Scottish Business Resilience Centre

A-Z

BUSINESS RESILIENCE COMPENDIUM

@SBRC_Scotland Scottish Business Resilience Centre enquiry@sbrcentre.co.uk

A-Z

BUSINESS RESILIENCE COMPENDIUM

The SBRC Business Resilience Compendium is a compilation of best practice obtained from a number of different sources into one trusted space. It's easily searchable and accessible by any business regardless of size or sector.

It's a one stop shop that offers a variety of advice and guidance to help keep your business safe, secure and resilient against a number of threats that could harm your business and profitability.

The advice ranges from choosing the correct type of alarm for your premises, to business continuity, cyber threats, disaster recovery, physical security, HR, fraud, fire safety and many other types of challenges your business could face on a daily basis. The advice is impartial and is free. It will guide you to some SBRC factsheets and to other external websites, including some of our members, where expert advice can easily be found.

The Business Resilience Compendium will seek to ensure that you don't waste precious time searching for what you need and often not being able to find what you set out to achieve. There won't be any dead ends or frustration in trying to find what you're looking for.

It's all in the one trusted space!

A-Z

BUSINESS RESILIENCE COMPENDIUM


A

ALARMS

Choosing the right alarm system can be confusing due to the variety and different features that are available. Potential criminals will not want to draw attention to themselves and the sound of an alarm will cause most to quickly take what they can and leave, without exploring the entire building.

We have narrowed our advice down to two types of alarm systems:

- Remote Signaling and
- Audible only

Both alarm systems usually have an automatic cut-off, so the noise it sounds does not continue for more than twenty minutes.

For more information on Alarm information please see the following websites:

www.sbrcentre.co.uk/sbrcfactsheet to download our SBRC factsheet.

National Police Chief's Council Security Systems Policy:

www.policesecuritysystems.com

Secured by Design website:

https://www.securedbydesign.com/images/downloads/ALARM_STANDARD_TECHNICAL_GUIDE_A4_web_1.pdf

ARENA'S AND STADIA

If you work in or operate within an arena or stadium and are looking for security or protective advice and guidance please visit the Police Scotland website:

www.scotland.police.uk/assets/pdf/keep_safe/234532/stadia-and-arena

Major events protective security advice can be found on the Police Scotland website here:

www.scotland.police.uk/assets/pdf/keep_safe/234532/major-events

ASSET REGISTER

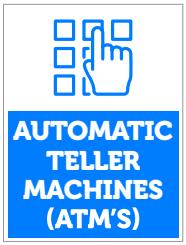
An asset register, which is also known as a fixed asset register, is a record that identifies the fixed assets of a business. Fixed assets refer to the assets that a business uses regularly to produce its in-come, and, unlike those assets in inventory, these assets are not considered as products that can be sold.

An asset register allows business owners to quickly retrieve information on an asset; including its description, purchase date, location, purchase piece, accumulate depreciation and estimated sal-vage value. It should be considered a useful tool in the prevention of theft; as all assets should be accounted for on the register.

ASSET RECORDS

It is of the upmost importance that you maintain an accurate record of all your company's tangible assets; including things such as the serial number, model and make of the property, whether it is identifiable, and if it has been marked with your post code and/or address. You should also record where it is physically located within your premises. Should a stolen item be returned to your busi-ness, it is necessary that you clarify whether your item has been sold or if it has been thrown away or stolen.

In the case of computers, for instance, your asset record should contain the details of the authorised operating systems as well as the software that you have installed on the computer. Recording this information will, amongst other things, enable a faster recovery after any incident which may occur involving the loss of a computer.



AUTOMATIC TELLER MACHINES (ATM'S)

Automated Teller Machines, (ATM's), act as an easy and convenient way to obtain cash. However, as they are convenient and easy, they also are a good target for criminals. If you are a business who manages or has an ATM machine, please consider the points on our SBRC factsheet for advice and guidance on how to minimise the risks associated with ATM machines.

Please see the following Police Scotland website for ATM attack guidance:

www.scotland.police.uk/assets/pdf/keep_safe/atm-device-theft-atm-gas-attacks-guidance?view=Standard

BANKING PROCEDURES AND CASH AND VALUABLES IN TRANSIT

If considerable amounts of cash need banking or collected on a regular basis, the safest method of doing so is to employ a recognised cash-carrying-company.

If your business does its own banking, you must be especially careful.

BANKNOTES

Fraudulent banknotes are made and distributed by well organised criminal gangs for profit, which are often used to fund further crime activity in your community. The use of such banknotes has seen retailers, businesses, schools, charities and the elderly and vulnerable in the UK stripped of their hard-earned cash.

Seasonal times such as Christmas often see more cash (notably £20 and £50 notes) changing hands, and fraudsters often take advantage of this by targeting busy shops and those businesses which employ temporary staff.

For more information on how to confirm a genuine banknote, please refer to the information and advice below:

Scottish Banknotes:

www.scotbanks.org.uk/polymer-banknotes.html

Bank of England banknotes:

www.bankofengland.co.uk/banknotes

Northern Irish banknotes:

www.acbi.org.uk/education-material/know-your-norther-ireland-banknotes.html

Crimestoppers

https://crimestoppers-uk.org/campaigns-media/campaigns/don-t-buy-into-counterfeit-cash

You can use the voluntary, free-of-charge Banknote Checking scheme which promotes the checking of banknotes at the point of sale. It does this through training for those who require it and does so in order to reduce the number of counterfeit notes in circulation.

Videos and Online Banknote Training:

These are all available on Bank Websites (usually under the individual notes). You can find all Bank of England banknotes up-close; including the details of their security features in the banknote guides:

www.bankofengland.co.uk/banknotes/retailers-and-businesses/banknote-checking-scheme

The National Crime Agency also provide advice and guidance on their website:

https://www.nationalcrimeagency.gov.uk/what-we-do/how-we-work/providing-specialist-capabilities-for-law-enforcement/counterfeit-currency

Betwatch consists of a community-based crime prevention scheme and is run by gambling licensees to create a safer gambling environment. It has wide ranging support; ranging from the Gambling Commission to Police forces. The goal of Betwatch is to include a variety of other gambling sectors within their scheme. In fact, and since late 2017, the casino sector has become involved with Betwatch. According to their information note, they are also in discussion with the Adult Gaming Centre (AGC) to include them within schemes that already exist.

Further advice:

www.gamblingcommission.gov.uk/PDF/Betwatch-toolkit.pdf

A great amount of bomb threats are hoaxes, and are often designed in order to cause panic and disorder. In the rare occasion that a bomb threat is genuine, terrorist individuals and organisations also may be seeking to frighten businesses, the public and communities. Often, bomb threats are made in order to draw attention to a particular cause or to mislead the police. Although many bomb threats to involve a two-way call between individuals, some threats are increasingly been known to be sent through email or social media platforms.

No matter how silly the bomb threat may seem, this form of communication is an offence. Alert the police by dialing 999.

It is important that you, as a potential recipient, and either as a direct victim of the threat or a third-party used to pass the message, have plans which detail how information relating to the bomb threat is recorded as well as acted upon and how this information is passed to police.

Further information on this can be found on the Police Scotland website:

https://www.scotland.police.uk/keep-safe/246633/246642/

You can also find information on the Government Website:

https://www.gov.uk/government/publications/bomb-threats-guidance

The National Terrorism Security Office website also offers guidance

https://www.cdn.ac.uk/wp-content/uploads/2016/08/NaCTSO-Guidance-Note-1a-Police-Scotland amended-Advice-to-Education.pdf

Promising, receiving, accepting, giving or requesting a bribe is a criminal offence. In order to protect your business, you should consider developing an anti-bribery policy – especially if there is a risk that someone who you employ or who works on your behalf is exposed to bribery.

The anti-bribery policy that you develop should reflect the level of risk your business may face. Generally speaking, your policy should reflect and provide

- What your approach to reducing and controlling the risks of bribery is
- The rules your business puts in place about hospitality, donations and receiving and accepting gifts
- Clear guidance on how you conduct your business (e.g. how to negotiate contracts)
- Rules on stopping and/or avoiding conflicts of interest

You should read the leaflet below from the Government for more information on how the current bribery laws may affect your business:

http://www.justice.gov.uk/downloads/legislation/bribery-act-2010-quick-start-guide.pdf

The National Crime Agency also provides guidance:

https://nationalcrimeagency.gov.uk/what-we-do/bribery-and-corruption

The Advisory, Conciliation and Arbitration Service offer the following advice on their website:

www.acas.org.uk/index.aspx?articleid=3332

Business continuity is often regarded as a management process. This management process provides a framework to ensure the resilience of your business to any possibility. It also helps to ensure your business can continue providing your service to whoever is your key customer. On top of this, it protects your reputation and brand. Business Continuity provides a foundation for planning to make sure that your business can continue to thrive following any form of unplanned or disruptive event. This includes simple accidents to more serious things such as criminal activity and forms of natural disasters. The plans that you develop and the frameworks which go along with this must be clear and concise as well as fit to the needs of your business. Ideally, your business continuity plan should be integrated into the ways in which you perform your business. Instead of having to catch-up with the effects of accidents etc. on your business, a continuity plan will ensure that you are planned for any incidents that may occur.

Regardless of the size of your business, business continuity must be considered. If you are a smaller business, the key principles of business continuity will be the same as those businesses which are multinationals. The plan you draw up should be reviewed and updated annually.

To reduce physical and asset loss, it is important to ensure that the plan you draw up for your business can be instigated as soon as possible after the event occurs.

In drawing up your plan, you will have to consider the following:

- Guidelines for management
- Identifying what your serious risks are
- Prioritising the operations that must be maintained, and how you will maintain them
- Assigning employees to disaster teams
- Undertaking a complete inventory of your business
- Knowing where to get help
- Documenting the plan
- Reviewing your plan with key employees; training your employees, and testing the plan
- Maintaining the plan
- Understanding if your suppliers have a business continuity plan that can be implemented in a way that the event does not have a large impact on your business

Businesses can suffer simply due to a lack of tried and tested plans that could help keep them trading. Don't allow your business to be one of them.

For information on Business Continuity that includes training courses and providers as well as knowledge and resources, you may which to visit the business continuity institute:

www.thebci.org

The Scottish Government also provide advice and guidance on preparing for and dealing with emergencies through their website https://www.readyscotland.org

SBRC member plan B Consulting also provide advice and guidance in relation to business continuity:

www.planbconsulting.co.uk

Police Scotland website offers further advice:

www.scotland.police.uk/keep-safe/246633/246669/

In order to be adequately secure against potential break-ins, ensure that all doors on your buildings are constructed of solid quality. All accessories to the doors; such as locks, bolts and other fitments should always meet the necessary security standards for the level of risk your business faces. Ensure that lock and fitments are inspected on a regular basis to ensure that they are working and fit for purpose. Similarly, ensure that the frame structures on all windows are fitted with good quality locks and limiters and are fully secured; ensuring that both the fitments and window glass meet the required standards.

With particularly vulnerable windows, consider fitting security bars or grilles, and inspect surrounding masonry regularly for weaknesses and deterioration.

Ensure that you have a competent locking up procedure controlled by a member of staff you trust.

Additional information can be found on the Physical Security Advice and Measures | CPNI | Public Website. Available here:

- **www.cpni.gov.uk/physical-security**
- **www.cpni.gov.uk/intrusion-detection**
- **www.cpni.gov.uk/tracking-systems-0**
- **www.cpni.gov.uk/perimeter-intruder-detection**

Police Scotland also provide advice on their website:

- **www.scotland.police.uk/assets/pdf/keep_safe/234532/secure-in-the-knowledge?view=Standard**

Police Scotland also provide more generic advice for businesses at:

- **www.scotland.police.uk/keep-safe/246633/246636/**

Although operating on the same model and concepts of 'neighbourhood watch', Business Watch operates on a commercial level. It creates a partnership types of law enforcement as well as businesses and those who represent business interests. Business Watches seek to and actively achieve a reduction in crime and serve to deter and prevent criminal activity through cooperation and education. The programs available to businesses vary according to need, but successful groups adhere to these fundamental steps:

- Promote forms of communication and understanding between businesses and forms of law enforcement
- Enhance and encourage forms of cooperation among businesses
- Teach businesses and organisations how to crime-proof their own properties, watch over neighbouring businesses, and document and report any activity they deem suspicious
- Develop a mechanism to quickly disseminate information about area crime

Program Benefits

You are taking important steps in producing a safer environment in the business world (as well as in your community as a whole) if you begin or join a Business Watch program.

In addition to reducing crime, Business Watch also offers many other benefits, including opportunities to:

- Get to know other businesses in your area and network with them.
- Develop a good relationship with police forces and other law enforcement
- Offer your businesses employees with education and training
- Win publicity and community goodwill for your business.

Although you can (and should) protect your business with the right security gear, you can enhance security with the knowledge that everyone is working with you and looking after you. Everybody in your business holds a dedicated knowledge of your business and its surrounding area. If you inform police about anything that you believe to be suspicious you are helping to reduce opportunities for criminal behaviour to occur.

As a part of cooperating in a business watch scheme, all businesses agree that they will remain as vigilant as possible when on the lookout for suspicious and criminal behaviour. Never hesitate in contacting the police if you see something suspicious going on at a business near-by. In order to communicate with other business, you can use collectively purchased radios, as some schemes have already done. However, some schemes are noted to find it easier to have a real-time information sharing system in place that can help them work in unison with the radio or as a stand-alone solution.

Conducting regular informal meetings between partners in the Business Watch scheme and police personnel can help establish methods of targeting resources to reduce crime by sharing information.

For a definitive guide to security within this area, please use the links below:

Scottish Business Resilience Centre website

www.sbrcentre.co.uk/media/2147/cart_security_guide_12mb.pdf

Road Haulage Association website

www.rha.uk.net/news/regional-news/scotland-and-northern-ireland-region

Freight Transport Association

fta.co.uk

Police Scotland Website

www.scotland.police.uk/assets/pdf/keep_safe/234532/supply-chain

Additional advice and guidance can also be found within the Road Safety Section of ROSPA

www.rospa.com/road-safety/

viii

It can take as little as 10 seconds for a thief to remove something from your car- but there are steps you can do to prevent this from happening. The best way to make sure that the belongings you take with you in your car are safe is to ensure that you lock your car whenever you leave it – even if it is only for a short while. Other steps you can do to prevent having your possessions stolen is to:

- Remove everything from the car.
- Ensure that you always close your windows (and sunroof, if applicable)
- Do not store anything in the boot; take these possessions with you
- Store your car ownership information in your home, and not in your car.
- Always ensure that you remove the keys from the ignition.
- Take all your sat nav and removable stereo equipment with you.

Further, using secure (theft resistant) number plates can make your number plates less attractive to potential thieves.

Where you park can make a big difference to the safety of your car and your belongings. Where possible, park in car parks approved by the Police Safer Parking Scheme. You can identify these car parks by looking for their distinctive 'Park Mark' signs.

Further information can be found below:

The Safer Parking Scheme

www.parkmark.co.uk

National Car Parks

www.ncp.co.uk

ix

CASH IN TRANSIT

Cash and Valuables in Transit (also known simply as CVIT's) companies are those companies which are involved in the sorting, storing and transportation of cash as well as other valuables. Such companies are typically associated with retail and financial organisations. However, they also work with Local authorities as well as other members of the public sectors. This is especially true for when having cash is needed for dayto-day business. CVIT's play a vital role in the protection of cash as well as its replenishment for the business world as well as the wider community.

Now, CVIT operatives are licensed under the Private Security Industry Act; which only adds to their high standards of security and training. Regardless of the size of your company, there are range of CVIT services that can meet your needs.

Due to the very nature of the CVIT service, crime is a notable challenge. Since the mid 2000's, the industry has suffered significant losses, following attacks in both cash centres and couriers. As a result of this, the industry has now invested a considerable amount into security measures and new technologies in order to combat robbery. These include DNA dye and glue which works to protect cash as well as target the ways in which money is handled in cash centres, vehicles and ATMs. It also includes new forms of CCTV and body cameras as well as other protective equipment and en-hanced training for those who courier the cash. These sorts of investments have assisted in reducing the number of successful attacks as well as making sure that any money that is stolen is unusable.

Further guidance can be found on the Health and Safety Executive website:

http://www.hse.gov.uk/violence/toolkit/cashhandling.htm

CARAVAN SECURITY

As they are unoccupied more than your main home, caravans are often considered more attractive to thieves. Occupants of caravans are likely to change fairly regularly, and local people may become used to seeing a number of different faces. Caravans may be equipped with expensive, high standard cycles and/or electrical gadgets. As these can be easy to steal and sell one, caravans are an attractive site for thieves.

For more information please see the Camping and Caravanning Club website below:

www.campingandcaravanningclub.co.uk/helpandadvice/technicalhelp/datasheets/keeping-your-caravan-motorhome-or-trailer-secure/

The use of CCTV alone cannot reduce or deter crime. It can however be used in conjunction with other methods of crime prevention and can assist in the detection of offenders.

There is a common misconception that police own CCTV cameras. In reality, most CCTV you see are owned predominantly by local authorities and private businesses.

www.cpni.gov.uk/cctv

British Security Industry Association (BSIA)

planning, design, installation and operation of CCTV surveillance systems code of practice and as-sociated guidance

www.bsia.co.uk/Portals/4/Publications/109-installation-cctv-systems.pdf

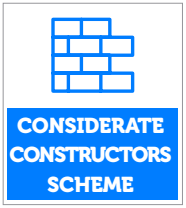
If you operate a cinema and/or theatre and are looking for security advice in this regard please visit the Police Scotland website

www.scotland.police.uk/assets/pdf/keep_safe/234532/cinemas-and-theatres

Computers and laptops are often very attractive to potential thieves. The theft of your computer, however, can have far reaching implications for your business. Although the replacement of the hardware itself will be a considerable issue for you, as is the interruption it will cause to your business, perhaps the most concerning problem occurring from the theft of a computer is the fact that your data can be in the hands of anyone; and they could use it for commercial advantage.

If you have responsibility for security and protective services within the commercial centre area and would like advice and guidance in this regard please visit the Police Scotland website:

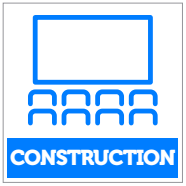
www.scotland.police.uk/assets/pdf/keep_safe/234532/commercial-centres



A non-profit making, independent organisation founded in 1997 by the construction industry to improve its image.

More information can be found below:

www.ccscheme.org.uk



Construction Site Security

For best practice advice and guidance in site security please see below webpage from the British Security Industry Association

www.bsia.co.uk/Portals/4/Publications/123-construction-site-security-a-guide.pdf

According to the Merriam-Webster dictionary, a contingency plan is most commonly understood as a plan devised for an outcome that is different from any usual or expected plan.

Contingency plans are often used in order to manage and for those exceptional risk that, although very rare, may have disastrous consequences. Businesses and Governments often conceive these plans.

Take the disastrous consequence of a plane crash. Imagine a plane carrying many of your employees crashes and kills all of those on board. Your business could be ruined by such a loss. As a result of these risks, however rare, companies often have procedures put in place which can be undertaken should these disasters actually occur. Contingency plans can include policies which aim to mitigate the consequences of a potential disaster – such as restricting the number of employees that are allowed to travel on one plane at one time. If a crisis should occur, contingency plans are developed in order to explore and prepare for any possible incident.

In the time of crisis, contingency plans are often developed to explore eventualities and prepare for them should they occur.

Further information can be found here, on the Scottish Government Website:

www.readyscotland.org/my-business/

NaCTSO[xii]

The National Counter Terrorism Security Office (NaCTSO) consists of a police unit which supports the the 'protect and prepare' strands of the government's terrorism strategy. In supporting a network of approximately 190 counter terrorism security advisors (CTSAs) who are staff and police officers in local police forces, NaCTSO's primary role is to provide aid on all features of counter terrorism protective security to identified industry sectors.

NaCTSO provide help, advice and guidance to both government and industry to try to protect from terrorist threat. The help, guidance and advice they provide covers:

- Popular, crowded places throughout the UK
- Hazardous sites and dangerous substances
- In working with the Centre for Protection and National Infrastructure (CPNI), they provide information on the critical national infrastructure
- Personal security

Guidance Links

The following link provides guidance on the protection of crowded places from terrorist attacks:

www.gov.uk/government/publications/crowded-places-guidance

ACT awareness e-learning was developed as part of a ground-breaking partnership between the retail giant Marks and Spencer and Counter Terrorism Policing. This E-Learning provides information on how to spot the sigs of suspicious behavior and what you should do if an attack should take place.

www.gov.uk/government/news/act-awareness-elearning

Stay Safe Film (Run, Hide, Tell):

www.gov.uk/government/publications/stay-safe-film

This film provides advice for the public on the steps they can take in order to keep themselves in the extremely rare event of a firearms or weapons attack.

