to any criminal activity.

Evidence Gathering

Data can serve as valuable evidence in criminal investigations. Security cameras, access logs, and transaction records can be crucial in identifying and prosecuting criminals. This information can also be used in civil cases to recover losses from crimes.

Continuous Improvement

Data allows businesses to continually assess and improve their security measures. By analysing incidents and near-misses, they can identify weaknesses in their security protocols and make necessary improvements.

Predictive Analytics

Data can be used to develop predictive models that forecast when and where business crimes are likely to happen. This enables companies to allocate resources, such as security personnel or surveillance, more effectively to prevent crimes before they occur.

Resource Allocation

With data, businesses can allocate their security resources more efficiently, they can determine which areas or assets are most vulnerable to crime and therefore prioritise the security efforts accordingly.

Compliance

Using data to demonstrate compliance with policy and regulations can help avoid legal issues, penalties and monitor the effectiveness of training.

The NBCC has developed a new national approach to data sharing to tackle retail crime. Please visit the Data Sharing page to find out more.

Appendix One
Retailers self-assessment check list

Prevention

- Do you have a crime prevention strategy?
- If so, who has ownership?
- Does the strategy cover the areas included in this guidance?
- How is it reviewed to take into account new and emerging threats?
- Do your crime prevention products hold a security rating/testing accreditation, for example Secured by Design?
- How often do you review your crime prevention policies and products? Are they still fit for purpose?
- Do you share your best practice and learning?
- Do you keep updated with new ideas and products?

Reporting

- What is your company stance with reporting, internally and to the police i.e. do you report everything?
- How is this shared with your staff?
- Do you keep a record of how many crimes are reported, both internally and externally? Can this data easily be shared externally?
- Who has ownership for reporting crimes e.g. just managers, security staff?
- Do your staff know how to report a crime and what information they need to include to ensure you get the right response?
- Are your staff able to report a crime online?
- Why are your barriers to staff reporting a crime?
- Does your security provider have authorisation to report crimes on your behalf?
- Do your internal definitions and reporting platforms align with policing?
- What contact details do they give when reporting a crime i.e. if they left the organisation would the police be able to make contact?

Offender Management

- What is your company policy in managing and deterring offenders?
- What is your policy in relation to the detention of offenders?
- How do you monitor and manage offenders across your business?
- Do you know who your top offenders in each area?
- Do you prioritise/risk rate them?
- Do you have a banning process? Is it a credible and effective process?
- Do you support diversion schemes such as Restorative Justice, offender to rehab etc.?
- Do you conduct your own investigations/surveillance?
- Do you know which offenders have Criminal Behaviour Orders and what their conditions are?
- Can you provide quality intelligence and evidence packs to police for your offenders?
- Do you have a process for civil recovery?

Training

- Are you aware of the training videos offered by the NBCC?
- What staff training is in place to prevent crime and violence against your staff?
- How do know it is being followed and adhered to?
- How often do you review your training?
- Who gets the training?
- What are your priorities?
- Where do you get your training?
- Is your training compliant/accredited/fit for purpose?

Employer's Framework

- Do you invest in products and processes to safeguard your staff?
- Do you have a process to identify violence and abuse incidents against your staff?
- How do you support staff that have been a victim of crime?
- Do you enable your staff to support police and investigations?
- Do you have an Employee Assistance Program?
- Do you provide counselling etc?
- Do you refer to external agencies e.g. EIDA (domestic abuse)
- Do you have a safe spaces initiative, are staff aware of it?
- Do you have a lone worker policy?

Corporate Support

- Do you have the right resources to deliver your strategy?
- Is crime prevention/security an agenda item with the board?
- Do you have the right numbers of staff to support your prevention strategy?
- Do you have an appropriate budget?
- Do you create and review crime prevention/security policies and procedures?
- Do you have a police/law enforcement liaison?
- Do you have a specific security/crime team/hub?
- What support do you have in place to minimise offending e.g. Do you have utilise security guards/store detectives?

Technology

- How is technology being used to protect your staff?
- What technology do you utilise e.g. Body worn video, tagging, facial recognition etc?
- Do you have a Security Operation Centre?
- Do you use technology to support crime prevention e.g. trackers, CCTV, AI etc?
- Can you utilise police Digital Evidence Management Systems (DEMS)?
- Is your CCTV quality sufficient for the positive identification of offenders?
- Are your cameras in the right location to capture good facial images?
- Who has access to your CCTV system to allow police to collect the evidence?
- Do you monitor your stores remotely?
- Do you use an Alarm Receiving Centre?