The Police Scotland website offers the following assistance

www.scotland.police.uk/keep-safe/246633/246645/

And a video from the Police Scotland website on suspicious activity

www.scotland.police.uk/keep-safe/246633/246648/

Protecting against Terrorism

www.scotland.police.uk/keep-safe/246633/246654/

Security Searches

www.scotland.police.uk/keep-safe/246633/246660/

Bus and coach security

The link provides information on how operators can improve or maintain their security in order to reduce chances of violence on buses and coaches as well as stations and depots.

www.gov.uk/government/publications/bus-and-coach-security-recommended-best-practice

SCaN (See, Check and Notify)

Protect your organisation from a range of threats with SCaN training from NaCTSO and Centre for the Protection of National Infrastructure (CPNI).

www.gov.uk/government/news/security-training-package-empowers-staff-to-see-check-and-notify-scan

Threat Levels and what they mean

www.mi5.gov.uk/threat-levels

First Aid advice during a terrorist incident

www.gov.uk/government/publications/first-aid-advice-during-a-terrorist-incident

Recognising suspicious behaviour

www.youtube.com/watch?v=GTFNYtKf6m8

Recognising suspicious items

www.gov.uk/government/publications/recognising-the-terrorist-threat/recognising-the-terrorist-threat#suspicious-items---guidance-for-the-public

A range of videos from the Centre for the Protection of the National Infrastructure which look at overseas travel, cyber crime, insider threat, firearms incidents, physical security, CCTV and many other items of interest.

www.youtube.com/channel/UCdV9jDLVEhnUGQlQLMX8rfg

Secured By Design

www.securedbydesign.com/images/downloads/resilient-design-tool-for-counter-terrorism.pdf

NYPD Shield

Although directed towards the private sector in New York, NYPD SHIELD is an umbrella program for a series of current and future Police Department initiatives relative to private sector security and counter terrorism. It is a public private partnership based on information sharing.

www.nypdshield.org/public/default.aspx

It is vital that we have a safe and healthy workspace - we spend so many of our waking hours at work. Despite the amount of policy the government has made and all employers do to prevent them, critical incidents occur in work places every week. Although no amount of preventative action can stop major incidents occurring, there are ways in which an incident can be managed. These measures can improve the outcomes for all involved – including passers-by and your employees.

A critical incident can include acts ranging from an unfortunate accident to a serious criminal act. According to others, these can include;

- Armed Robbery
- Assault
- Threat to Life
- An Accident
- A Death
- Terrorism

Witnessing any of the above, even if you are not directly involved, can also be regarded as a critical incident.

Regardless of what actually causes a critical incident, the result of witnessing it or being involved can be distressing. These traumatic experiences can cause different reactions in different people. Although the initial response may seem to be disbelief and shock, other, later responses can also include:

- A reluctance to return to the location of the incident
- Having a higher level of anxiety
- A heightened awareness of potential danger
- Having upsetting memories of the event
- Having problems sleeping
- Experiencing a loss of appetite
- Not being able to relax

A Critical Incident Response (CIR) intervention can provide individuals with psychological support following a critical incident. These interventions are designed to ensure that common responses to critical incidents are normalised and, where possible, prevent more abnormal responses such as Post Traumatic Stress Disorder (PTSD) from occurring.

Your organisation should identify the risks of a critical incident in their workplace and should have a plan about how to react should one occur. One of the best ways to support a plan development is to ensure that you have an Employee Assistance Program (EAP) that will respond to critical situations and employ psychologists. A reliable EAP provider will hold the ability to meet everyone affected by the critical incident quickly and reassure your business of what is required should a critical incident occur.

Employing psychologists following a critical incident means that an assessment of the situation on your employees can be made and follow up support arranged if needed.

You should not ignore the potential impact a critical incident can have. You should reassure your employees that your business and third party organisations are there to support them should they be involved in and witness a critical incident.

Some of your employees may prefer to return to their usual lives quickly, whilst others may take longer. You should recognise and make allowances for the differences in your employees. Help and assessment from a psychologist should be able to provide your business with guidance in this area if it is needed. Although every situation is unique, the long-term avoidance of returning to their normal lives (i.e. work, the location where the incident occurred etc.) is generally discouraged.

You should offer ongoing support to any one of your employees should they need it, whether you deem that everything has gone back to normal or not. It is common for employers to not realise that an employee is still struggling long after the incident has occurred.

Revo [xiv]

Revo has shared protective security guidance in order to assist managers nationally who may benefit from it.

Revo support around 2,300 individuals and over 400 organisations that are within the world of retail property and placemaking. The community Revo has plans, creates, develops and operates places and communities throughout the towns and cities in the UK for people to work, live and enjoy. Members of Revo include publicly and privately listed retailers, as well as owners of retail property, local councils, and advisors and consultants of all sizes.

The guidance produced by Revo is aimed at managers or retail and leisure businesses, and particu-larly those which are based in shopping centres. It sets out the general principles and good practice associated with a model called Integrated Safety Management (ISM) at a non-technical level. Its purpose is to provide general managers with enough understanding to have the ability to confidently assure themselves that the technical business of planning for critical incidents in their environments follow outlined accepted and robust guidelines. It must be stressed, however, that an ISM is a start point. Major/Critical incidents management will rarely, if ever, work without a context of systemati-cally managed activities that develop the capability in the organisation and its people.

The guidance outlined in the ISM covers:

- Preparing (risk, planning, training and exercising),
- Responding to major incidents; and
- Recovering from major incidents

In this guidance, no prior knowledge of major/critical management is assumed.

The ISM is based on (but adapted from) the basic approach of the civil emergency management community. It is well trusted and tried; being the standard framework for continuous improvement in major incident management for over 25 years. It is stressed that this is capstone guidance. Your intention should be, in due course, to follow it up with more detailed guidance suitable for practitioners.

More information can be found here:

https://nbcc.police.uk/attachments/Managing%20a%20major%20incident%20NEW.pdf

Police Scotland website offers the following guidance in relation to preventing robberies:

www.scotland.police.uk/assets/pdf/keep_safe/234532/working-with-business-to-prevent-robbery

The Cross-sector Safety and Security Communications (CSSC) hub is a part of a partnership between law enforcement agencies, local and national government organisations and businesses in the private sector. In operating under a charity status, the CSSC aims to help businesses remain safe and secure by providing them with information that can help them develop robust resilience and emergency preparedness plans.

More information is available here:

www.thecssc.com

Cyber-crime, or computer-oriented crime, is generally understood as crime that involves a computer and a network. Within these crimes, computers can either be used as the commission of a crime or can be the target.

For further information about how you can recognise and reduce your risk of becoming a victim of cyber-crime, please refer to the links below:

Online safety for businesses with Get Safe Online

www.getsafeonline.org

The Advisory, Conciliation and Arbitration Service offer the following advice on their website:

www.acas.org.uk/index.aspx?articleid=3375

The Scottish Business Resilience Centre:

www.sbrcentre.co.uk/services/cyber-services/

The little book of big scams:

www.ourwatch.org.uk/wp-content/uploads/2018/06/the-little-book-of-big-scams.pdf

The National Business Crime Centre – Little book of big scams:

https://nbcc.police.uk/guidance/little-book-of-big-scams-third-edition

The National Business Crime Centre – Little book of cyber scams:

https://nbcc.police.uk/guidance/little-book-of-cyber-scams

The National Business Crime Centre – Little leaflet of cyber mistakes:

https://nbcc.police.uk/guidance/little-leaflet-of-cyber-mistakes

The National Cyber Security Centre, Cyber information sharing platform:

www.ncsc.gov.uk/cisp

The National Cyber Security Centre:

www.ncsc.gov.uk/

The National Crime Agency:

www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime

Police Scotland:

www.scotland.police.uk/keep-safe/keep-secure-online/cybercrime

CYBER

Centre for the protection of the national infrastructure:

https://www.cpni.gov.uk/cyber-security

Tips for Staff

The below link is for the National Cyber Security Centre. The training that the link provides is free of charge, easy-to-use and is usually completed in under 30 minutes. It explains to employees why cyber training is important and how cyber-attacks happen. It then covers four key areas:

- defending yourself against phishing
- using strong passwords
- securing your devices
- reporting incidents

The training, although mostly aimed at SMEs, charities and the voluntary sector, can be applied to any business and/or organisation. It's been deliberately designed for an audience with little knowledge of cyber security and has tips which can complement any existing policies and procedures. It is available by clicking the below link.

www.ncsc.gov.uk/training/top-tips-for-staff-web/story_html5.html

CYCLE SECURITY

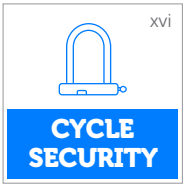
Bike security should be a serious concern for cyclist as well as anyone who is thinking of buying a bike or taking up cycling. Unfortunately, bikes do get stolen and are rarely recovered. In fact, a study conducted by University College London (available here) suggests that, once bike theft occurs, many individuals just give up cycling.

If you do not have the opportunity to park and leave your bike behind a locked door when it is not in use, you should buy a bike lock. While having a bike lock is better than not having one, you should always take into consideration what level of protection the lock is able to provide your bike. You can test your lock again Sold Secure (available at www.soldsecure.com). However, and although helpful, this is not required by any law or policy in the UK.

You should always use your bike lock, even if you are only leaving your bike for a short amount of time. If you do not have a lock, anyone can steal your bike. If you lock your bike, only those who know how to break a lock have the opportunity to steal it.

Where possible, you should lock your bike to secure, solid object like a bike stand. You should al-ways ensure that whatever you lock your bike to is a closed loop. This means that a potential thief cannot simply lift the bike over the top of the object. You shouldn't use anything that is flimsy either – the thief can simply cut that instead of the lock.

If you choose to use a U-Lock you should lock the bike down low, and towards the bottom bracket or seat tube. Where possible, you should attempt to fill the shackle of the lock with as much of the bike and object you are locking it to will fit. Attempt to leave as little daylight in it as you can. Doing this will make it much harder to detach without a key.



Locks with are shorter and narrower than others are often more difficult to attack than larger ones, but more difficult to attach to the bike. If you use a cable or a chain to lock your bike you should wrap it in a way that makes sure it is kept tight – doing such makes it stronger against any form of attack. Should you use a gold-standard lock with a proper key, the lock is likely to be both pick and drill proof. You should make your lock as hard to get to as possible. Keep a spare key for your lock somewhere safe.

Make sure your bike lock doesn't seize and oil it every so often. You should use oil and place it into holes in the lock and make sure you work it in by repetitively opening and shutting the lock. Should your lock completely freeze over winter, you should firstly pour hot water over it and then oil it afterwards, using the technique describe above.

Always try to lock your bike in a public place where it can be seen by many people, and is well lit. If you can, lock your bike somewhere that is covered by CCTV.

According to previous research, roughly half of recorded bike thefts occur from the bike owner's property. If you have room at your house, try and keep your bike locked within the house. If you own a garage or a shed, you should use a wall or floor mounted anchor lock for that added bit of security. If you are going to use a shed or garage in order to store your bike, you should have a decent lock for your shed. You should also consider having some form of alarm system – this will deter thieves.

There are a wide range of locks up for sale. The more security you want the more you will have to pay.

The thin cable locks for sale are officially known as 'immobilisers'. The lightest ones on sale use 2mm wire cables and a combination lock which is in a plastic body roughly the size of a mobile phone. Unfortunately these types of locks won't be able to stop a thief from taking your bike – they can easily be broken with cable cutters. They may be okay when you are leaving your bike for a cou-ple of minutes.

Unfortunately, it is often the case that people think a thicker cable (i.e. a 7mm cable) will provide greater security for bikes. They do not. Although harder to cut, the extra thickness is sometimes just extra plastic.

D-Locks (or known more commonly as U-locks) provide what is probably the best compromise between security and portability for most cyclists in towns. These can be easily carried in the brackets of the bike which are fixed to the frame. If you live in a high-risk area or own a more expensive bike, you should consider using a U-Lock which has a smaller shackle.

If the weight of the lock is not a concern to you, motorcycle-style security chains offer some of the best protection. It must be noted, however, that many of these can still be bolt-cropped. You can use, in addition, and although not commonly found in the UK, a nurse's lock (also known in the frame or a wheel lock). These types of lock fit permanently to the bike's seat-stays. This type of locks works by consisting of a locking bar which sits between the spokes of the back wheel. This ensures that no one can ride off with the bike. This type of lock is always there.

Even if your bike is locked securely thieves can still parts of it. If your bike has parts that are held together by a quick release skewer, then they can be removed by thieves in a matter of minutes. If you have to lock your bike up in a place which is in public and busy, you should consider adding extra security to your bike. You can bind the quick release levers to the frame in order to add additional security. Alternatively, you can replace the quick release skewers with Allen bolts. You will need dedicated tools to do this.

Bike thieves are also noted to steal bike saddles. If you do not want to continually loop an extra cable through the stays every time you lock your wheels, then you should consider creating a permanent anchor from you bike salle to the main frame of your bike. You can do this by using an old bike chain and feed it through an inner tube.

In order to protect your bike further you can:

- Use immobilise or bike register to identity and register your bike
- Etch your postcode to the main frame of your bike
- Remove the saddle of your bike and take it with you when you leave your bike
- Keep photographs of your bike, and identify any distinctive marks or features it may have

What should I do if my bike gets stolen?

- Report it to the police. Use 999 if the theft is still happening. Use 101 if the theft has already happened.
- If your bike is taken from a train station or a tube station, contact the British Transport Police on 0800 405 040
- You should check popular selling sites such as eBay and Gumtree to see if your bike (or parts of it) is being sold. If you do this you can sign up for alerts for bikes that match your bikes description.
- Use social media to share that your bike has been stolen
- If you have a local bike shop let them know your bike has been stolen, just in case someone brings it in for repair

Your household insurance may already cover bike insurance. Often, it is the case that the maximum value of the bike is approximately £300. Alternatively, you can take out cycle-specific insurance in its own right. Cyclecover provide this.

If you choose to insure your bike, remember and write plenty of information about your bike. Record the frame number of your bike. Take a photo of your bike where you store it. If you still own it keep the receipt of purchase for the bike.

If you purchase a lock, it may come with a guarantee if your bike is stolen. Check the small print. You may have to send the lock to the company. However, it is unlikely thieves will leave the locks lying around.

The only way to ensure your bike never gets stolen is to keep an eye on it constantly. However, with a good lock and some common sense you can keep your bike safe.

Protective and efficient security for your business depends on a variety of different measures that are used to detect, deter and delay any attack from occurring. The cyber security measures that your business has should form part of a multi-layered strategy that includes physical and employees/people security. All businesses rely on the availability, confidentiality and integrity of their data. The essential everyday services that we use rely on the integrity of cyberspace as well as the infrastructure, systems and the data that underpin it. This is why cyber security is increasingly important to ensure businesses have the best protection.

More information can be found at the following websites:

National Cyber Security Centre:

www.ncsc.gov.uk/guidance

Cyber Essentials:

www.cyberessentials.ncsc.gov.uk/advice/

Centre for the protection of the national infrastructure:

www.cpni.gov.uk/cyber-security

See also Cyber, Page 25

Regardless of the size of your business, it is likely fair to say that it relies on IT to function. However, all IT - whether it is a mobile device or a cloud-based application - is open to failure.

Ensuring you have the practice of preparing for downtime, and of the taking steps to ensure a quick return to normality is often understood as disaster recovery (DR) planning. It is not easy to create effective DR plans, and this is especially true if you are only a small business. Creating an effective DR plan requires time, knowledge and expertise.

Most commonly, a DR plan will consist of the policies and procedures that your business will follow when its IT services become disrupted - regardless of its cause. The fundamental idea of DR plans is to have steps and procedures that will restore your business procedures back to normal as quickly as possible.

The DR plan you create should take into account the following points:

- **IT services:** Which business processes are supported by which IT systems? What are the risks presented should your IT system stop working?
- **People:** In a given DR process, who are the stakeholders (both on the business and IT side) that need to be taken into account?
- **Suppliers:** Which of your external suppliers would you need to contact in the event of an IT outage?
- **Locations:** Should your normal premises be rendered inaccessible, where will you work?
- **Testing:** How will you test the DR plan you create?
- **Training:** What sort of training and documentation will you provide to end users?

At the heart of most DR plans are two very important KPI's. These are typically applied individually to different IT services: recovery point objective (RPO) and recovery time objective (RTO). Although the jargon may seem confusing, RPO's and RTO's are not, and they are in fact very simple:

RPO: The maximum age of a back-up before it stops being useful. If you and your business can afford to lose a day's worth of data in whatever system you may have, you can set an RPO of 24 hours.

RTO: The maximum amount of time that is permitted to elapse before the backup is implemented and your normal business processes are resumed.

Creating a DR plan for your small business is complicated, but many existing ones follow a similar structure which encompass definitions, duties and simple step-by-step plans and responses to procedures and maintenance activities. Some examples, like those developed by Ontrack UK, include:

- **Introduction:** A summary of the objectives and scope of the plan (including what your IT services are and the locations they cover. Your RPO's and RTO's for different services, and your testing and maintenance activities). You should also include a revision of histories to track changes.
- **Roles and Responsibilities:** Your DR should also include a list of all the internal and exter-nal stakeholders involved in each of the DR processes- complete with their contact details and description of their duties
- **Incident Response:** Make sure to cover when the DR should be triggered, and how and when you will notify your employees, management, partners and customers.
- **DR Procedures:** In this section, and once the DR plan is triggered, the stakeholders can start to action a DR process for each of your affected IT services. Within this section, you should discuss these procedures step-by-step.
- **Appendices:** These should include a series of other lists, forms and documents relevant to your DR plan- such as the lists of details on alternate work locations, insurance policies, and the storage and distribution of DR resources.

There is no point creating a DR if you are not willing to allocate the sufficient resources or training to staff to support the DR plan. Keep the plan up to date; as time passes and your business grows, you will likely employ new and adapt to other IT systems, and it is important these are integrated into the DR plan.

Lastly, it is vital that you test your DR plan and know whether you RPO and RTO's are viable, and whether your procedures are fit for purpose. Test it in its entirety from time to time - this will show you if any of your outline processes do not work together, or whether they are fine. Doing so will also allow you to account for anything that you may have initially failed to account for.

The threats posed by Drones or Unmanned Aerial Vehicles cover a broad range of factors.

Some examples are:

- Nuisance and/or reckless use
- Protest
- Reconnaissance
- Espionage
- Physical attack

To find out more about some of the risks posed to your business please see below:

www.cpni.gov.uk/counter-unmanned-aerial-vehicles

Dealing with Substance Misuse at Work

First and foremost, you must make sure that your employee handbook outlines clear information on your business's disciplinary measures and investigatory interviews. You must assure that this handbook is available to everyone.

As a part of your businesses drug and alcohol policy, you should clearly explain your expectations on the use and misuse of drugs and alcohol whilst at work. This is especially true if you run a business where alcohol is readily available. If you allow your employees to drink at work, you must outline the expectations on how they are expected to preform, or state that you employ a zero-tolerance policy. Within this, it is vital to include all information of the expectation UK legislation has on alcohol and drugs, and especially on drink driving.

If your business plans on implementing searches for drugs and potentially confiscating substances, you need to provide information of this. The same applies if you are planning on screening for drugs and alcohol. It must be noted, however, that this sort of searches can foster a culture of mistrust among your employees, they are often expensive, and they often do not work.

Your policy also must include information of which individual is responsible for implementing said policy, and how any suspected substance misuse will be investigated.