Engagement

- How do you engage with police and other groups?
- Are your stores members of local BCRPs?
- If yes, how do the stores support the BCRP e.g. engage with shop watch briefings, radio scheme?
- Are you aware of what BIDs you pay into and how much you pay?
- What services do you get from the BCRP/BID you support?
- If there is a BCRP is it accredited, or working towards it?
- Do your stores know who the local police team are, have they engaged with them?
- Do you know who your force PCC is, have you engaged with them?
- Do you support Safer Business Action Days?

Data

- How is data used to monitor your prevention plan?
- Do you share data with your partners/industry colleagues?
- Do you have Information Sharing Agreements with police or partners?
- Do you have a system/platform to capture data in a useable way?
- Do you use data to understand the vulnerabilities within your business?
- How do you share data with policing? Is it in a consumable method and in a format that make it easier for police?

Appendix Two
Legislation

Law & Liability

As business owners there is a wide range of specific legislation that you must comply with.

In addition to those responsibilities, you also have a more general legal 'duty of care', under Common Law, towards those that work within and use your premises, including customers.

There is also further legal duty under the Health & Safety at Work Act 1974 and the Management of Health & Safety at Work Regulations 1992 to assess and control any risks to protect those/anyone who may be affected by your business activities.

There are legal and commercial reasons why businesses should assess and review their security to deter, reduce and mitigate criminal acts, including terrorism.

If this is undertaken in a structured way, recorded, and reviewed appropriately, this includes the possibility of lower insurance costs and the reduction of the risk of any potential criminal prosecution or penalties under health and safety legislation.

More information about your legal and statutory duties can be found at:

www.protectuk.police.uk/law-and-liability

The Risk Management Model

This is an example of a risk management tool, highly recommended by Protect UK.

The Occupiers Liability Act 1957 & 1984

Businesses also need to be aware of The Occupiers Liability Act 1984.

This has implications for those who want to implement preventive measures intended to deter intruders unlawfully entering their premises.

The Act sets out the duties which an occupier of a premises, including businesses, owes to persons, other than visitors, i.e. trespassers and intruders, who come onto their premises.

The Act states that an occupier owes a duty to intruders in relation to risks of which they are aware, and against which they may reasonably be expected to offer some protection.

Therefore, it is their duty to take reasonable steps to ensure that the intruder does not suffer injury; but it also provides that their duty may be discharged by taking reasonable steps to give warning of the danger or discourage persons from incurring the risk.

So far as crime prevention is generally concerned, the effect of the Act is that an occupier will be liable for injuries sustained by an intruder because of any crime prevention devices or measures, whose existence is not reasonably apparent to an intruder.

Therefore, in terms of crime prevention, it is always advisable to warn potential intruders of the risks they would encounter trying to enter premises without permission.

An example would be the use of rotating vanes on top of a perimeter fence. Signage works as specific warning and a general deterrent.

If this is done where devices or measures are installed, which could cause injury to intruders, the likelihood is that the occupiers or businesses concerned will have complied with their requirements under the 1984 Act.

It is good practice to use signs and warn people of dangers.

Data Protection Act 2018 & GDPR

Additional legislation you need to be aware of and comply with is the Data Protection Act (2018) and the UK General Data Protection Regulations (GDPR). These cover the use of personal information and the correct installation and use of any CCTV system to protect your business.

This is all overseen by the Information Commissioners Office (ICO)

If you are a sole trader (or small business owner), you will find lots of useful information available regarding the Data Protection Act to help you remain compliant at:

https://ico.org.uk/for-organisations/making-data-protection-your-business/

https://ico.org.uk/for-organisations/sme-web-hub/checklists/data-protection-self-assessment/

Use of CCTV:

- Have you complied with the Data Protection Act (see information below)
- Have you considered other security measures to compliment and support CCTV
- If you already have CCTV are you able to operate it correctly
- Can you access and download clear images
- Regularly review your CCTV system to ensure it remains fit for purpose
- Is your equipment and installation compliant with BS 62676

You must:

- Put up a sign to let people know CCTV is being used and why
- Be able to provide images within 40 days to anyone you've recorded. (There can be a charge for this access) Ensure they are of 'evidential' quality
- Share images with appropriate legal authorities, e.g. the police, if they ask for them
- Keep images only as long as your business needs them

More detailed information regarding CCTV surveillance guidance and assessment can be accessed at:

https://www.gov.uk/government/organisations/biometrics-and-surveillance-camera-commissioner

This provides a whole range of CCTV camera guidance tools and templates to ensure your CCTV remains fit for purpose and compliant.

This includes a buyers' toolkit for CCTV for small businesses that may be thinking about purchasing a surveillance camera system.

Police Crime Prevention Initiatives

2nd Floor, 50 Broadway, St James's Park,
Westminster, London, SW1H 0BL

Tel: 0203 8623 999

Email: enquiries@police-cpi.co.uk

Web: www.policecpi.com

Home Office

Secured by Design

SBD

Official Police Security Initiative

POLICE CPI

Police Crime Prevention Initiatives