Further information on drugs and alcohol can be found on the Scottish Centre for Healthy Working Lives website:

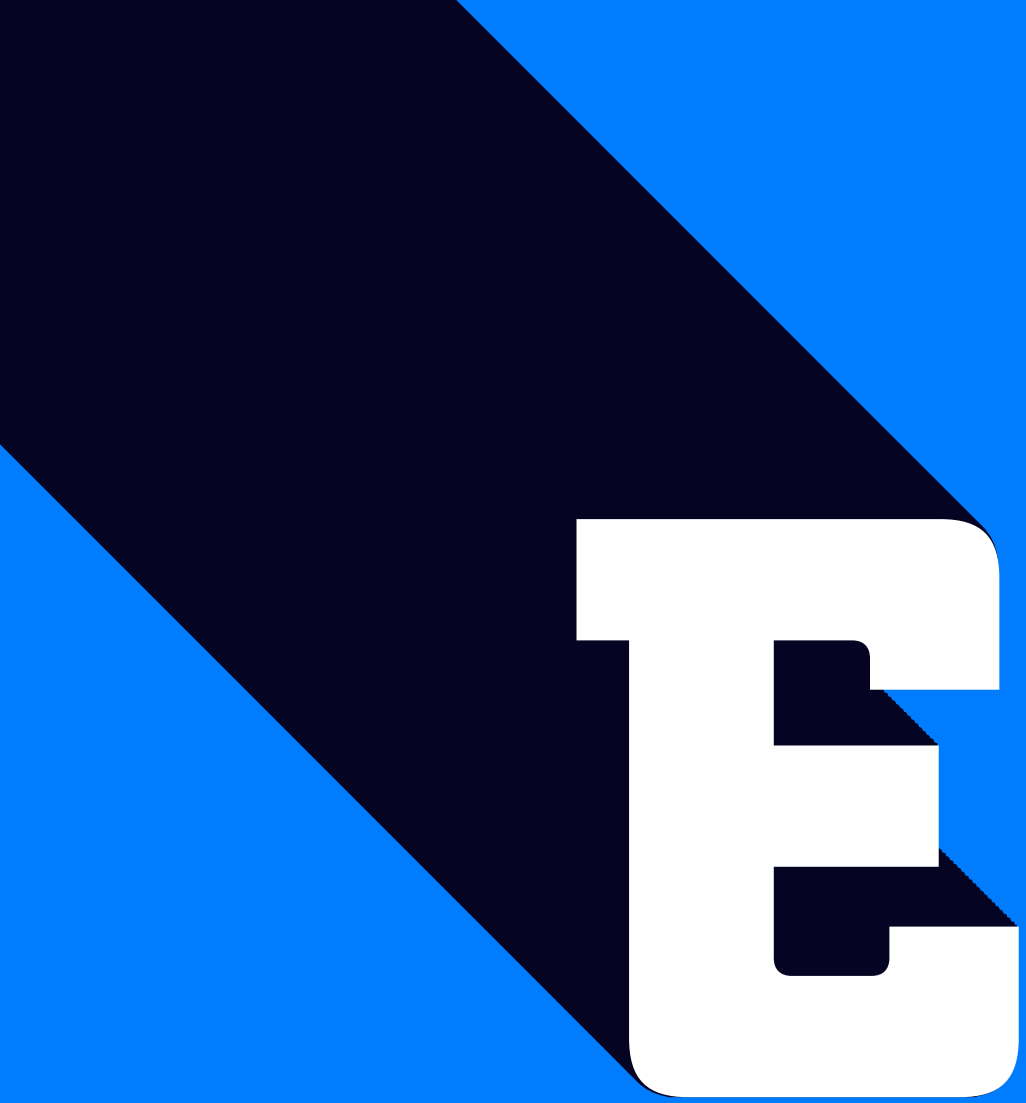
www.healthyworkinglives.scot/workplace-guidance/health-improvement/Pages/health-improvement.aspx

Advisory, Conciliation and Arbitration Service website

www.acas.org.uk/index.aspx?articleid=1986

Police Scotland Website

www.scotland.police.uk/keep-safe/personal-safety/substance-misuse



If you are responsible for security and protective measures within an educational establishment please visit the Police Scotland website:

www.scotland.police.uk/assets/pdf/keep_safe/234532/education-sector

Consider discussing and drawing up your plans with:

- Your local police
- Your local fire and rescue service
- The ambulance services
- Emergency planning

For fixed premises like stadiums and arenas, you should discuss your plans with the venue management. You should do this and make sure the complexity of your discussions is proportionate to the risks that are involved with your business. As you are the organiser in the situation, the emergency services that you collaborate with must ensure that you make clear who is responsible for what during an emergency or critical incident.

Your emergency plan should ideally look to address the following basic requirements:

- How to get everyone away from immediate danger
- How to get emergency services onsite and assist them
- How you will handle casualties
- How you will deal with those who have been displaced but not injured
- How you will liaise with emergency services and other authorities, and, if the situation is serious, how you will hand over responsibility for the incident or emergency
- How you will protect property

The procedures for staff and volunteers to follow in an emergency should include:

- How staff should raise an alarm and how they should inform the public
- What the onsite emergency responses are (such as the use of fire extinguishers)
- How staff should summon emergency services and work with them
- What the crowd management, and evacuation where necessary, procedures are
- How they should evacuate people with disabilities
- What the traffic management procedures are (including emergency vehicles)
- What the incident control is
- What sort of first aid and medical assistance they should provide

Ensure you have enough medical assistance and ambulances onsite. Cooperate with your local NHS and ambulance services so they can assess what your needs are against what their local capacity is.

At events where ambulances are onsite, excluding smaller lower-risk events where emergency ser-vices may not be needed, you should make emergency plans in conjunction with the local NHS ambulance service. These plans should clarify how patients will be transported to hospital should the need arise.

Refer to the Events Industry Forum's 'purple guide' as it includes examples of first aid and medical assessments for an audience at an event.

You should make sure that you have individuals who will implement your organisations emergency procedures if there is an emergency or critical incident. Make sure that the relevant individuals, whether they are staff or volunteers, know and understand what they should do in the case of an emergency.

Ensure that they know:

- Where all of the exits are located
- How to safely use all of the emergency equipment
- How to raise an alarm
- Who should be receiving instructions from

Major incidents and emergencies can develop very quickly. Ensure that you are equipped to move individuals in your premises to a total or relative place of safety without any delay. The following may help:

- Plan escape routes, and make sure that they are always unobstructed and ready for use
- Ensure that all doors and gates that lead to final exists from your premises, as well as site exits themselves, are available for immediate use around the clock. Make sure they:
  - Are always unlocked. However, if you are fearful about security, you should staff the door, not lock it.
  - Are always free from any obstacles
  - Are always open outwards in the direction of the escape

You should always consider using signs, especially for those who are unfamiliar with escape routes. You should light all the escape routes sufficiently to ensure that they are safe for people to use in an emergency. All the emergency lighting that you use should meet the requirements outlined in British Standard BS 5266-1. You should use an independent power source like a generator just in case your main electric supply fails. If you use floodlighting or lighting towers as a temporary light source, but make sure that it does not shine in people's faces when they are walking along the escape route. This will make it more difficult for them. Consider using festoon lighting along the escape route in order to prevent glares.

You should always plan on how to evacuate people to a place of relative safety from the incident from which they can make their way to a place of total safety from the incident.

Your emergency plan must include a plan which states what additional assistance you will people with all forms of disabilities, children and those with limited mobility. Your emergency plan must also detail on how you will safely evacuate children who are separated from their parents (such in play arenas). Make sure you do this, so parents do not defy the normal direction of escape trying to reach their children.

Always plan for how you will communicate official event messages to the public, and in collaboration with the emergency services. Consider the use of social media.

Once your risk level is reduced to an acceptable level, you can consider returning to business as normal - but only do so after a consultation with any other key agencies you have on site (such as the emergency services). Make sure your staff are ready to be back in their roles and all your services are ready to go on as normal.

If any emergency service declares an emergency/major incident on site of your business or premises, everyone must work under the command of the police. It must be noted that the police may declare only one part of the event as being under their authority, but in your capacity of the event organiser, may leave other parts of the event under your control.

In the vast majority of cases, the validation and testing of your emergency plan will take the form of a table-top exercise. In this, you and others will work through a range of scenarios to establish the effectiveness of your outlined responses.

The Business Emergency Resilience Group (BERG) have produced a guide which outlines a list of considerations and offers links to further advice if it is required.

The document is available at:

- **www.bitc.org.uk/campaigns-programmes/communities/business-emergency-resilience-group/prepare**

and further information is available on the Business in the Community Website:

- **www.bitc.org.uk/scotland**

Joint Emergency Services Interoperability Principles

- **www.jesip.org.uk**

Government Websites

- **www.gov.uk/topic/public-safety-emergencies/emergencies-preparation-response-recovery**
- **www.gov.uk/guidance/emergency-planning-and-preparedness-exercises-and-training**

The Scottish Environment Protection Agency (SEPA) is a non-police reporting agency, and it able to send reports to the Procurator Fiscal recommending prosecution. SEPA works with the Crown Office and Procurator Fiscal Service to improve the prosecution of environmental crime in Scotland.

For more information please see below

Zero Waste Scotland

www.zerowastescotland.org.uk/

Scottish Government WebsiteS:

www.environment.gov.scot/our-environment/

www2.gov.scot/Topics/Environment/waste-and-pollution/environmental-crime-taskforce

Europol Website

www.europol.europa.eu/crime-areas-and-trends/crime-areas/environmental-crime

Scottish Environment Protection Agency Website

www.sepa.org.uk/regulations/how-we-regulate/policies/environmental-crime-protocol/

Government Website

www.gov.uk/report-an-environmental-incident

It is vital that you have plans in place to effectively respond to health and safety incidents and other emergencies that may occur within your premises.

The emergency plan that you create should be created in proportion to the level of risk that is presented by your event activities, as well as the potential extent and severity that the incident may have.

Using the resources you have available to you within your premises, you should develop emergency procedures that should be followed by your staff and any volunteers you may have. Such incidents can include sudden bad weather, a fire, or any sort of structural failure.

You should also consider what your response to more serious emergencies you will have; especially those incidents that will require response and help from any emergency service.

Extortion (which is also commonly known as a shakedown or outwrestling or exaction) is a criminal offence that consists of the obtaining of money, property or services from an individual or institution through forms of coercion. It is often used by organised criminal groups (OCG).

It must be noted that the actual obtaining of money or property is not required in order to commit the offence. Simply making the threat of violence which refers to the requirement of money or property to stop any other violence is sufficient enough to commit the offence of extortion.

Exaction refers not only to the extortion demanding and obtaining of something through force but also to the means of infliction of something such as pain and suffering or making somebody endure something unpleasant.

Extortion can be conducted on-line with recent such instances occurring to major companies as well as individuals. It is essential that no monies are paid as a consequence and that any such threat is reported to the police. In general terms the threat will come in the form of an e-mail and demand payment in bitcoin. Care should be taken not to open links from email recipients which are not known to you as they can contain a virus to close down systems with a demand to pay and have any data returned.

Further information can be found below:

www.europol.europa.eu/publications-documents/prevention-and-coping-strategies-kidnapping-hostage-taking-extortion

The Anti-Counterfeiting Group (ACG) are the voice of businesses who help shape deterrents against counterfeiting within the UK. They believe work to represent the interests of a wide range of businesses and individuals in the UK in order to ensure that businesses and business owners have the right to protect their brand from being used illegitimately by other individuals and businesses. They campaign in order to change the view that counterfeiting objects and goods is simply a harmless activity and hope to expose it for what it is: a serious organised crime. Members of the ACG are widespread and represent approximately three thousand brands in 30 + countries.

Their website is available here:

www.a-cg.org

Scottish Anti Illicit Trade Group

The Scottish public are regularly exploited and defrauded by criminals who sell them illicit products. These sales have a negative impact on Scottish society, as, unlike legitimate businesses who produce legitimate products, these criminals do not pay taxes- something which is vital to the funding of our public services. The illicit goods that these criminals sell may be of poor quality and can even be injurious to the public's health. It is vital, therefore, that we develop and undertake processes that help tackle these trades.

The Scottish Anti Illicit Trade Group holds an extremely important role in bringing together different sectors from across the business and government worlds in order to reduce the ways in which illicit trade hurts our society.

More advice and guidance can be found on the Europol website

www.europol.europa.eu/crime-areas-and-trends/crime-areas/intellectual-property-crime

Intellectual Property Office

www.gov.uk/government/organisations/intellectual-property-office

Your farm yard will contain valuable equipment that will appeal to thieves - such as power tools and quad bikes. Any isolated buildings, barns, machinery and livestock will present the greatest risk in regard to theft. The following are tips you can consider employing in order to reduce your farms risk of becoming a victim of theft:

See Rural Crime, page 93

The following points have been developed by the National Counter Terrorism office and are a ten-point security plan for those registered users of Ammonium Nitrate. You must adhere to these points and must immediately report any activity you deem suspicious regarding this material. Suspicious activity can include theft of the material, as well as the attempting to purchase the material when not licensed to do so. These ten points are:

- You should never store fertiliser where the public have access to it
- You should never leave fertiliser in your field over night
- You should never leave fertiliser near, or visible from, a public highway or road
- You should note that it is a criminal offence to sell on ammonium nitrate fertiliser without having the appropriate property certificate (also known as a detonation resistance certificate)
- You should always record when fertiliser is delivered to you, and when you use it
- If it is possible, you should lock your fertiliser in a compound- so long as it is in regard to HSE safety guidance
- You should always fully sheet your fertiliser if you store it outside, and you should check regularly to ensure your stack has not been tampered with
- You should carry out regular stock checks of this material
- You should report any stock discrepancy or losses to the police immediately
- You should always purchase your fertiliser from a Fertiliser Industry Assurance Scheme (FIAS) approved supplier

The vast majority of firearm and shotgun certificate holders display a high level of safety awareness. Always be aware that you are in possession of a lethal weapon. It only takes a lapse in concentration in which a tragedy can occur.

Further tips and guidance can be found from the Police Scotland website

www.scotland.police.uk/keep-safe/280693/stay-safe-firearms-and-weapons-attack

Fraud refers to those crimes in which an individual uses some kind of deception for the purpose of personal gain, and with technological advances, individuals are now becoming increasingly sophisticated in how they choose to commit fraud. Many of types of fraud now exist.

The following section provides information on the different ways individuals are noted to commit fraud and will provide advice on the ways in which you can avoid becoming a victim of fraud.

Reporting Fraud

If you want to report a Fraud, please contact Police Scotland by dialling 101.

Police Scotland, identity theft, fraud and scams

www.scotland.police.uk/keep-safe/personal-safety/identity-theft-fraud-and-scams

Police Scotland , If you are a victim of fraud

www.scotland.police.uk/keep-safe/advice-for-victims-of-crime/fraud/

Police Scotland, general advice on business fraud

www.scotland.police.uk/keep-safe/246633/246663/

Police Scotland, Bank Mandate fraud

www.scotland.police.uk/assets/pdf/keep_safe/bank-mandate-fraud?view=Standard

Police Scotland, business fraud advice

www.scotland.police.uk/assets/pdf/keep_safe/business-fraud?view=Standard

Police Scotland, general advice on business fraud

www.scotland.police.uk/keep-safe/246633/246663/

Complex/High Value Fraud

You should report fraud and any other financial crime to Police Scotland without delay. Reporting these sorts of incidents helps Police Scotland tackle fraud and allows them to identify areas of concern and patterns of behaviour. Any information you provide on fraud is valuable and could help prosecute offenders and ensure the safety of the public. Police Scotland will record all the information you provide, and the appropriate action will be taken.

If you do not wish to call, you can also email **contactus@scotland.pnn.police.uk**

Further information can be found on the National Business Crime Centre's website – little book of big scams business edition:

https://nbcc.police.uk/attachments/the-little-book-of-big-scams-business-edition.pdf

Police Scotland websites:

www.scotland.police.uk/keep-safe/personal-safety/identity-theft-fraud-and-scams

www.scotland.police.uk/keep-safe/advice-for-victims-of-crime/fraud/

www.scotland.police.uk/keep-safe/246633/246663/

CIFAS - The Uk's leading fraud prevention service

www.cifas.org.uk

Your business must have a clear and well-defined fire safety policy to ensure the safety of all individuals who may be on your premises. This policy should include the arrangements for the planning, the organisation, the control, and the monitoring and review of any fire safety measures you have.

Guidance on this can be found here:

Scottish Government website

www2.gov.scot/Topics/Justice/policies/police-fire-rescue/fire/FireLaw/GeneralGuidance

Scottish Fire and Rescue Website

www.firescotland.gov.uk/your-safety/for-businesses.aspx

Emergency Fire Action Plan

Your business should have a written emergency fire plan. This plan should set out the action that your staff and any other people who may be in your building should undertake should a fire break out. You should keep this plan on your premises and ensure that it is written in a format which means everyone can understand it. All you staff should know it and it should inform the training and instruction that you provide. You should make the plan available for inspection by the enforcing authority.

UFAS Reduction (Unwanted Fire Alarm Signals)

Within the United Kingdom 44% of Fire and Rescue call-outs turn out to be UFAS activations, Unwanted Fire Alarm Signals false alarms. During 2014/15 The Scottish Fire & Rescue Service within the Greater Glasgow area alone responded to 14,800 incidents of which 40% (6000) were UFAS incidents. False alarms result in approximately 27 minutes of business interruption time and a financial impact of an average of £848 per incident to a business. The cost to the Scottish Fire & Rescue Service to attend each UFAS incident is approximately £1970 but not only that, false alarms impact upon SFRS operational resilience in terms of resources available to attend more serious incidents, they impact negatively upon our operational training effectiveness and community safety initiatives as well as increasing risk to members of the public and our fire crews on the road travelling to UFAS incidents. Attending UFAS incidents also needlessly increase the carbon footprint of the service due to fire appliance movements.

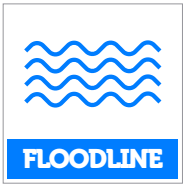
Unwanted Fire Alarm Signals

https://www.firescotland.gov.uk/your-safety/for-businesses/unwanted-fire-alarm-(ufas).aspx

Preparing your business for a flood

In order to ensure that your business is prepared for a flood you should:

- Make sure that your gutters and drains are in good repair
- Move all valuable material from the ground floor areas as well as basements and yards. If you cannot find any form of alternative storage you should consider moving your valuable materials up high and out of the reach of any flood waters
- If your business resides in what is considered a flood risk area, you should consider buying temporary defenses. The National Flood Forum runs the Blue Pages which provides a good starting point. If you have already bought temporary defense products, you should make sure that they are accessible at all times and fit correctly
- Ensure that you and your employees have access to email, contact details and documents. In the event of a flood, you and your staff may have to work from home.
- Check your insurance policy.



Floodline is operated by the Scottish Environment Protection Agency (SEPA) and provides anyone with information and advice on how to prepare and cope with the effects of flooding. Its open 24/7.

Their website can be found here:

https://www.sepa.org.uk/environment/water/flooding

More information can be found in the following websites:

Scottish Government website

https://www.readyscotland.org/my-business/

Independent flood directory

http://bluepages.org.uk/

Federation of Small Businesses

https://www.fsb.org.uk/resources/small-businesses-and-flooding-what-are-the-options

Flooding and small businesses

http://floodresilientbusiness.co.uk

If you are a petrol forecourt retailer, we ask you to take into consideration the following crime prevention advice. This advice has been developed in order to reduce petrol forecourt crimes, such as biking. It should be noted that, whilst the list below is not exhaustive, it is aimed primarily at helping you examine your premises and the procedures that you may have.

First and formost, you should examine the layout of your forecourt. You should look to see if you have:

- Any business practices that may encourage/invite crime (like permitting customers to pump their fuel before paying, for instance)
- A large number of fuel pumps
- Have less than two attendants on duty
- Not having a pre-pay option available during hours of heaviest losses
- Inadequate lighting
- Your store windows covered in papers and adverts
- Poor quality and/or little CCTV

You should also examine your procedures:

- Have you developed an active policy which details how you will prosecute non-payers?
- Have you developed and displayed signs which tells people you will prosecute them if they do not pay?
- Is there a management system for your petrol pumps? One that turns off outside pumps when you are quiet, for instance.
- Do you actively examine the number of drive-offs you have (including what times they happen, and how often they happen) as well as how you act on them?
- Do you examine the procedures you use in order to vet your staff? What kind of crime prevention and reduction training do they receive?
- Do you have a reward system in place for your members of staff that prevent crimes?

BOSS Forecourt watch is a crime reduction partnership developed in order to meet the requirements of police and fuel retailers who are within one police force area. It looks to ensure that law enforcement agencies such as the police as well as fuel retailers and oil companies work with each other in order to meet their crime reduction objectives while also reducing the demand places on police resources.

The watch primarily targets serious offenders and has introduced tested procedures in order to minimise retailer loss. Areas which have implemented Forecourt Watch, research shows, have seen associated crime reduce by 50%. BOSS has established upwards of 130 Forecourt Watch schemes in police forces throughout the United Kingdom. The advantages of them include:

- Providing a safer environment for both staff and customers
- Having a reduced demand on police resources
- Having an efficient and standardised system of self-reporting which helps retail service stations
- Having a proven reduction in forecourt crime incidents
- Allowing for liaison with a single police point of contact which enables streamlined reporting of biking incidents
- Heightening local awareness with the support of the BOSS marketing and public relations team
- Professional debt recovery processes which are now introduced
- Support for individual retailers from the BOSS regional coordinators
- The development of new electronic reporting technology which can help improve the accuracy and speed of reporting by proving retailers and police with a direct link to one another
- BOSS Forecourt watch is available to any police force in the United Kingdom,.

The theft of fuel is a concern to both police and rural communities. Fuel is often stolen from vehicles and storage tanks by using siphoning equipment that can differ from using basic tubes to more sophisticated tools involving pumps and the cutting of fuel lines.

Further advice on fuel theft can be found by clicking on the following links:

Stop fuel theft

/www.stop-fuel-theft.net/

Fuel theft solutions

www.fueltheftsolutions.co.uk/

Association of Convenience stores

www.acs.org.uk/sites/default/files/imported_images/2017/02/ACS-Advice-preventing-Fuel-Theft-D4-10.01.17-AW-SPREADS-LR-V2.pdf

The General Data Protection Regulation (GDPR) came into force on the 25th May 2018. If you do not know already now, please ensure that you take time to know exactly how this may affect your organisation. It must be noted that the GDPR will continue to apply to the UK after Brexit negotiations take place in order to allow for businesses across the EU to work together.

A reform of data protection law in Europe has been driven by the increasing use (and abuse) of personal sensitive information. This reform has shifted the power away from the organisations that collect, analyse and use such data to the citizens to whom the personal data belongs.

If your business handles and uses personal information, you will need to consider what action you will take in order to protect the data you have under the GDPR.

These new measures in data protection will bring benefits to citizens, as well as businesses and organisations. The measures in the GDPR will:

- Enhance the citizens' rights, and help them to have faith and confidence in the services that they use
- Combat international crime by allowing for better cross-border cooperation of law enforcement
- Remove obstacles to cross-border trade, and enable an easier expansion of businesses across Europe

The key changes outlined in the GDPR include:

- That people will have increased rights of access to their personal data, as well as portability and deletion.
- That organisations will now be held more accountable for what, why and how they process information
- That fines for breaches of such, may increase to 10-20 million Euros, or 2-4% of turnover- whichever is largest
- It will now become mandatory to report significant breaches of data to the Information Commissioner within 72 hours of being made aware of it- especially if it's likely to result in a risk to people's rights and freedoms.
- Public sector organisations must now appoint a Data Protection Officer, who will report directly to the highest level of management. This is now also applicable to organisations that monitor individuals systematically and on a large scale - as well as those which process special categories of personal data on a large scale.

What can you do to ensure your organisation to be prepared for GDPR?

In order to comply with the GDPR, you should start with making sure the basics are in place. In order to do this, use ICO's 12 steps:

https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf

You should also look at their website for more information.

You may also want to consider the 'Cyber Essentials Scheme' as well as the 10 steps to Cyber Security, both of which have been developed by the Government in order to ensure that any organisation can protect themselves against common cyber-attacks.

The ICO's Data Protection Toolkit for SMEs:

https://ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment-toolkit/

Being able to enjoy a relaxing game of golf helps create an atmosphere and Scotland's golf courses provide the perfect opportunity for business people and recreational users to enjoy a game of golf with plenty of time for talking and perhaps sealing that important businesses deal. Criminals unfortunately also see this as an opportunity.

If it is understood as 'the way that organisations or countries are managed at the highest level, and the systems for doing this', governance, at a governance level, can be considered as distributed from the highest level of the organisation, being administered via systems.

Good Governance, therefore, can be achieved in organisations by both the development and use of systems that ensure the consistency and repeatability of processes. Most prominently, it is vital that this be cascaded from the highest level of organisation.

The most simple and immediate benefits of good governance can be found below:

- Good governance can result in an efficiency of processes- due to the repeatability and con-sistency of tasks
- It can also result in the visibility of errors- the repeatability and consistency can quickly highlight any non-conformities in the process
- It can result in smoother running operations- products within your process, when 'fire-fighting' is eliminated, will follow either a 'conforming' or 'nonconforming' route
- It can also result in the conforming of products in the market- it can ensure that when your product reaches the market, it meets the intended specification and works correctly

However, good governance can also have a much wider, positive impact on businesses. Examples include:

- Culture: consistent good governance can create a culture of excellence. The leadership's behaviour will define the behaviour of the workforce. It is a lot easier in such circumstances for individuals to fit in with this culture, and those who do not fit in will be easy to spot
- Reputation: good governance will produce good products. This will result in a good business performance. The reputation of your company can make it or break it.
- Financial Stability: having good governance will reduce the threat of safety, legal, performance and warranty concerns, all of which have the ability to severely impact your organisation, as well as any stakeholders or other parties interested in it. These individuals may include customers, staff or even whole communities.

The disadvantages of poor governance can be considered as the inverse of all the points made above (as well as more). A simple google search will provide examples of large organisations with deep rooted poor governance issues.

Often, there is a very apparent disconnect between the operating functions of the organisations and its leaders. Often, to the extent that the level and impact that the poor governance is not appreciated until it is too late, and a serious event occurs. Organisations can take years to recover from the se-vere impacts of these sorts of events and can often be left facing severe legal and financial redress.

The growing focus on good governance has extended to the public and is often connected to the ethics of the organisations. Customers are now increasingly invested and connected to the ethical stances held by the organisations they choose to purchase from. This, combined with the increased legislation and penalties for poor business performance, has meant that organisations now have to ensure that they seek to govern properly, and acknowledge all stakeholders and interested parties.

The benefits that good governance hold should be attractive to your organisation, especially as it is linked to business sustainability and profitability. It can also build a positive reputation and healthy culture.

What is hate crime?

Hate crime is any criminal offence which is perceived, by the victim or any other person, to be motivated by hostility or prejudice based on a personal characteristic.

A hate crime could happen to a person because of:

- Race/ethnic origin
- Religion
- Gender identity
- Sexual orientation
- Disability

It can come in many forms such as;

- Name calling
- Harassment
- Discrimination
- Being ignored
- Being made fun of
- Verbal or physical attack
- Having your things stolen or damaged
- Being bullied

Challenging and reducing hate crime

Hate crime can inflict a greater psychological distress on the victim than a non-bias crime and victims can suffer severe post-traumatic stress symptoms such as depression, anxiety and anger.

Violence and harassment take place as part of hate crimes, often over sustained and prolonged periods of time with long term physical and psychological effects on victims, children and families. For many this abuse may be verbal abuse received on a daily basis, intervention is required at this level before abuse escalates.

Further advice and guidance can be found at the following websites:

Advisory, Conciliation and Arbitration Service:

www.acas.org.uk/index.aspx?articleid=5771

Police Scotland:

www.scotland.police.uk/keep-safe/advice-for-victims-of-crime/hate-crime/what-is-hate-crime/

Third party reporting:

www.scotland.police.uk/contact-us/hate-crime-and-third-party-reporting/

Scottish Centre for Healthy Working Lives:

www.healthyworkinglives.scot/workplace-guidance/fair-treatment/equality-and-diversity/Pages/legal-duties.aspx

xxxii

HEALTH AND SAFETY

If you think health and safety has to be complicated - it doesn't.

Below you will find some useful information for employers and those who want some basic advice on what they must do to make sure their businesses comply with health and safety law.

Managing health and safety doesn't have to be complicated, costly or time-consuming. In fact it's easier than you think. If you have taken reasonable steps to prevent accidents or harm to your employees (and the injury or illness was caused after 1 October 2013), you shouldn't have to pay compensation.

For many businesses, all that's required is a basic series of practical tasks that protect people from harm and at the same time protect the future success and growth of your business.

For more information on Health and Safety, please visit the following websites:

Health and Safety Executive

www.hse.gov.uk/business/index.htm

Scottish Centre for Healthy Working Lives

www.healthyworkinglives.scot/workplace-guidance/health-risks/Pages/health-risks.aspx

www.healthyworkinglives.scot/workplace-guidance/managing-health-and-safety/Pages/managing-health-and-safety.aspx

Health Sector

If you work or operate within the health sector and looking for security and protective advice please visit the Police Scotland website:

https://www.scotland.police.uk/assets/pdf/keep_safe/234532/health-sector

xxxiii

HERITAGE CRIME

Any offence which harms the value of heritage assets and their settings is considered a heritage crime. Should it cause damage to assets and areas that are of particular historical interest, the offence itself covers a wide range of activities which include:

- Theft of an Architectural nature
- Refusal of planning enforcement as well as undertaking unauthorised development and excavation
- Anti-social behaviour including public urination and causing criminal damage (like Graffiti)
- Having an unauthorised fire as well as fire-raising
- Undertaking unauthorised mental detecting and partaking in metal theft
- Fly Posting and Advertising
- Damage to vehicles

In the vast majority of cases, most assets are damaged by individuals who are not aware of the impact that their behaviour and/or actions are having (usually in the cases of fly posting and public urination).

As heritage assets are extremely valuable, putting right damage to them is costly to the tax payer. The recent rise in metal theft from ancient monuments, for instance, is costing the public purse hundreds of thousands pounds.

Tack and saddles are vulnerable in a single horse farm but even more so in livery stables where numerous people come and go and you often see valuable items lying in the open.

The best form of defence is to remove it, if you can take it home, if not consider the following methods advised by the NFU:

www.nfumutual.co.uk/news-and-stories/tack-and-trailer-security/

Tidy tack rooms also provide the following advice

https://tidytackrooms.co.uk/tack-room-security/

The Centre for the Protection of the National Infrastructure defines hostile reconnaissance as "Purposeful observation with the intention of collecting information to inform the planning of a hostile act against a specific target."

How to recognise and mitigate against this threat is provided in the CPNI website:

www.cpni.gov.uk/disrupting-hostile-reconnaissance

If you work, manage own or operate a hotel or restaurant and need security advice, please visit the following Government website:

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/374923/Hotels_Restaurants_Reviewed.pdf

In addition to providing security information, the link also aims to provide advice on how those in hotels can reduce the risk of terrorist attacks and limits the damage an attack might cause.

By its very nature, attempting to begin a discussion about human trafficking can be both complex emotive.

As it is broadly understood, human trafficking is a form of modern-day slavery, whereby individual from where they live through different means, such as force as well as fraud and coercion. Individ usually taken for:

- Sexual exploitation: to work in prostitution and other areas of the sex industry
- Domestic servitude: where individuals are forced to work as nannies and servants in private hom are often treated poorly, and have extremely long working hours
- Forced labour: people are sometimes forced to work in construction, nail bards, and hotels and
- Forced criminal activities: individuals are also noted to be forced to work in areas such as cannab and in industries where they sell pirate DVDs

You can find advice about human trafficking from the following charities and agencies:

www.nationalcrimeagency.gov.uk

www.migranthelpuk.org

www.gla.gov.uk

www.slavefreealliance.org

The way in which you manage your businesses HR can make or break it. Many areas, such as:

- Hiring an employee
- Trying to help and support employees in the processes of grief
- Trying to undertake disciplinary procedures
- Trying to manage the poor performance of your employees, and trying to dismiss them
- Changing the terms of employment
- Trying to deal with pregnancy and maternity related discrimination and
- Providing references for former employees

Can be difficult to deal with. The links below provide free templates which you can adapt to your business. They range from hiring employees, to helping employees deal with grievances and managing poor performance. The links are available here:

Fairways Recuritment who are an SBRC member

https://fairways-uk.com/resources/employer-resources/

Advisory, Conciliation and Arbitration Service website

www.acas.org.uk/index.aspx?articleid=5636

xxxiv

IMMOBILISE PROPERTY REGISTER

Immobilise is the world's largest free-of-charge register of possession ownership details. Together with its sister sites (the Police's NMPR and CheckMEND), it forms an extremely effective tool which helps reduce crime and help reunite recovered personal property within their rightful owners. Immobilise can be used by members of the public as well as business owners in order to register all their valued and cherished possession as well as company assets. What is exclusive to Immobilise is that when you register your items and ownerships with details, they are viewable to the Police na-tional property database (the NMPR).

As a direct result of immobilise, there are hundreds of cases a week where property is reunited with its rightful owners, or information is collected that assists the Police in investigating offences which involve stolen goods. The online checking service is checked thousands of times each day by the UK police forces in order to trace owners of lost property and reunite them with their possessions. In fact, immobilise is the only ownership registration service that is supported by all the UK Police forces, as well as the Greater London Authority and the Mobile Phone Industry.

You can find more information on the Immobilise website:

www.immobilise.com

xxxv

INFORMATION SHARING

An information sharing protocol/agreement refers to a framework that details the secure and confidential obtaining, retaining, recording, storing and distribution of information between different partner agencies and participating organisations. The framework is an agreed set of principles about the sharing of personal and/or confidential information, and it allows each participating organisation which signs up to understand the legal powers and circumstances in which it needs to and should share information, and what its responsibilities are given the fact they have the information.

It should be noted that if your organisation is involved in providing services to the public, then you have a legal responsibility to ensure that the use of personal information you have is lawful, as well as securely controlled and adheres to the rights of individuals.

The sharing of information about individuals between public authorities is often a vital part off keeping individual safe, and in order to ensure that they can get the best services possible. However, you should only share this information when it is legal to do so, and necessary to do so. Further, you should only share information if you have adequate safeguards in place to ensure the security of the information

Insider threat refers to those persons who 'exploits, or has the intention to exploit, their legitimate access to an organisation's assets for unauthorised purposes' (CPNI, 2009).

Generally speaking, there are three different types of an insider. These include a:

- Deliberate Insider: those who obtain employment for the purpose of deliberately abusing the access they are given
- Volunteer/Self-initiated Insider: Those who obtain employment without deliberately intending to abuse their access, but, at some point, personally decide to do so. This can also refer to a careless member of staff
- Exploited/Recruited Insider: Those who obtain employment without deliberately intending to abuse their access but do so at some point due to being exploited or recruited by a third party to do so

The SBRC has created an awareness presentation for businesses, and they hope that these will be able to provide you with a better awareness of the ways in which you can protect yourself from aspects of insider threat.

Further advice and guidance can be found here on the following websites:

Police Scotland

https://www.scotland.police.uk/assets/pdf/keep_safe/234532/employee-and-insider-threats

National Business Crime Centre

https://nbcc.police.uk/guidance/insider-threat-identity-verification

CPNI website

https://www.cpni.gov.uk/reducing-insider-risk

Public Liability Insurance

If you have a business that involves dealing with people face-to-face, and a customer or member of the public who is in your premises has an accident and becomes injured, then public liability insurance can help you shield your business against any claims, compensations payments and legal costs that may arise as a result. The insurance also covers you and your employees if any damage is caused to your customers property, either on your premises or not. You have the option to choose public liability insurance as a standalone policy, or you can choose to bundle it together with an employer's liability insurance policy in order to give you an extra layer of protection.

See Fake Goods

Intellectual Property or IP, are the original concepts and ideas developed and created by you and by your employees, or workers and advisors contracted to you, that become corporate assets. This includes but is not limited to:

- inventions
- work processes
- articles, blog posts, case studies
- Books
- newsletters
- illustrations
- photos
- music
- logos
- product and business names
- slogans
- movies
- Games

They are things or ideas that you or your employees have created that support your business.

Since IP has a value, and it belongs to you, you need to protect it.

The four major types are:

Copyright. Books, software, architectural drawings, articles, blog posts, graphic designs, and movies are all covered by copyright.

Trademark. This protection is given to original words or combinations of words, symbols, and de-signs that you or your employees create relative to your business. The symbol TM at the end of a word indicates that this is trademarked, and ® means that the trademark has been registered.

Patent. Patent protection is given to product or process inventions, giving the creator exclusive control over how their idea is used. There are three types of patents: utility (for a process or machine), design (original graphical representations), and plant (as in flora and fauna).

Trade secret. Trade secret protection is given to special formulas, programs, or techniques you develop that are crucial to your business.

For more information please see the links below:

Government websites:

www.gov.uk/intellectual-property-an-overview

www.gov.uk/topic/intellectual-property

https://www.gov.uk/government/organisations/intellectual-property-office

European Union Intellectual Property Office:

https://euipo.europa.eu/ohimportal/en

Federation of Small Businesses:

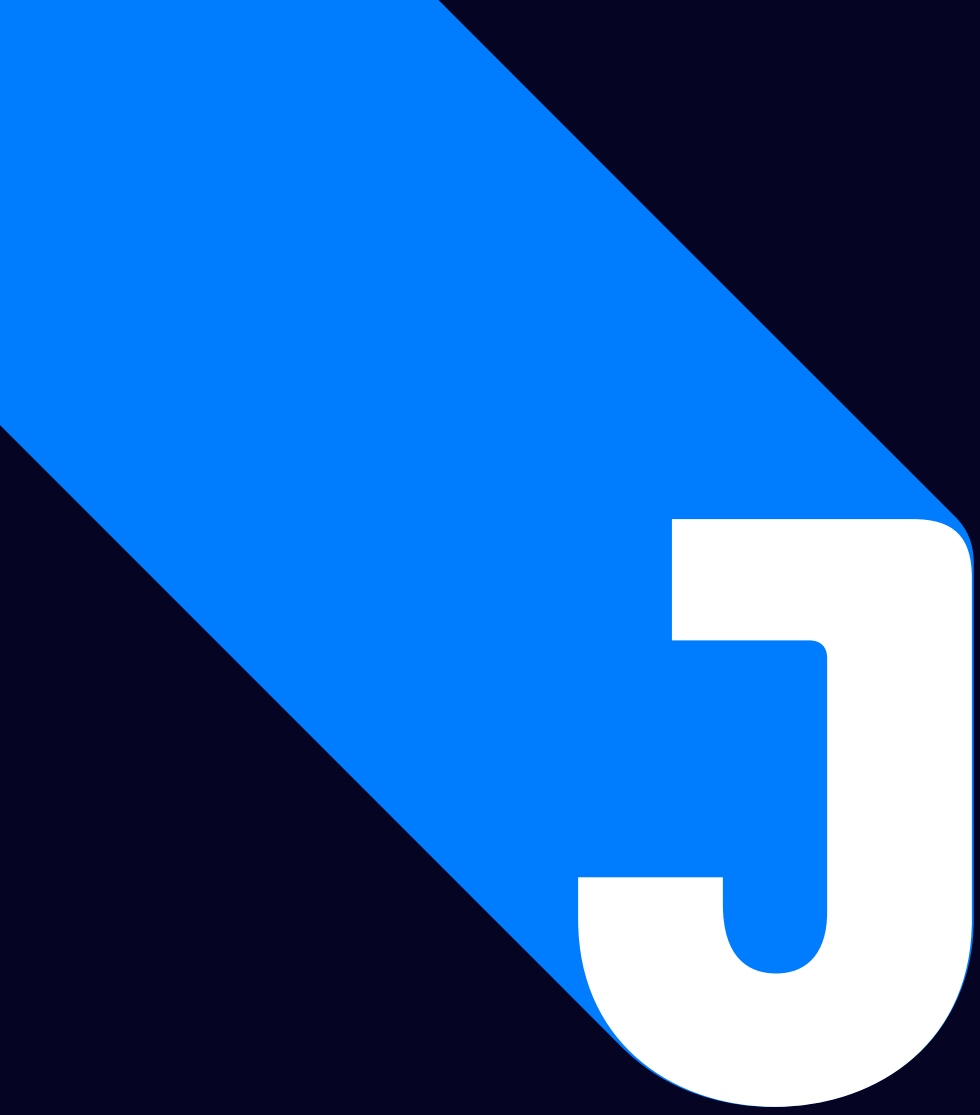
https://www.fsb.org.uk/resources/everything-you-need-to-know-about-intellectual-property

SBRC member – Snapdragon:

https://snapdragon-ip.com

Intellectual Property Management Services

www.ipms.uk.com



Originally starting as a two-year programme between 2012 and 2013, the Joint Emergency Services Interoperability Principles (or JESIP for short) attempted to improve the ways in which emergency services such as the Ambulance and Police work together when responding to major indecents which required multiple agencies.

JESIP produced some vital information and guidance on how individuals can improve multi-agency responses to major incidents. They published this report which sets out a standard which should be adopted to multi-agency working, as well as provides training and awareness items that can be used for organisations to help and train their staff.

Although the initial focus of JESIP was for mutli-agency responses to major incidents, the standard set out is scalable. The five joint working principles and models within JESIP's approach can be ap-plied to any type of multi-agency incident. It can even be used in environments where businesses and organisations need to work together more effectively.

You can find more information on JESIP here:

www.jesip.org.uk/home

Having a partnership refers to having an arrangement between two or more organisations, groups or individuals that work together in order to achieve a common aim. The term is used widely nowadays and is sometimes even used to refer to situations where one powerful organisation consults with one another, or where they are simply buying goods from one another. You should note that these are not really partnerships in their true sense. If they were, then every single time your team was approached for information or advice, or someone ordered a product or service from your team, then you would technically be working in a partnership.

What distinguishes the above interactions from a true partnership? Well, partnerships often have the following characteristics:

- All parties which form the partnership have some form of personal stake within it
- All the parties are working towards a common aim, and share a similar ethos or system of beliefs
- The parties in the partnership work together over a reasonable period of time
- The parties within the partnership agree that the partnership is necessary
- All parties understand what each party can contribute to the partnership
- There are levels of trust and respect between all the parties in the partnership

A partnership can be undertaken successfully than individual endeavours when it is ensured that no one group/organisation or individual is left with the responsibility of doing everything; especially when it lies outwith their perception, knowledge, skills and other forms of resources. Having the ability to access a wide range of ideas as well as being able to share the financial burdens of trying to achieve a desired aim also means that organisations, groups and individuals may be able to confi-dently tackle the issues that they might otherwise steer clear of.

Partnerships are also noted to be successful as they:

- Allow parties to share the risk, responsibilities, resources and creativities that they have
- Allow parties to feed of one another's energy and enthusiasm
- Are able to attract funding from a number of different sources
- Afford the ability to highlight different issues, problems and solutions
- They provide more potential for efficiency as well as productivity. Within this, they also of-fer support and diversity

Nonetheless, for partnerships to be able to provide such value, you must put in a large amount of planning, as well as have a large degree of flexibility, commitment and energy for all the parties that are involved. Having planning in place, for instance, will ensure that a successful partnership will have a backup plan that comes into place in the event that one (or multiple) cannot attend a meeting or event. This could mean having a plan that allows an organisation to be filled in at a later date, or taping the event or meeting in order to send them it to fill them in. You could also have delegated decision-making arrangements.

All parties within the partnership structure should be tolerant and flexible enough to understand the times when other parties may not be able to attend a meeting, but also rigorous enough to ensure they can identify those groups who are not 100% committed to making the partnership to work.

For more information:

https://www.scotlandstowns.org/

Business Crime Reduction Partnership (BCRP)

A BCRP is a business-led, not-for-profit subscription-based making action group which works with the police as well as local authorities in order to tackle and subsequently reduce the criminal activities and other forms of deviant disorders which are affecting businesses. The aim within the BCRP is to create a safer environment for businesses in the UK's retail community; including both small to medium sized enterprises and large department stores. If you would like more information on the BCRP, click here.

Scottish Improvement District (SID)

A Scottish improvement district is a funded business body formed in order to represent and improved defined commercial areas. They are noted to be powerful tools for directly involving local businesses in local activities and making the space for the business community and local authorities to work together in order to improve the local trading environment. If you are a business owner, having a SID means that you will be able to be plugged into a cohesive organisation which, at its heart, looks after you interests. They will keep you informed of local initiatives that are designed in order to create a safer environment for your business and will keep you involved in them too.

Pubwatch

Pubwatch consists of a voluntary scheme which afford licensees the ability to work together in order to reduce anti-social behaviour which is associated with alcohol and substance misuse. It also helps improve the safety of the premises for customers within businesses, the staff which work within them, and the community in which the premises is located.

Secured Environments

Secured Environments refers to a police certification scheme which awarded to organisations once they are able to show that they have adopted the six principles that are key for protecting themselves from crime. More information can be found here.

National Association of Business Crime Partnerships

In the UK, there are well over 250 business crime reduction partnerships currently operating- and these range in size from limited schemes which operate in smaller cities to bigger city-wide operations which employ several staff and have a plentiful number of members. These partnerships work closely with police forces and councils to make sure that their local communities are a safe place to live and work in as well as visit. Furthermore, and as funding for statutory services is getting increasingly tighter, business crime partnerships are gaining more and more influence and more and more importance.

Business Crime Reduction Partnerships in the UK

The National Association for Business Crime Partnerships, also known under the acronym NABCP, is a membership body which represents all business crime reduction partnerships at a national level. Its work seeks to promote the concept of BCRPs to national and local governments as well as to increase the collective effectiveness of the some 250 partnerships across the UK by lobbying for greater and better resources and influence.

The NABCP also acts as a repository of information which offers its members a range of resources on things such as recent legislation and accreditations as well as news about different innovative ideas which are being employed by its members. You can find more information on the NABCP by clicking here.

For a variety of ways to keep safe during the day and night please click on the below links to learn more:

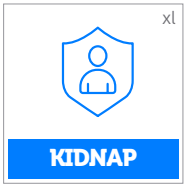
Police Scotland websites:

http://www.scotland.police.uk/keep-safe/

https://www.scotland.police.uk/keep-safe/personal-safety/

Crimestoppers:

https://crimestoppers-uk.org/keeping-safe



Depending on your personal and or professional circumstances, you and your family may be at a higher risk of being affected by a serious crime such as kidnapping, as well as hostage taking and/or extortion. Previous experiences have highlighted that when such crimes occur, they are often well thought out by the attacker. They may for instance take advantage of their victims established routine and habits in order to formulate their plan. Understanding that this may be one possible way that potential attackers may think out their plan should help you identify any 'weak' spots in your routine and take the necessary steps in order to reduce your risk of becoming a victim of these crimes. This idea is also applicable to other crimes, such as robberies.

The below brochure aims to highlights ways in which you can minimise potential and foreseeable risks; suggesting how you can do these in order to be as safe as is possible. You should consider using it for both personal use and in accordance with your countries national and company laws, as well as your business policies and procedures. It may reinforce what you already know and may also make you consider some new ideas. It provides information and recommendations for how to react to critical situations like kidnapping.

For more information:

CPNI website:

www.cpni.gov.uk/optimising-people-security

National Crime Agency website:

https://nationalcrimeagency.gov.uk/what-we-do/crime-threats/kidnap-and-extortion

If you want to carry out 'licensable activities'- which include:

- Selling alcohol
- Serving alcohol (even if no one is paying for it)
- Serving any hot food and drinks between 11pm-5am
- Providing different forms of entertainment- such as live music, film and a dance performance

from any particular venue, you should contact your local council in order to apply for a premises license.

You will still require a license even if your activities are for charity (although, in this case, you may not need to pay for it).

Restrictions

You have to be 18 or over in order to apply for a premises license

Conditions

You must either be the designation premises supervisor (DPS) or have one appointed in order to apply for a licence. A DPS can hold a personal licence to sell alcohol. If you have any gaming machines on your premises, you may also have to register to pay machine game duty.

In addition to the above, it is also possible that there may be other conditions added to your licence, such as an age-checking policy.

Length of licence

Many of the available premises' licenses have an unlimited duration- but require you to pay an annual fee.

How to apply

Contact the council local to where your premises are based.

You must ensure your application for the premises includes:

- Your details (including any criminal convictions you may have)
- The details of your designated premises supervisor (as outlined above)
- A detailed plan of the premises you are applying for
- Your planning certificate, your buildings standards certificate, and, if you are applying for food to be sold, a food hygiene certificate

You will also need to include your 'operating plan'. This plan includes the details of:

- The activities that you are planning to hold on your premises
- The times during which alcohol will be sold
- The times during which food will be sold and
- The capacity of your premises

From this, you will be charged a fee which is based on the rateable value of your premises.

Extending your licence conditions

If you wish to extend your licence conditions and, sell alcohol outside of your licensed hours, for instance, you must apply to your council in order to extend the hours of your licence.

Displaying your licence

You are required to display your 'licence summary' at your premises and do it in a place where it can be easily seen. The other pages of your license must also be kept on the premises in a safe place. Police and council officers have the right to ask to see them at any time.

Fines and Penalties

Should you carry out a licensable activity at your premises without a license, you can be fined £20,000, sent to prison for 6 months, or even both.

You can also be fined £1000 for failing to produce your licence when asked to (usually by a police or council officer).

Best Bar None

Best Bar None is a national accreditation and award scheme for licensed premises. Participants are given lots of support and advice to improve the safety of their staff, premises and customers and to adopt high management standards.

More information:

www.bbnscotland.co.uk

For more advice and guidance on protective security for bars, pubs and clubs visit the Police Scot-land website:

www.scotland.police.uk/assets/pdf/keep_safe/234532/bars-pubs-and-clubs

Generally speaking, lone-working refers to an employee undertaking work-related duties when they are not in the presence of, or easily accessible to, other employees. If your employee is a lone-working, you, as their employer, have a responsibility as outlined within the Health and Safety at Work Act (1974) to provide 'a safe and secure environment for every member of staff'.

Your employees should have the skills and adequate training in order to carry out their job in a satisfactory manner. These skills should include knowing how to ensure their safety whilst they are carrying out their roles. Your employees should also be made of the procedures and protocols your business has which outline what should happen if things go wrong. Although you should ensure that your employees know this, the responsibility is theirs to follow them.

Encourage them to think about:

- What working alone means to them
- In what circumstances they find themselves working alone
- How often they work alone
- If working alone gives them any concern
- What risk they believe their job poses to them
- How they evaluate these risks and
- How they minimise these risks

When thinking about their safety, ensure your employees considers the risks and balance the two.

There are numerous websites that you can visit in order to access more advice, information and assistance from when looking at employee lone working. They are as follows:

Suzy Lamplugh Trust:

www.suzylamplugh.org/

Health and Safety Executive

www.hse.gov.uk/toolbox/workers/lone.htm

National Business Crime Centre – Lone Working Guide

https://nbcc.police.uk/article/?id=6169084a3523475a580b5ff1043153ab

Protect the livestock on your farm:

Livestock theft is incredibly difficult to protect yourself against, and is becoming increasingly common. Thieves often don't use the main point of access to a field choosing to cut through barbed wire or fence instead. It is a crime that often needs a degree of organisation, as dogs are used to round up the sheep and put them on a trailer.

Whatever the type of premises you are safeguarding, security lighting is one of the most effective ways you can take in order to safeguard from unwanted visitors. Before you look to install these lights, however, you should adapt what can be considered a 'criminal mindset' and should look to identify the most vulnerable parts of your building. You should consider installing lighting in areas of easy concealment near doors and windows and should cut any bushes or trees that offer a place where individuals can hide, or, conversely obscure your vision of your property.

In order to maximise the efficiency of security lighting, it is necessary that you buy and fit a lighting system that is fit for the purpose of your premises. You should ensure that your lights are:

- Vandal resistant and located in a position which makes them inaccessible
- Operated by what is called a 'dusk to dawn', PIR or time switch control. A PIR detected movement, and can make people aware when others are present
- Positioned where the buildings are well overlooked. Placing them where their illumination is hidden may aid trespassers
- Not placed in areas with overgrown landscape
- High pressure sodium lights- which are noted to give a good quality of light and are also economical to operate.

LED lights and LED lighting are also established as a low energy and low maintenance way in which to keep your premises well lit. LED lighting is stated to be ten times more energy efficient than current incandescent lights, when running at the same light output. They do this by running at close to room temperature, which means less energy is waste on heat (both in terms of the lights themselves, and the air conditioning you may have to put on in order to counteract the heat coming from the incandescent lights). They are also more durable than other lights on the market; being re-sistance to the heat, the cold, as well as shock and vibration. On top of this, they are also noted to last tens of thousands of hours when they are used at the rated current.

You should also note that coloured surface finishes can improve the lighting levels around your premises. Speaking generally, the correct lighting scheme should be able to provide illumination to the main circulatory routes that surround your premises, any car parking areas you may have, the entrance and exits to the buildings, the perimeter of your buildings, and the recesses in the building line.

Street Lighting

All street lighting for adopted highways and adopted footpaths, as well as private commercial estate roads and footpaths and car parks should comply with BS 5489, and all light pollution should be minimised. Light pollution must be minimised as, if artificial light is not properly controlled, both psychological and ecological issues may occur.

Commercial Unit Lighting

Commercial lighting should be designed so it provides a uniform spread of light, as well as a clear colour rendition. It should also avoid deep shadows, and, like above, minimise light pollution. The Luminaries should be stable and resistant to multiple things; such as adverse weather conditions, vandalism and tampering. Ensure you take these into account when looking to buy and install com-mercial lighting.

All the security lighting that you buy should be employed in areas of your premises where surveillance is considered important, and it is for this reason that the lighting design and layout you employ should support any natural surveillance you may have and the CCTV that you have. The lights should not be restricted by trees or other landscaping features.

The cables and switchgear for the lights should be well protected, meaning they should be installed underground or in an enclosed within a steel conduit. Ensure that they are kept out of the reach of unauthorised personnel. If you deem it necessary, you can protect any cables of switch gear with a suitable alarm system.

Secured By Design:

https://www.securedbydesign.com/guidance/research-case-studies-guidance/lighting-against-crime

CPNI:

https://www.cpni.gov.uk/security-lighting


M

xxxv

MAIL ROOM SECURITY

Police Scotland provide advice in relation to security within the postal system. The postal system can be used to deliver threatening or dangerous mail, although this still remains unlikely. It allows the perpetrator to remain anonymous. If a suspect package is found, the Emergency Co-ordinator should be advised immediately, along with Security.

https://www.scotland.police.uk/keep-safe/246633/246657/

xliv

MENTAL HEALTH

Our mental health affects how we act, think and feel, and encompasses our psychological and social well-being. It is a significant factor in determining how we deal with stress, how we relate to others, and impacts the choices we make in our everyday lives.

Mental ill health can manifest itself in many ways, from common disorders such as anxiety and depression, to more complex conditions such as schizophrenia and bipolar disorder.

It is unlikely that everyone will always experience good mental health. Normally, mental health is fluid depending on your life experiences. It is normal to experience both good mental health, as well as bouts of stress and anxiety.

Put simply, those who experience good mental health work more productively. They interact well with colleagues and make a valuable contribution to the workplace environment. In fact, a recent study by the Chartered Institute of Personnel and Development highlight the effect that mental health can have on organisations. This study found that, in terms of those will mental ill health:

- 37% of individuals are more likely to get into conflict with their fellow employees
- 57% struggle with juggling multiple tasks
- 80% find it difficult to maintain focus
- 62% take more time in completing tasks
- 50% are noted to be potentially less patient with customers and clients of the business

The study also found that, stress is a major cause of long-term absences in both manual and non-manual workers.

More guidance on mental health and wellbeing in the workplace can be found at the following sites:

Advisory, Conciliation and Arbitration Service website

www.acas.org.uk/index.aspx?articleid=1900

Scottish Centre for Healthy Working Lives

www.healthyworkinglives.scot/workplace-guidance/mental-health/Pages/mental-health.aspx

Federation of Small Businesses

www.fsb.org.uk/resources/mental-health-help-for-small-businesses

xxxvii

METAL THEFT

Due to the continuing demand for all metals, which is partially driven by global economies, the overall price of metal has increased considerably.

All metal is currently desirable to thieves, however, a combination of re-sale value, demand, and quantity available means that some metals are more desirable than others. The high price of copper, for instance, has been a consistent factor in its theft.

There is no archetypal metal thief; with those responsible ranging from the opportunistic individual through to organised crime groups. The latter often have access to specialised machinery, which enables them to carry out metal theft on a larger scale.

There is also evidence to suggest that some metal theft offences are committed by, or in some way facilitated by, those employed within the relevant industries.

xlv, xlvi

MODERN SLAVERY

Modern Slavery is an international crime that affects millions of people worldwide. Many victims currently reside in the UK. Nearly all individuals that are exploited via modern slavery receive little to no pay for the work they are forced to undertake; and are often controlled by threats, physical force, abduction, fraudulent activity, deception, and coercive control.

Anyone can fall victim to modern slavery, including human trafficking, and they are usually exploited in the following ways:

- Labour exploitation
- Sexual exploitation
- Domestic servitude
- Organ harvesting
- Criminal exploitation

Often the victims are children, who can be subject to sexual exploitation, forced begging and illegal drug cultivation. Individuals are often sold to another criminal and then forced to partake in another form of exploitation.

In 2016, the UK identified that there were approximately 3805 potential victims of human trafficking, which is a 17% increase on the previous year. Of these 3805 individuals, approximately 1278 were children. Cases of modern slavery are hugely prevalent amongst those who are deemed to be vulnerable, or those who are within minority and excluded groups.

Variables such as poverty, unstable social and political conditions, and limited opportunities at home are all key factors which can heighten someone's vulnerability to becoming a victim of modern slavery. Those with addictions are also extremely vulnerable, often exploited by abusers fuelling their addictions in order to exert control over them.

Potential victims have been reported from a total of 108 different countries of origin. The top seven nationalities for potential victims of modern slavery include British, Albanian, Vietnamese, Nigerian, Chinese, Romanian and Polish.

If you are concerned about an instance of potential modern slavery, your first point of contact should be the police. Should you have information on modern slavery, such as who is responsible, or who may be at immediate risk of harm, you should dial 999 immediately. If you wish to make a call anonymously, you can call Crimestoppers on 0800 555 111.

In addition, if you have any information that could help identify, discover and recover any victims of modern slavery crimes in the UK, you can contact the Modern Slavery Hotline by calling 08000 121 700.

More information on modern slavery can be found at the following website:

www.unseenuk.org

Police Scotland:

www.scotland.police.uk/about-us/human-trafficking-and-modern-slavery

National Crime Agency:

www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/modern-slavery-and-human-trafficking

Money laundering is a global problem and can undermine the integrity and stability of your business, as well as the wider financial market.

Individuals can use a variety of methods in order to launder money. Usually these methods fall into two categories:

- **Cash-based money laundering:** This involves the physical movement of money across national borders, or individuals using companies with a high cash throughput as a cover. They will make numerous small payments, which are masked by the larger transactions, as this reduces the likelihood of individuals being caught.
- **High-end money laundering:** This is often considered 'specialist' and usually involves transactions that have a significant value. In addition, this type involves the abuse of the financial sector.

More information on money laundering is available on the National Crime Agency website here:

www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/money-laundering-and-terrorist-financing

xlviii

NATIONAL BUSINESS CRIME CENTRE

The National Business Crime Centre (NBCC) officially launched at the end of 2017. It was established as a result of the Home Office Police Transformation Funding. It is overseen by Commissioner Ian Dyson who is the NPCC lead for Business Crime.

At present, the NBCC does not offer either a proactive or investigative capability. They are, however, willing to support other partners from both police and business communities, as well as act as a conduit for sharing advice and trends nationally. They promote research into current crime trends, and support the initiation of new crime prevention projects, demanding specification for policing resources when required.

Their workstreams encompass their three main strategic strands of Partnership, Intelligence and Prevention, with their primary objectives including:

- improving partnerships within the business community and promoting best practice nationally
- raising police standards in order to improve both the understanding of crime, and to reduce the impact of crime nationally, through prioritisation of crime prevention
- enabling businesses to target resources more efficiently by sharing intelligence
- working with national intelligence partners in order to tackle travelling criminality and organised crime networks, by the effective use of intelligence to disrupt organised crime at a national level
- enabling businesses to protect themselves from cyber-crime, fraud, and terrorism, by acting as a centre of excellence to support all UK businesses
- Providing violence reductions plans for businesses and their employees
- Providing safeguarding advice, as well as links to training and promotion of best practice
- Supporting national policing teams
- Producing national standards and accreditation for Business Crime Reduction partnerships
- Providing fraud/cyber messaging to businesses on behalf of specialist units, where appropriate
- Assisting with Counter Terrorism messaging to businesses on behalf of the Cross Sector Security and Safety Communication network

More information regarding the NBCC can be found on their website at the following address:

www.nbcc.police.uk

The National Vehicle Crime Intelligence Service (NaVCIS) is a national police unit, whose purpose is to protect communities in the UK from the harmful effects of vehicular financial crime and associated criminality. They do this by coordinating both strategic and operational responses by police forces across the UK, whilst providing specialist operational analysis. They are dedicated to developing and disseminating strategic intelligence to assist with detecting offences and apprehending offenders. They also promote tactics and provide crime prevention advice to both the finance industry and the wider community.

NaVCIS works in collaboration with the National Police Chief's Council and the National Crime Agency, as well as numerous government agencies such as the DVLA. They also collaborate with key private sector organisations such as the Caravan Safety and Security Group.

The core functions of NaVCIS are:

- developing and promoting tactics and advice on crime prevention for the finance industry and wider communities
- supporting UK police forces by investigating specialist crimes such as those pertaining to plant and agricultural machinery
- providing a link with tracking companies to develop more efficient ways in which to recover stolen vehicles
- providing a specialist ports capability; incorporating recovery, enforcement, and intelligence support

In 2017, the information disseminated by NaVCIS was instrumental in assisting the vehicle finance industry in preventing fraudulent applications, valued in excess of £800,000.

More information regarding NaVCIS can be found on their website at the following address:

www.navcis.police.uk

1

NATIONAL CENTRE FOR RESILIENCE

Scotland's National Centre for Resilience (NCR) is located within the Crichton Campus in Dumfries. They work to ensure that communities across Scotland are adequately prepared to deal with any natural hazards, for example, flooding or landslides.

At its heart, the NCR aims to improve our understanding of the impact that natural hazards can have on a community. They also provide support to those who respond to such natural hazards, as well as the communities who may be affected, by providing practical tool kits and resources for those who operate at ground level.

The NCR also bolsters the working relationships between practitioners, academics and policy-makers, to develop best practice in dealing with natural disasters. It also aims to provide research capabilities to meet the needs of the resilience community.

The NCR comprises of many strategic partners including:

- The Scottish Government
- The MET Office
- The Scottish Fire and Rescue Service (SFRS)
- The Scottish Environment Protection Agency (SEPA)
- Police Scotland (PSOS)
- The Scottish Funding Council (SFC)
- The Scottish Flooding Forum
- The Edinburgh Centre for Carbon Innovation
- The University of Glasgow
- Transport Scotland
- The British Geological Survey and
- The Natural Hazards Partnership

More information regarding the NCR can be found on their website at the following address:

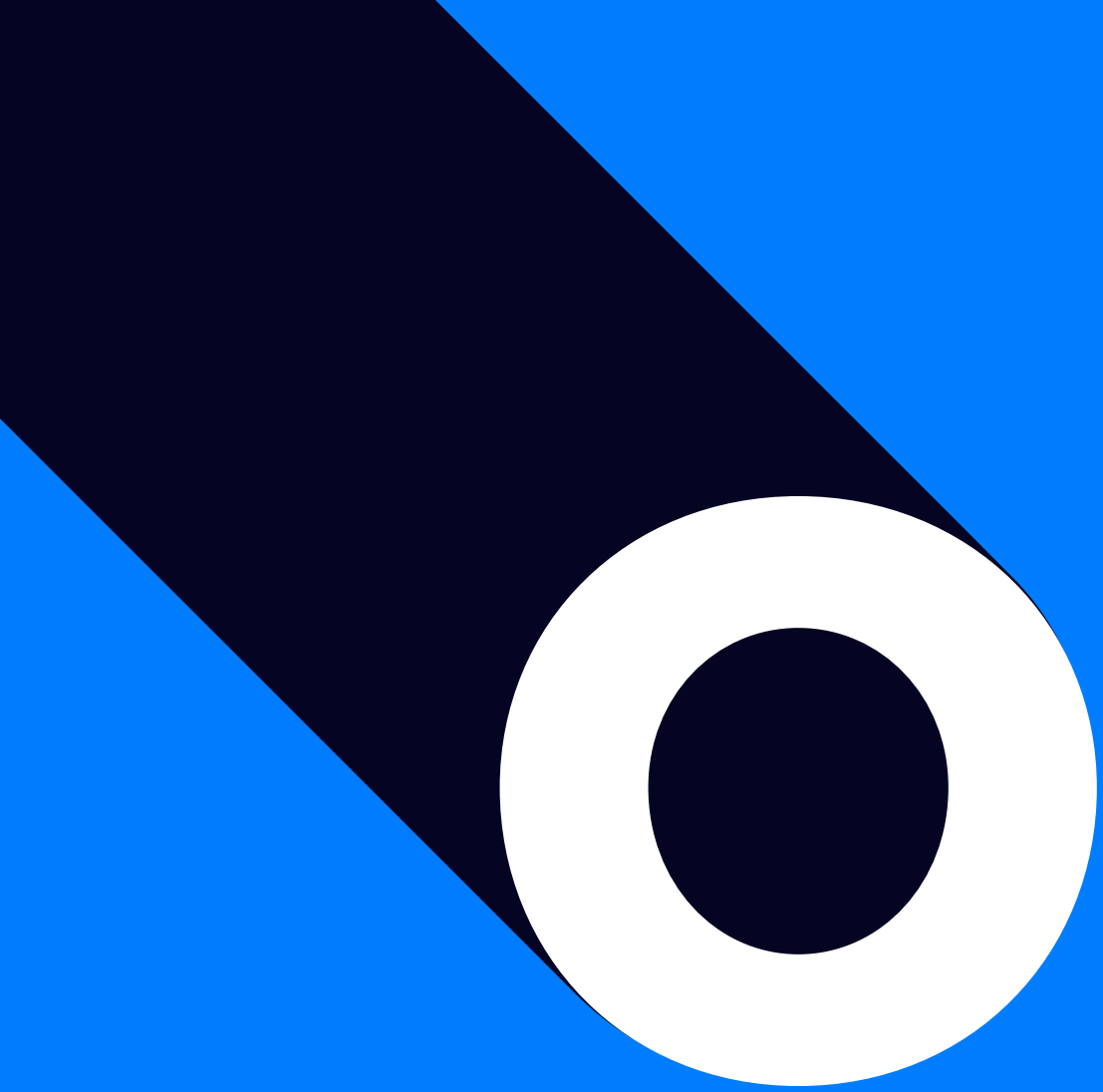
https://www.gla.ac.uk/research/az/ncr/

You can follow them on Twitter:

@ResilienceScot

and their e-mail contact details are:

nationalcentreforesilience@glasgow.ac.uk



Whether your business is large or small, you need to ensure that you take the appropriate steps to protect yourself and your staff. Although there is no single answer to reducing crime, the following SBRC Factsheet is designed to help create a safe workplace for you and your employees, and mitigate any criminal opportunities.

We should all recognise and be aware of the impact that a crime against a minister of a religion, or their place of worship, can have. This is not just in terms of them individually, but also how this can affect the whole faith community.

Places of Worship are attractive to thieves for a variety of reasons. Metal Theft, Insecure buildings and limited security provision are just some of the indicators that are attractive to the would-be thief.

Please see the SBRC factsheet to help keep your place of worship more secure and less attractive to the opportunist criminal.

Police Scotland website also offers the following advice and guidance:

https://www.scotland.police.uk/assets/pdf/keep_safe/234532/places-of-worship

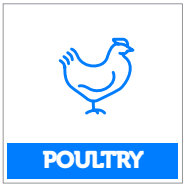
The theft of plant and machinery is a very costly problem, especially if you live in a rural environment. If you own (or hire) any form of plant or agricultural machinery, you should consider the following advice and protective measures.

Equipment register

https://www.equipmentregister.co.uk/

Equipment & Registration Scheme to the Construction & Agricultural Industry

https://www.cesarscheme.org/



The theft of poultry can have a devastating effect on the business owner and often increases at certain times of the year. There is also the welfare of the animal to consider too.

If you work or operate within the Private Hire and Taxi sector you will undoubtedly deal with strangers on a daily basis. This means working in often isolated places and carrying cash. You will come into contact with people who have been socialising and maybe under the influence of alcohol or other substances.

The following advice from the Police Scotland website is designed to help keep yourself safe when at work:

https://www.scotland.police.uk/keep-safe/246633/private-hire-taxi-safety-advice

A majority of the decisions undertaken by departments have what is understood as a procurement implication. These procurement implications have the ability to impact what the overall cost of carrying out a decision is. In this scenario, cost is used to refer to the total cost of the service or good. Not just the price that is paid.

Within the private sector, procurement is primarily understood as a tactical function which works to help improve a business's/organisations profitability. In its most general sense, procurement can help to streamline business processes as well as reduce materials and costs needed. In doing this it can identify better sources of supply for your business. In many businesses and organisations, procurement is emphasised and recognised by having a 'head of procurement' at Executive Board Level.

However, within the public centre, the use of procurement is harder to define. In the public sector, there are no publicly declared profits or losses, and no shareholder's dividends to be cashed out. However, there remains a need to maximise both in terms of teaching and research within the funds available. Most commonly, this money comes from public funding, usually in the form of grants or student fees. In essence, the sector's shareholders are taxpayers, staff or students. As such, there is an essential requirement on public sectors to ensure that the funds that are provided by the 'sectors shareholders' are managed in a responsible manner and to ensure that the ways in which they funds are managed demonstrate value for money as well as probity.

If you have a higher level of expenditure, the need for transparency and non-discriminatory action is no longer an act of good-will but is a legislative requirement. The European Procurement legislation, which is implemented within the UK, states that all requirements for supply and/or services (above £172,000 approximately) and works (above £4.3 million approximately) are appropriately advertised and tendered in line to the published rules.

Within an institution, an expenditure is often made up of two distinct elements:

- Pay (salaries and wages) and
- Non-pay (all other expenditure)

Procurement is concerned with the management of a large proportion of non-pay expenditure, which includes the everyday costs of your business. It also ensures that the best possible value for money can be achieved in terms of committing this expenditure. This expenditure can be further divided into categories. One relating to pay used in order to obtain goods and services from others, and the other including payments made to educational establishments and other establishments such as HMRC. Within this, the procurement function is concerned with obtaining the goods and services you require from appropriate suppliers which, consequently, enable the institution to meet its objectives in a well meaning manner. It has been estimated that, within institutions, non-pay expenditure usually accounts for 30-40% of its entire expenditure.

The following link contains overviews to various models and toolkits which can be used by the sector:

- **Efficiency Measurement Model (EMM).** This has been designed to help provide a structured process within which you can record efficiencies achieved by your own procurement projects
- **Legislation.** This has been developed to help specify in the legislation that public sector institutions must monitor how they are spending their funds.

- Integrated Benchmarking Information Systems (IBIS). This model has been developed in order to help with the strategic management of different institution's procurement activity. It does so by analysing historical expenditure in order to provide a helpful framework which can help inform future activity. This model considers the different levels of professional pro-curement involvement, as well as the types of procurement arrangements you already have in place. This is in terms of how you secure value for money, and how you review the quali-ty of your institution's suppliers.
- Key Performance Indicators (KPI). This details performance measures which are sector-wide and under development, many of which have been generated for collected data and analysed using other models. It contains an overview of simple transactional measurements that have been developed in order to help you review the procurement activity of your institution
- Whole Life Costing (WLC). This is a model which has been designed for use when prepar-ing the tendering processes (usually to a developed awarded criteria) and later to present a framework for the methodical evaluation of the tender submissions. This evaluation will include the consideration of the total costs of operating and owning, as well as the end of life costs which are associated with the project.

Scotland Excel:

http://www.scotland-excel.org.uk/

Immobilise is the world's largest register of ownership details for property. In collaboration with the police-operated website NMPR (National Mobile Property Register, available at **www.thenmpr.com**) as well as CheckMEND (available at **www.checkmend.com**), immobilise.com assists the police with detecting crime and allowing stolen (and subsequently recovered) personal property to be returned to its rightful owner.

Immobilise.com can be used by members of the public, as well as businesses, in order to register their valuable possessions and/or company assets. All account holders who have registered their items and ownerships details on immobilise.com will then be available and viewable on the NMPR website.

This online checking service is utilised by all UK police forces in order to return stolen and lost property. It is also checked by a wide range of recovery agencies and lost property offices across the UK. Immobilise.com is the only ownership registration site that is supported by all UK police forces, including those in the Greater London Authority.

Similar to the Green Flag Award for parks and the Blue Flag Award for beaches, the Purple Flag Award is an accreditation process. Towns and city centres that meet and/or surpass the standards of excellence outlined for managing the evening and night time economy (ENTE) are awarded Purple Flag status. Your town or city centre will only achieve a Purple Flag status if it is safe, vibrant, well-managed and offers a positive experience to its customers.

There are a comprehensive set of standards, as well as management processes and good practice ex-amples, that are designed to help transform a town or city's ENTE. These are available alongside a research, development and training programme. In other words, Purple Flag is a positive initiative that allows towns and cities to indicate that they provide an entertaining, safe and diverse ENTE. It is available throughout the UK and Ireland and is now even being implemented internationally. In the UK, Purple Flag is the only scheme available which focuses on both the negative aspects that must be addressed, as well as the potential for economic growth and community enhancement.

Should you become a Purple Flag stakeholder, you will experience the following benefits:

- A strong partnership with good working relationships between all involved in the ENTE
- An improved public image and a better raised profile
- Wider patronage
- Increased expenditure and footfall
- Lower levels of crime and other forms of anti-social behaviour
- A more successful mixed-use economy
- A stronger diversification (which will help entice a wide and varied consumer offering)
- Regeneration and development of the area
- Helping foster positive perceptions

If you would like more information on the Purple Flag Award, it can be found on the National Business Crime Centre website at:

https://nbcc.police.uk/guidance/purple-flag-scheme


Q

liv

QUALITY ASSURANCE

Quality assurance is considered a means of preventing mistakes and identifying defects in any manufactured products within your business. It is also a way of avoiding problems when you deliver products or services to your customers. Most generally, quality assurance encompasses two principles:

- 'Fit for Purpose' whereby the product must be considered suitable for its intended purpose and
- 'Right first time' whereby mistakes should be eliminated

The terms quality assurance and quality control are sometimes used interchangeably. Both refer to the ways in which businesses can ensure the quality of a service or product. Quality assurance, in this context, is often used to describe the 'implementation of inspection and structured testing as a measure of quality' . The term control, conversely, is often used to describe the fifth phase of the DMAIC model which is used as a data-driven quality strategy to improve processes.

Quality assurance comprises of both administrative and procedural activities that are implemented in a quality system. This is done in order to ensure that requirements and goals for a service, activity or product will be satisfied. According to the Marketing Accountability Standards Board, quality assur-ance refers to the systematic measurement, comparison with standard, monitoring processes and associated feedback loop with confers with error prevention.

Quality assurance, therefore, includes the management of the quality of the raw materials you use; your assemblies; your products and components; the services related to the production of your goods; as well as its management, production and inspection processes.

More information can be found here:

www.iso.org/iso-9001-quality-management.html

QR CODES

In this context, 'QR' stands for 'Quick Response' or 'Quick Read' and describes the square barcodes full of digital dots that are very common today. They are intended to save you time by taking you directly to a website, without the need to note down the web address or input it manually into a search engine. If you own a smartphone, it is likely that you are already using QR codes by using your built-in phone camera to scan the QR code to find out more information on any given product.

QR codes are easy and convenient to use and can be found everywhere; from magazines to tourist monuments. This prevalence has led to criminals seizing the opportunity to hijack QR codes; with the intention of either tricking victims into downloading malware onto their devices, or in order to phish for confidential information. This is achieved by diverting individuals away from genuine websites to doctored ones. They may look like the real thing, but they will contain phishing software designed to capture personal information, most likely to be used for identity theft. Alternatively, they may download malware onto your mobile device to steal personal information, or upload spam advertising on your device.

According to a report developed by tech site The Register, it is common for criminals to simply place their QR stickers over the legitimate one. In this way, there is virtually no way in which to tell if the QR code is genuine or not. When placed on billboards and other popular public places such as train stations, normal QR codes will be placed in easy to see and easy to reach areas. This provides an ideal opportunity for criminals to place their own hacked stickers over them.

In fact, it has been reported in Europe that criminals have been placing stickers randomly on public walls and buildings, knowing that a curious passer-by will likely scan one. In theory, hacked QR codes could be placed anywhere - even in hospital waiting rooms – however there are no known instances of this occurring within the UK.

Generating a QR code is a relatively simple thing to do, and you do not need any sophisticated equipment. An internet search will show current websites where you can insert a website address and generate either a genuine or fraudulent QR code image in seconds.

5 ways you can protect yourself:

- You should never scan a QR code that doesn't appear to be linked to anything else, or that has no accompanying text to explain what the code will do. Do not scan a code that just seems to be stuck randomly on a wall or floor.
- Always be wary about scanning QR codes on posters in public places like a train station, even when information is presented to accompany the code.
- If you do decide to scan a QR code in a public place, ensure that what you're scanning is not a sticker. A quick finger check will tell you - if it's a sticker, do not scan it.
- Always use a QR code scanner app that will check the website before launching it on your phone. As stated earlier, smartphones are vulnerable to malware and are frequently targeted. These apps are readily available - just search 'secure QR reader app' in your device's app store. One of the most common apps and best-known for android handsets is 'Snap'. 'QR pal' is another app and is available for all popular operating systems. Since we have not tested any others, we cannot make recommendations.
- If you scan a QR code and it directs you to a website requesting submission of confidential information such as passwords, do not enter any information, even if it appears to be a genuine website. You can always check the website at a later date.

If you do come across what appears to be a fake QR code attached to a product or building, consider warning the owner of the site so that others do not fall victim to the scam.

READY SCOTLAND

Although there will be challenges to managing a business on a daily basis, there is always the risk of a more serious disruption to your business as a result of an emergency situation, whether man-made or occurring naturally. Even relatively small disruptions to a business can have serious consequences in terms of cash flow and customer commitments.

Ready Scotland provides more information on the handling of serious disruptions, which can be found by visiting the link below:

https://www.readyscotland.org/my-business/

lvi

RECOVERY STRATEGIES

In order for your small business to survive, you need to have a business recovery strategy. Having a business recovery strategy means you can ensure that, following a disaster such as flood, your business can return to its essential operations quickly. If your business fails to recover from a disaster quickly and well, then the consequences can be extremely damaging.

Developing and having a recovery strategy can help your business maintain continuity from the very earliest point after disaster occurs. The recovery strategy you have should always focus on prioritising and identifying what resources you believe to be critical to the function of your business. This may include things such as your IT systems. In using your business strategy to identify potential threats and/or risks that your business faces, you can develop a course of action which you can use in order to recover from different scenarios.

The business recovery strategy you develop should include plans which enable key employees to resume their work with the appropriate facilities that they need. A list of facilities that key employees require, in addition to alternative resources such as laptops and mobile phones which could be rented, should be included within the recovery strategy. If company data is stored on a company website, it should be backed up with a provider who is external to the business sever so that essen-tial data can be accessed during an emergency.

Threats to your businesses continuity can range from natural disasters, and failures of IT systems. You should note that although natural disasters can devastate your business, so can things that affect yur business data. If you, for instance, lose your customer data, you can be fined for a failure to comply with the General Data Protection Regulations under the Data Protection Act. Not only may you be fined, but your businesses reputation will be at risk as will your revenue due to a drop in cus-tomer confidence. A business recovery strategy should therefore always outline all the potential risks that could impact upon a business.

Should a disaster occur, it is imperative that a business is able to communicate with others who are deemed valuable to the business, such as customers or the media. Any strategy must include a communication plan and should also outline which employee is responsible for what activity, in terms of coordinating business recovery activities. A project manager and senior executive are likely to be responsible for putting the plan into action. Other important workers will need to know how and where they will resume their work. Any other employees will require information on how they are to return to work post whatever incident occurs. Your recovery plan should include a list of contact details which should be available for business suppliers and customers for them to call so a staff member can explain how the business is recovering post incident and what the relevant arrangements are.

The following articles may assist you with planning your own business recovery strategies:

- **Company Disaster Plan Examples**
- **Disaster Recovery Plan vs. Business Continuity Plan**
- **Increase Sales and Revenue: 5 Essential Strategies**
- **Recover Lost Revenue**

REGIONAL RESILIENCE PARTNERSHIPS

https://www.readyscotland.org/ready-government/resilience-division/

RESTAURANTS [lvii]

See also: Hotels

Cafés and restaurants can often become targets for fraud whereby individuals may appear to be genuine customers but who then deliberately leave the premises without paying for their meal. Often these individuals will target numerous premises as part of a fraudulent scheme. Instances such as these are detrimental to any business, however, there are ways to reduce the likelihood of such crimes occurring.

If a premises has a cark park, then it should always be kept clean and well lit, with designated park-ing bays clearly defined/painted. If possible, CCTV should be installed and clearly signposted, which can assist with number plate image capture. If individuals perceive there to be a high level of security outside a premises, they will likely assume that this is also the case inside.

Always examine any exit points for a premises from a security perspective. The general rule is the fewer the better. If there is an outside smoking area which is not segregated from the street, and all members of the dining party are outside, then individuals could easily leave without paying. Ensure there are sufficient members of staff to patrol any such areas on a regular basis, and consider in-stalling CCTV cameras to facilitate surveillance of all outside spaces from within the building.

If you require advice on CCTV, as well as details on approved suppliers, please click here to visit the National Security Inspectorate website; and here to visit the Security Systems and Alarms Inspectorate Board.

A high standard of customer service is one of the most effective ways to deter an opportunistic criminal, as this demonstrates that the establishment is focussed on customer care. Encourage employees to pay close attention to customers, make eye contact and engage in polite conversation. The higher the standard of customer care, the lesser the chance of someone leaving a premises without paying.

lviiilix

RETAIL CRIME

Retail employs 253,490 Scots – 13.4% of the total private sector workforce and is one of the country's most dynamic industries. Along with wholesale it accounted for 15% of all new businesses formed in Scotland in 2013. Scotland has 23,550 retail outlets, 11.9% of all business outlets and there is an annual spend of around £2.55bn in Glasgow which is the UKs second biggest shopping destination.

The following tips can reduce the likelihood of an individual committing theft by shoplifting:

Recognise how to spot a shoplifter and provide the relevant training to all members of staff so that every employee knows the behavioural indicators of a potential thief. Someone intent on stealing may display the following behaviours:

a. Attempting to look inconspicuous whilst avoiding retail and security staff
b. Appearing nervous; visibly sweating, or having a flushed complexion
c. Picking up an item, putting it back, and then picking it up again
d. Paying more attention to what is going on around them, rather than the product that they have in their hand, or goods on the shelves
e. Wearing a large coat, regardless of the weather conditions, or carrying a large bag

It is important to remember, however, that not every person displaying these behaviours is planning on stealing. These are just signs to look out for.

Sometimes, even if there is suspicion that someone is shoplifting, nobody knows what to do about it. You should therefore ensure that all your employees are trained to implement the comprehensive shoplifting policy that your business has in place if they believe they have spotted a shoplifter.

People who are trying to shoplift will be discouraged if they believe they have been spotted; so good customer service skills can help prevent theft. If you have a suspicion that somebody may be planning on shoplifting, approach them and ask if they would like any help. Or, perhaps, tidy shelves that are near them to make sure they know you are there.

If it is possible to change the layout of your premises, the following techniques will ensure that people attempting to shoplift find it more difficult to leave the premises in possession of goods:

f. Sit the cash register by the door of the premises so that individuals have to walk directly past a member of staff when leaving. Never leave it unlocked.
g. Try and reduce the number of blind spots across your premises. You can do this by moving where you put your displays or by using a more effective form of lighting.
h. Keep displays lower down, it will be easier to see customers, and potential thieves, over the top of them

Items that are more likely to be stolen should always be made a harder target for shoplifters. If it is a possibility, place them in locked display cases. If this is not possible, place them next or near to the till; or somewhere where a member of staff will always be able to see them.

It will be difficult to identify what has been stolen without an oversight of what stock is within the premises. Always keep up to date with stock takes and inventories. This will help identify any in-stances of theft, and can also highlight patterns and allow changes to be implemented in response to those patterns.

You should put up warning signs advising customer that they are subject to surveillance via CCTV cameras and highlighting the consequences of their actions should they steal from your premises. These can both act as an effective deterrent for any potential shoplifters.

lviiilix

RETAIL CRIME

Introduce additional security measures such as CCTV cameras, tags, and alarms. Consider hiring a security guard if you believe your business is at a serious risk of theft.

Some may have local retail crime initiatives, which can be used to share information on known shoplifters. CCTV can also be connected to other premises in the neighbourhood, which will make it easier to identify and hopefully catch those individuals who shoplift.

Remember that the above are only tips, and the onus is on you to take appropriate action and implement preventative measures to keep your premises safe. You should also check your insurance doc-uments so that you know what you are covered for under your policy.

See also: Retail Crime Booklets 1 and 2.

lx

RISK MANAGEMENT

Over the past five or so years, many businesses have become concerned only with the concept of loss prevention, and not the concept of crime prevention. As long as their insurance policy adequately covers the loss, then it is likely that a business will only undertake the most of basic preventative measures. This is ill-advised, as it is not possible to mitigate all the potential losses from with crime and insurance.

Management are required to assess what risks their businesses face in terms of criminality. As a result, they must then consider strategies that will either prevent the potential loss, or, reduce the risk to a manageable level. From a manager's perspective, the actual loss can encompass anything that has the potential to corrode the core functions of the business and erode the profit of the business.

There are a number of security violations that have the potential to impede the probable and potential financial gain of your organisation. Although major disasters (such as fires) are often perceived as the only events which may cause disruption to a business, minor issues can also have serious and far reaching implications This is despite them often being regarded as insignificant. Generally speaking, anything which may cause a potential financial loss for your business or that may affect the core functions of your business, either in the present or in the future, is considered a risk.

You must continually assess the risks your business faces. A change of location, adding or removing a new staff member, or even the purchase of new electrical equipment are just some of the events that may impact upon a risk assessment. It is not only the actuality of crime, however, that should be considered. The fear of crime itself can hugely affect the opinions of the public and your employees; and if not addressed, this fear could subsequently create a hostile working environment.

You should always keep a security register or diary and ensure that it is well-maintained. If the de-tails of incidents are recorded accurately, alongside every associated cost, then the data can be analysed soon after the event, thereby identifying any trends and establishing what constitutes the most effective preventative action.

Although commercial break-ins may be very common in some areas, many businesses only become aware of the high crime risks presented to them once they become a victim themselves. It is at this point, regrettably, that most businesses consider different forms of crime prevention. The likelihood of a second or subsequent attack on your business within a short time following the original break-in is very high.

Even the most insignificant crimes can have a considerable impact on business. For example, a computer being stolen during a break-in can be hugely problematic. In most cases, it is not the actual computer that is of primary concern (the primary cost), nor is it the repair costs to the building or the lack of work that may achieved while waiting for a replacement (the secondary costs). Rather, it is the risk that individuals may now have in their possession confidential business information or customer information. It would be difficult to mitigate the 'repercussion costs' as it is known by insurance, that this situation would present, as such effects cannot be simply quantified.

It is the repercussion costs that are often the most damaging to a business, as the financial loss and rates of employee satisfaction can also be destroyed through crime.

If the risk that a particular crime occurring toward you is very low, and the costs of the security measures needed to protect against it are very high, then it would likely be more effective to mitigate whatever loss you experience by insurance, rather than trying to meet the high preventative costs yourself. However, the subsequent high premiums you are likely to face as well as the secondary losses and likely inconveniences you will have to work with will have to be considered, as the improved security costs may not be as significant.

If you are a manager of a business, you will need to regularly assess, monitor and evaluate the costs of your security measures. This includes both those which are proposed and achieved.

The following SBRC Factsheet provides some tips to consider when trying to keep your business safe from the threat of robbery:

More information can be found within the violence reduction booklet available at the following link:

www.scotland.police.uk/assets/pdf/keep_safe/234532/working-with-business-to-prevent-robbery

RURAL CRIME

See also: Farm Crime.

Many of the crime prevention techniques that are outlined in other areas of this compendium, such as the section entitled 'Keep Safe' are just as relevant for rural areas, as they are for urban. The rural communities of Scotland are often some of the safest places to live and work. The nature of the environment and the ways of life, however, mean that you should consider the following crime preven-tion tips as additional considerations which are unique to rural communities:

- The protection of livestock
- Securing plant/farm machinery
- Preventing theft from fuel tanks
- Securing tools and horse tack

Advice on the scheme 'Rural Watch' can be found here:

https://www.neighbourhoodwatchscotland.co.uk/news/test-news-article/

A guide to Farm Building Security is available here:

https://www.scotland.police.uk/assets/pdf/keep_safe/343027/rural-crime-buildings

A guide to Equine Security is available here.

www.scotland.police.uk/assets/pdf/keep_safe/343027/rural-crime-equine

A guide to Livestock security is available here:

www.scotland.police.uk/assets/pdf/keep_safe/343027/rural-crime-livestock

A guide to All Terrain Vehicles and Quad Bike Security is available here:

www.scotland.police.uk/assets/pdf/keep_safe/343027/rural-crime-quad-bikes

You can find more relevant documents by clicking here:

www.scotland.police.uk/assets/pdf/keep_safe/343027/rural-crime-quad-bikes

Other useful organisations

Scottish Grocers Federation

SGF is the National Trade Association for independent convenience stores in Scotland. There are 5,545 convenience stores in Scotland- which provide over 42,000 jobs with a total value of sales of some £4 billion annually.

Federation of Small Businesses

The FSB offers its members a wide range of business services including advice, financial expertise, support and a powerful voice in government.

www.fsb.org.uk

National Federation of Retail Newsagents

NFRN members benefit from a range of advice, support and resources for this sector.

https://nfrnonline.com

Association of Convenience Store

The ACS supports local shops and supports its members through effective lobbying, comprehensive advice and innovative networking opportunities.

www.acs.org.uk

See: Cyber and Fraud

Postal Scams

Contacting victims of crime via the postal service is a common method for scammers to use, however, as the techniques they use become more and more sophisticated, it is becoming increasingly difficult to differentiate between scam and junk mail from legitimate companies. The following list details some of the most common postal scams:

You may receive letters which tell you that you have won a cash prize. Within the letter that tells you this, however, you may be asked to telephone a premium rate number and/or asked to pay a free in order to 'release' your prize. Never respond to these letters if you receive one, even if they appear genuine. A genuine lottery draw will not ask you to pay a fee in order to collect your winnings.

You may receive letters claiming that the individuals have 'seen' something in your future and require money from you in order to disclose what they have seen. These scammers will often coordinate their attacks with other scams, to give the impression that they are predicting good fortune, such as the lottery and prize draw scams. Never respond to these individuals, even if they threaten you or try to alarm you by saying they have predicted something negative. The letter may be written as though you have been specially chosen, however the same letters are sent out to millions of people.

Pyramid scheme scams take the form of chain letters or investment schemes which often promise that individuals can make a profit with no or little risk involved. Within these schemes, you will then be pressured to encourage other individuals to join the scheme. Alternatively you will be told to send money to the individual who originally contacted you, before you receive any return on your investment. You should never join one of these schemes. These schemes involve the use of overpriced products which actually hold little value. You should ignore any messages that seem threatening if you do not respond to the original message, as this is a common tactic used to recruit new members.

Individuals trying to commit fraud may claim that they have lost all their money due to some form of unfortunate circumstances and ask you for help. Individuals often then claim that they need to pay for some form of serious expense, such as an operation, and will ask you for financial assistance. These stories are fake. Do not respond, not even to say no to the request. Doing so will only encourage the individual to continue to contact you with similar pleas.

You may receive a letter, which is addressed to you personally, advising that somebody has left you a sum of money within their will. The letter will often make reference to a genuine law firm and may even provide what appears to be a genuine email address, postal address and website details. Always check with the Solicitors Regulation Authority (which you can do by clicking here) to verify the authenticity of these letters. The Solicitors Regulation Authority website regularly receives reports of similar scams and updates their website accordingly.

You may receive a request to help an individual transfer money out of their country (which is not your own) in return for some form of reward. The letters look very official and are often written to appear as though they have been sent from a government official or from a solicitor. Never reply to the letter and do not provide them with your bank details or personal information. In some cases, it is easier to identify these types of scam letters as they are badly written, containing numerous spelling mistakes and/or poor grammar.

These scams involve offering an individual work to complete at home providing a registration fee is paid. Following payment, there may even be an offer of an interview via a telephone call. Legitimate employment agencies, however, will never charge a registration fee.

To protect yourself from postal scams, you can:

- Contact the Mailing Preference Service (by clicking here) to have your name and contact details removed from the direct mailing lists that exist in the UK. You should note, however, that this will not cover generic mail that is not personally addressed or mail from overseas
- Place a 'no junk mail' sign on your front door - you can either make this yourself or you can buy one easily and cheaply online
- Consider joining the Scam Marshal Scheme which allows you to forward anything you believe to be scam mail to the scheme, which helps catch the individuals responsible. Remember, if you receive mail that you believe may be a scam, never respond. Always throw it away.
- Contact someone if you are worried that you have received, or think you have received, something via the mail that looks like a scam. Consider talking to your family or friends, or anyone else you trust.
- Remember to always check the credentials of any company, including any legal professional, which appear on a letter that you receive

There is nothing to be ashamed of if you do fall victim to a postal scam. Many people do, and the scammers behind them use a range of techniques to carry out their scams, and the techniques are becoming more and more sophisticated. You should contact Action Fraud if you think you have been a victim of a scam. They will try to track the individual responsible. If you are concerned about whether or not a scheme is legal, you should contact the Citizens Advice Customer Service by clicking here for more advice. You can also click here for more support for scam victims.

Individuals who are still on mailing lists as well, as those who are categorised as being internetless, are increasingly becoming the preferred targets of both postal and telephone fraudsters. These individuals tend to be older people and/or those who live alone and are vulnerable in some way.

The charity Think Jessica produces an array of booklets, leaflets and other materials to help inform those who are not able to research things online about the different scams in circulation, and the methods scammers are using. The materials are also designed to give these individuals more confidence in helping them recognise if they may have fallen victim to a scam and giving them the knowledge on how to report it. Perhaps more importantly, the materials also provide signposting to agencies that they can go to for help.

Since beginning, Think Jessica have built up strong partnerships with a variety of different organisations who also work to help fight scams, especially when they target vulnerable people and older people. These organisations include Action Fraud.

You can find more information about Think Jessica by visiting the link below:

www.thinkjessica.com

When you undertake a comprehensive physical inspection/evaluation of the security systems, controls and their parameters in a public/private property, asset or an organisation, you are undertaking a physical security assessment. This is a combined process which involves conducting concentrated audits and analysing the results. This analysis then provides an overview of the physical security mechanisms of the facility in its entirety. Please see below for further information.

When you undertake a physical security assessment, you undertake a well-define process which is usually adopted to meet with the differing requirements from standard organisations and regulatory authorities. When you undertake a physical security assessment, every type of security system that is installed in your premises will be examined thoroughly. Click here to access a workplace security audit template.

A number of both natural and human cased factors can threaten your businesses resources, assets, sensitive information and secrets. These factors can contribute to either the partial or complete destruction of a business. These threats often occur through one of two pathways – either through the IT Network or through physical invasion.

Generally speaking, it is much easier for a hacker to gain access to your IT resources if they are able to physically gain access to your premises. Your premises should, therefore, have security systems that are 100% effective, and active 24 hours a day. You can ensure that you achieve this by implementing frequent physical security audits, as they can help identify any flaws and deficiencies that exist within security systems, which can then be resolved. Having a robust security system is a must for safeguarding your businesses assets, as well as an information that relates to your business.

A physical security assessment and a physical security audit may look similar, but they do have differences. In a physical security system, for instance, the availability as well as implementation and maintenance of security systems are dealt with. A security audit evaluates the level of effective implementation of the security policy of the organisation; by employing the help of different security controls. The physical security audit can help find the gaps and loopholes that exist within existing security mechanisms. On the other hand, the security assessment helps study the security loopholes that exist in the system and need for the new systems. The security assessment is therefore a much wider process than undertaking a security audit.

Undertaking a physical security audit can help uncover problems within your premises. A robust security system may include having things such as CCTV systems, alarm systems and physical locks. Undertaking a physical security audit may help find out the security gaps within an existing business security policy, with the help of the visual inspection and the operational activities.

Some of the main problems that can be uncovered by a physical security audit may include:

- A lack of proper follow up by higher management in relation to the security policy
- Poor levels of motivation, supervision, and monitoring of the security personnel hired from third-party contractors. This may result in an improper adherence to security policy procedures
- A low level of precaution and care undertaken by employees whilst around the valuable assets of a company (such as laptops and office equipment)

- Both employees and security staff being poorly trained, or not being aware of the security policies and procedures that are vital when accessing/working with assets, as well as on leaving the company
- Individuals not wearing company identification badges, or not wearing them all the time; the pictures of the badge holders or the badges themselves being unrecognisable
- A poor level of control over visitors to the company; or a poor level of control over employees.

When to undertake a physical assessment will vary in terms of the organisation, the location, and any local regulations or industry rules and compliances. For the majority of cases, security assessments are conducted on an annual basis. In some cases, and especially within mission critical organisations, security assessments are conducted on a semi-annual or quarterly basis. Before undertaking a security assessment, check that the assessment outline complies with any local authority rules and regulations, as well as any industry best practices.

New start-up companies initially considering the aspect of physical security, must complete the following steps:

- Assess the physical security level presented within the business
- Choose what the suitable controls are to mitigate the risks found
- Devise ideas of security and its management policy
- Implement the controls as per the policy created
- Manage the controls as per the security management policy
- Continue to audit and assess the security level at certain, defined intervals
- Should any major issues be found, correct them as soon as possible

The following are key points to consider when conducting a physical security audit checklist:

- Management policy
- Physical security policy
- Risk assessment
- Staff security
- Access control
- Data/information security
- Forms of emergency communication and rapid response
- A technology review

If there is not a good policy of physical security assessment in place, it will be difficult to manage a business without there being high risk factors.

Further advice can be found on the CPNI website:

https://www.cpni.gov.uk/physical-security

In the correct environment, having a security guard may not only assist in reducing crime, but also help reduce the fear of crime by reassuring the public and your employees. You can hire security staff from various manned guard businesses, or you can employ them directly as you would any other member of staff.

When enquiring about security services, consider the following points:

- How long has the company been in operation and trading?
- What kind of insurance does it have? Particularly, what type of liability and indemnity insurance does it have?
- Does the company issue written contracts?
- What kind of vetting procedure does the company have when employing staff?
- Do the guards which are part of the company have terms of employment, for example a maximum amount of hours/shifts worked a week?
- Do they produce identity cards? What type of uniform do they use?
- Are the staff trained? Do they get qualifications as a part of this training?
- Does or will the company sub-contract to a security company lesser than them?
- Does the company operate a control room? If not, how are their staff controlled and supervised whilst in work situations?
- Does the company work to an Industry Code of Practice (BS7499 and BS7598)? Does it have independent certification to verify this?
- Do they have the ability to supply references from similar companies to you?
- You should consider the need for a replacement when one of your original guards is off ill or on holiday
- You should give careful consideration to any consequences which may arise from any unlawful arrests. Whoever you employ the security guard from may be liable to pay any damages under the principle of 'vicarious liability'.
- Depending on the wider context, you should note that one of the most damaging consequences of any civil action (for things such as wrongful arrest) may be the negative publicity and damage to the company name. Incidents like this can attract attention for all the wrong reasons and permanently damage the company's reputation.

Further information can be found here:

https://www.cpni.gov.uk/professionalising-security

https://www.sia.homeoffice.gov.uk/Pages/home.aspx

lxiv

SERIOUS ORGANISED CRIME

Serious organised crime refers in general terms to the generating of wealth at the expense of others, and it includes things such as drug-dealing and money laundering. In 2015, the Serious Organised Crime Strategy (click here to read) aims to reduce the harm which is caused by serious organised crime by ensuring that all the partner bodies work well together. It focuses on four key objectives;

- **Divert:** to divert people from using products of serious organised crime and becoming involved with serious organised crime itself
- **Deter:** to deter serious organised crimes groups by ensuring that the private, third and public sector organisation are supported in protecting themselves and one another
- **Detect:** to identify as well as detect and prosecute those individuals who are involved in serious organised crime
- **Disrupt:** to disrupt serious organised crime groups

For more information:

https://www.scotland.police.uk/keep-safe/280693/280696/

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/752850/SOC-2018-web.pdf

National Crime Agency website

https://www.nationalcrimeagency.gov.uk/

lxii

SECURE SUPPLY CHAIN SCOTLAND

SSCS works with its members to protect their products and cargoes by developing crime prevention measures, exchanging information on relevant security and regulatory issues, sharing best practice and circulating intelligence.

You can find more information on them by visiting the link below.

https://www.sbrcentre.co.uk/about-us/our-focus/sscs-secure-transport/

SCOTTISH BUSINESS RESILIENCE CENTRE

The Scottish Business Resilience Centre (SBRC) is a non-profit organisation which exists to support and help protect Scottish businesses.

Its unique connection to Police Scotland, Scottish Fire and Rescue Service and Scottish Government gives them exclusive access to the latest information on legislation, criminal trends and threats, allowing them to provide the very best advice to safeguard your staff, customers and business.

They offer a wide range of business resilience services, delivered by their expert team of trusted professionals, seconded police and fire officers and innovative Ethical Hacking students from Abertay University.

They work in partnership to protect people, places and processes and they are constantly looking at new ways to keep businesses free from risk.

www.sbrcentre.co.uk

Places which are usually crowded and easily accessible to the public, including shopping centres, bars and pubs, are an attractive place for terrorists. If you would like site specific advice which could help you make your premises safer, you should contact your CTSA (by clicking here) or use the non-emergency police number 101. You can also view guidance on the National Counter Terrorism Office website by clicking here.

Further advice can be found on the Scotland's Towns Partnership webpage:

https://www.scotlandstowns.org/town_centre_toolkit

Shoplifting: ***See Retail Crime***

When you are home alone, you can ensure that you stay safe by:

- Checking that all the windows are securely closed and locked if appropriate
- Locking all the doors from the inside and removing the keys
- Only letting in people who knock on your door if you know who they are. If you don't know who they are, don't let them in. Always check who is there before you open your door. Use a spyhole and chain if you have them fitted
- If you have a back door to your property, you should always lock it before you go to answer the front door. Try to get into the habit of always keeping it locked.
- Never tell any unknown caller, including phone callers, that you are home alone. Lie if you have to and tell them that someone else is home

When you are out and about, you should:

- Avoid going down dark alleyways or walking routes you do not know
- Always keep an eye on what you are drinking. Even soft drinks can be spiked. Never leave your drink unattended in public.
- Always trust your gut feeling. If you feel uneasy for any reason, you should change your route or go somewhere that you feel safe
- Always try and look confident and walk purposefully
- Set your phone to vibrate or silent so you don't appear as an obvious victim to those looking to steal mobile phones
- Always be aware of what is happening around you - don't text and walk, or have your headphones in with music playing very loudly
- Before getting in a car for a lift anywhere, text the car registration number to someone you trust
- Ensure that your phone is fully charged and, if applicable, has sufficient credit to contact someone in an emergency

When you are active online you should:

- Adjust the settings for your social media accounts, such as a Facebook or Twitter, to ensure that only friends or followers (in the case of Twitter) can see your personal details and direct message you.
- When you are gaming online, use a name that you have made up. Do not be tricked into giving out your personal details to other players.
- Do not have anyone on your instant message list that you don't know in real life
- Take the time to learn how to keep things like your personal information and your bank details secure online
- Treat anything that is said in a chatroom and/or a forum with due suspicion. Never assume it is true

It is normal, and good for us, to experience some pressures and challenged in life. However, if we are exposed to these pressures and challenges for a long time, it can lead to stress. Continual levels of stress can lead to both physical and mental health problems.

If you are an employer, you are expected to carry out an appropriate and sufficient risk assessment for levels of stress within your organisation. If you find any problems in these risk assessments, you are expected to address these problems. In order to help you carry out your stress risk assessment, you can click here and here to access resources produced by an external organisation called Work Positive. These guidelines are aligned very closely with the Health and Safety Executive (HSE) Management Standards.

Advisory, Conciliation and Arbitration Service website:

http://www.acas.org.uk/index.aspx?articleid=6062

TEN STEPS TO BUSINESS RESILIENCE

The following is a self-assessment tool that has been developed by the SBRC which enables businesses to manage risk simply and effectively, which will provide reassurance to investors, employees and customers.

You can access the self-assessment tool by visiting the link below:

www.10steps.co.uk

TOURISM

Scotland is generally a safe place to visit, however there are individuals out there who will be looking to take advantage of the unsuspecting tourist.

Please have a look at the Police Scotland Webpage to learn more in keeping yourself safe:

www.scotland.police.uk/keep-safe/personal-safety/tourists-and-visitors

If you would like more information, please click here where further information can be obtained from Scottish Natural Heritage.

For more practical tips and advice on travelling in and around Scotland to the the VisitScotland webpage where appropriate advice and guidance can be found.

www.visitscotland.com/about/practical-information/

TRAVEL

It is very important that you consider the health and safety of your employees while they are travelling, especially when overseas. While your employees are out on a business trip, in most cases it is likely to go well. However, sometimes things can go wrong, and when they do, you must have appropriate corporate safety and security procedures in order to effectively deal with them.

You can find further advice by using the below websites

Government website relating to foreign travel:

https://www.gov.uk/foreign-travel-advice

Advisory, Conciliation and Arbitration Service

www.acas.org.uk/index.aspx?articleid=2797

Travel aware

https://travelaware.campaign.gov.uk/

Police Scotland

www.scotland.police.uk/keep-safe/personal-safety/on-the-move

Government website relating to staying safe abroad

www.gov.uk/government/news/stay-safe-abroad-this-summer

The law in the UK states that the selling of age-restricted products to an individual who is below the legal minimum requirement is a criminal offence. There are different penalties, dependent on the nature of the sale.

The following table outlines age-restricted products in the UK, and the minimum age an individual must reach in order to purchase them:

Product	Legal Minimum Age
Tobacco products	18
Fireworks	18
Alcohol	18
Lottery tickets and scratch cards	16
Lighter refills containing butane	18
Solvent and volatile substances	18
Knives and offensive weapons	18
Aerosol paint containers	16

This table outlines the PEGI classifications for videos, DVDs and computer games:

PEGI Classification	Legal Minimum Age
3	3
7	7
12	12
16+	16+
18	18

More guidance for retailers can be found on the SBRC website:

www.sbrcentre.co.uk

lxviilxviii

VANDALISM

As the Metropolitan Police state, vandalism is where property is maliciously destroyed or damaged, not necessarily to gain entry to premises or a vehicle. Safeguard your property with our advice below.

Although it may feel like building a high wall or fence around your house will make it more secure, it means that it is hidden from view, and therefore, more tempting to vandals. Ensure that your property can be easily seen by your neighbours, and by anyone who may pass it. You can do so by ensuring that none of the hedges, fences or walls at the front of your house are taller than one metre. By doing this, you also ensure that any potential intruders have little to no places to hide. You should also consider employing the use of lighting. You should consider having low-level white lighting, dusk-till-dawn around your house, and especially at parts of your property which have low visibility, such as the rear. The lights that you place around your property should be, at a minimum, three metres high, and ground with vandal-resistant castings.

When you create a boundary, you are really marking your territory. You can do this in a number of ways, such as putting up a low fence/wall/hedge, or planting flowerbeds or small bushes. You should, however, avoid a rockery or a border comprising of large stones, as these can be used to vandalise your property. You should also consider painting your driveway a different colour than your road, to ensure people know it is your property.

Ensure that your safeguard the vulnerable parts of your property - such as any ground floor windows. You can also consider employing the use of security film - which is a clear or opaque covering which can be stuck onto your property's window - in order to make them harder to smash the glass.

Also consider painting your walls, especially if they are white, with anti-graffiti coatings. Doing such will prevent any spray paint from bonding to the walls.

If you have a surface that individuals can sit on, make sure that you don't make it 'bottom friendly', so to speak. Consider, for instance, using planters with prickly plants- as these are difficult for people to stand around for too long. You should also consider securing the rear perimeter of your property with two-metre high fences which are topped with trellis; something that is lightweight, and thus, unable to support a person. This also makes a loud noise when rattled, making it difficult for anyone who is trying to gain access.

If you leave your property messy, it is likely that others won't think twice about adding to the mess, or simply hanging around it. Do not leave any rubbish lying around, and do not leave ladders, wheelie bins or anything else that can be used for vandalism easily accessible.

The company 'Secured by Design' provides both advice and the latest crime-prevention products.

You can access their website here:

www.securedbydesign.com

VEHICLE CRIME

Car thieves are becoming increasingly organised and in a few seconds can have your vehicle taken far away. Bear in mind that criminals will choose an easy target. By following the steps below you can make it difficult for a criminal to steal your car.

Interpol website:

www.interpol.int/en/Crimes/Vehicle-crime

Crimestoppers:

https://crimestoppers-uk.org/keeping-safe/vehicle-safety

Government website on bus and coach security:

www.gov.uk/government/publications/bus-and-coach-security-recommended-best-practice

See also Cargo and Road Transport Security Guide:

www.sbrcentre.co.uk/media/2147/cart_security_guide_12mb.pdf

Secured By Design Website:

hwww.securedbydesign.com/guidance/vehicle-crime

VEHICLE DRIVERS

You can find information about driver fitness by clicking on the following link, which provides guidance on fitness to drive from the Royal Society for the Prevention of Accidents :

ROSPA Guidance:

www.rospa.com/rospaweb/docs/advice-services/road-safety/employers/work-fitness.pdf

Please note that some drivers you may employ will require more specific driver health assessments, especially if their role involves them operating a forklift truck or large goods vehicles (LGV) as well as passenger carrying vehicles (PCV).

The HSE also provides information for medical professionals on the specific medical standards for your employees at work:

https://www.hse.gov.uk/workplacetransport/personnel/medicalfitness.htm

You can also look at the Healthy Working Lives website for more information on vehicles and driving for work

https://www.healthyworkinglives.scot/workplace-guidance/vehicles-and-driving-for-work/Pages/default.aspx

A cart security guide can be viewed on the SBRC website:

https://www.sbrcentre.co.uk/media/2147/cart_security_guide_12mb.pdf

VICTIMS OF CRIME

The Victim Support Scotland website provides support and information to any victim of crime and any witness of crime in Scotland.

The website is available here:

www.victimsupportsco.org.uk

lxix

VIOLENCE IN THE WORKPLACE

According to the Health and Safety Executive (HSE), work-related violence can be understood as "any incident in which a person is abused, threatened or assaulted in circumstances which relate to their work".

This definition, therefore, encompasses verbal abuse or threats as well as physical attacks. The following links can explain what the HSE is doing in order to address work-related violence. The links also provide access to a range of information which may be of interest to you and your business.

The Legal Requirements you need to understand:

https://www.hse.gov.uk/violence/law.htm

Do Your Bit - how to involve and consult your workers:

https://www.hse.gov.uk/involvement/doyourbit/index.htm

Guidance for licensed and retail premises on managing violence:

https://www.hse.gov.uk/violence/toolkit/index.htm

Preventing workplace harassment and violence: the guidance:

https://www.hse.gov.uk/violence/preventing-workplace-harassment.htm

VISITORS

Any visitor who enters your business or premises should always have to pass through a supervised reception area. If your business is larger, you should have an identity badge system. You should always keep a thorough record of all visitors, and only release badges when you have received a signature.

A member of staff should always accompany visitors, both when the leave and enter the premises. The staff responsible for this should always be trained in security awareness - especially those who work reception too.

For more information see the CPNI website:

https://www.cpni.gov.uk/robust-visitor-entry-processes

lxx

VISITOR ATTRACTIONS

In 2019, the threat of terrorist attacks in the UK is a very real danger. As per the terrorist incidents in 2007 which occurred in Haymarket, London; and Glasgow Airport; terrorists continue to attack crowded public spaces. This is due to the likelihood of there being limited protective security measures in place, meaning the potential to cause mass fatalities and casualities is far greater. Recent terrorist attacks also demonstrate that these individuals are also willing to use vehicles.

You must be aware that your attraction could be involved in a terrorist incident, regardless of how low the perceived risk may be. You may have to deal with a bomb threat; or with suspicious items that have been left in and around your premises, or that have been sent in the mail.

It is understood that in order to keep your attraction running, you need to maintain a friendly and welcoming atmosphere; and the advice which is available to you does not suggest that you need to develop and sustain a 'fortress mentality'. Instead, a balance should be created between fostering a welcoming environment and ensuring that those who are responsible for security are informed of the robust and protective security measures that are available to them. The surrounding environment should always be considered, such as protection from flying broken glass should windows be shattered.

For further information, see below:

Government website on Crowded Places

www.gov.uk/government/publications/crowded-places-guidance

Government website on visitor attractions

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/375180/VisitorAttractions_Reviewed.pdf


W

Leaving combustible materials lying around your property increases the potential that your property will be damaged, through an accident or otherwise.

In order to minimise this risk you should:

- Ensure that your waste materials are not left lying about your building. Make sure that all your waste is placed in the correct container
- Ensure that your goods and materials are always kept secure
- Ensure that all your waste bins and any skips you may have are stored in secure compounds. If this is not possible, you should only use lockable bins and skips
- Ensure that your security is sufficient enough so that individuals cannot break containers open, and things cannot be removed by thief's, animals or any bouts of bad weather
- You should understand that the waste you leave around may give potential thief's that you are holding valuable stock equipment (e.g. new computers)
- Ensure that all your litter bins are emptied on a regular basis, and contain fixed liners

More information on waste management can be found on the Keep Scotland Beautiful Website:

www.keepscotlandbeautiful.org

Illegal Waste in Scotland

The task of protecting and improving the environment in Scotland falls into the hands of Scotland's environmental regulator: The Scottish Environment Protection Agency (SEPA). SEPA work to try and help businesses and industry better understand the responsibility they have to the environment in the dissemination of legislation guidance, as well as helping businesses realise the economic benefits of being environmentally friendly.

SEPA undertakes intelligence-led work which targets illegal waste management processes that cause damage to the environment and pollutive effects. The illegal waste management processes that SEPA targets undermines and compromises the efforts that legitimate waste and recycling operators, as well as land-owners who dispose of their waste appropriately, who are often left to deal with the expenses that are associated with the reclamation of land and disposal waste.

Illegal Waste sites, within Scotland, are defined as those sites where the deposit, treatment, storage or disposal of different and multiple waste types are being undertaken as a business without them holding the appropriate license or exemption issues by SEPA.

SEPA is looking to work with law enforcement partners as well as local authorities, businesses and associated industry contacts in order to identify high risk sites, and in order to undertake an effective joint agency action.

The typical illegal waste activities include:

- Operating illegal landfills;
- Illegal skip hire operators;
- Undertaking of large-scale and persistent dumping and burning of waste;
- The illegal disposal of contaminated land
- The illegal storage of scrap car parts and other vehicles
- The processes of land raising with the use of wastes including demolition and construction
- The disposal of liquid wastes
- The disposal of high costs waste, including those deemed medical and hazardous wastes (such as asbestos)
- The unauthorized storage or movement of waste and
- The illegal movement of waste (such as scrap cards) through and across international borders

If you are a local authority or land owner which is involved in the rental or lease of a premises to customers who operate in any waste or recycling should consider contacting their local SEPA office in order to inform them of any potential waste activity and ensure that subsequent operations are licensed appropriately.

If you want any further information or guidance on waste management in Scotland you should view the SEPA website:

www.sepa.org.uk

or contact the 24/7 SEPA pollution hotline on 0800 80 70 60.

You should prepare your business and employees for possible adverse weather conditions well in advance. If you do not, it can cost you.

Your business should ensure that every one of your employees and volunteers are aware of your adverse weather policies. If they are not, you should always explain these to them, and confirm that they understand any of the procedures you have outlined. You should ensure that you clearly state what you understand and have defined as 'adverse weather'. Employees should therefore know ex-actly when this policy will come into effect. You should also let your employees know when your business will allow them to go home. This should help you avoid any confusion should the weather force your business to close during a working day.

If any of your employees do need to work from home, they should have every opportunity to do so. Any policy put into place should allow employees to do this effectively and productively. Before any bad weather occurs, you should arrange a contact method to the company network. If it is needed, you should provide training about remote connection to your employees. You should ensure that this training is conducted prior to the winter season.

Although typically used for other reasons, you can conduct return to work interviews to discuss the problems caused by the adverse weather. In these interviews you should discuss any possible solutions for the next period of adverse weather - such as alternative transport an employee may need to travel home safely.

You should consider it a top priority to train your employees to deal with any task or duty essential to your business during adverse weather. You should also make sure that there are back up personnel for each critical business area. Doing such could require you providing additional training, but in the event that adverse weather occurs, and these procedures and processes are not covered, you will likely be relived.

You should consider developing a process for recognising those employees that do make it to work through difficult weather conditions. Make sure that you know which staff members make it into work and reward them appropriately. Rewarding your staff members does not always have to be with money, a simply mention or thank you should suffice. If you let staff know that their efforts are not unnoticed may encourage other staff members to make the effort next time.

You can find helpful links, numbers, contacts and advice in the event of adverse weather below:

Transport Scotland

www.transport.gov.scot/

The Met Office

www.metoffice.gov.uk/

Ready Scotland

www.readyscotland.org/

lxxxi

WEATHER

If you are travelling on the road, you should ensure that you and your vehicle are adequately prepared for the conditions. You should make sure that you have sufficient fuel in your vehicle, and ensure you have a supply of warm clothes, food and water with you in case you get delayed. Ensure your mobile has sufficient charge and plan the route you will be taking in advance. You should listen to news outlets (especially your local radio) and visit Travel Scotland before you set out.

The new warning levels are:

- Travel with Caution
- High Risk of Disruption
- Avoid Travel on the Road
- High winds- travel with caution - vulnerable vehicles

lxxii

WELFARE OF STAFF

A recent study undertaken by the British Government (https://www.gov.uk/government/publications/worker-wellbeing-and-workplace-performance) has suggested that an improvement in wellbeing of staff will result in an improvement of the work-place's performance. It suggests that this workplace improvement will span across the workplace financial performance, its labour productivity as well as the quality of its outputs and services. It also showed how better employee job satisfaction (which includes satisfaction with employee autonomy) has a positive and strong link with workplace performance. The wellbeing of your employees (as well as yourself) both inside and outside of the workplace should therefore be of importance to your business. You should work to get the very best out of your organisation and can consider adopting practices to increase the wellbeing of your employees - a trend that is becoming increasingly common.

Further advice on such can be found on the ACAS website:

www.acas.org.uk/health-and-wellbeing

and on the Scottish Centre for Healthy Working Lives website:

www.healthyworkinglives.scot/workplace-guidance/Pages/workplace-guidance.aspx

lxxiii

WHISTLEBLOWING

The term whistleblowing refers to the act of a worker passing on information which concerns protentional wrongdoing. Generally speaking, most of these cases will typically (but are not always) involve the employee discussing something that they have witnessed whilst at work. In order to be covered by whistleblowing laws, the worker who talks to you about the act must be convinced of the following two things:

1. They must believe that they are acting in the public interest
2. They must reasonably believe that the disclosure tends to show past, present or likely future wrongdoing which falls into one of the following categories:
   a. Criminal offences (including crimes such as fraud)
   b. Failure to comply with an obligation as set out in law
   c. Miscarriages of justice
   d. Putting someone's health and safety at risk
   e. Causing damage to the environment and
   f. Covering up wrongdoing in the above categories

Whistleblowing law provides your workers the ability to take their case to an employment tribunal if they believe they have been victimised at work or have lost their job as a result of 'blowing the whistle'. It is available in the Employment Rights Act 1996 (as amended by the Public Interest Disclosure Act, 1998).

More information on Whistleblowing can be found on the Government website

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/415175/bis-15-200-whistleblowing-guidance-for-employers-and-code-of-practice.pdf

ACAS website

www.acas.org.uk/index.aspx?articleid=1919

WILDLIFE CRIME

Generally, wildlife and habitats are protected because they are vulnerable and/or rare and they have a history of persecution. You are committing a wildlife crime when you recklessly or intentionally break the laws which have been developed in order to safeguard protected animals and protected areas.

Further information on wildlife crime can be found by clicking on the following links:

Police Scotland website

www.scotland.police.uk/contact-us/report-wildlife-crime

Scottish Natural Heritage

www.nature.scot/professional-advice/safeguarding-protected-areas-and-species/protected-species/wildlife-crime

Scottish Government website

www2.gov.scot/Topics/Environment/Wildlife-Habitats/paw-scotland

National Wildlife Crime Unit

www.nwcu.police.uk/


X

lxxiv

The festive period is often the busiest time of year for shopping. There are, however, individuals who will exploit this and will seize opportunities to commit crime. However, and in order to keep you and your business safe during the festive period, there are a number of preventative measures you can implement.

During the festive period, individuals are increasingly taking advantage of sale and events such as Black Friday and Cyber Monday. Often, they use online shopping platforms to do this and purchase their Christmas presents. If you do this, you should employ a couple of precautionary steps to lessen your chances of being targeted by criminals. You should also understand the dangers of social media – what you post online will stay online. You can find more about staying safe online in the Cyber section of this compendium.

When celebrating during the festive season, you may find yourself celebrating in pubs and clubs, especially for your work's Christmas party. Here are some key points you should consider which will help to keep yourself safe:

- Make sure you stay with your friends
- Stick to your pre-arranged plans
- Have your travel plans arranged prior to going out, especially your return journey home
- Be careful of what you drink, and never leave your drinks unattended
- Stay away from drugs and any other controlled substances such as psychoactive substances

In order to keep your home safe from criminals, consider the following steps:

- Leave some lights on around your property when you go out
- Keep your valuables and presents out of sight
- Open and close your curtains at the appropriate time of day
- Do not advertise on social media when you are out or away on holiday

During the winter months, you must ensure that your car is ready for the change in the weather. You should always ensure that your tyres, brakes, windscreens, wiper blades and windows are free from defects. Always be aware of the changing road conditions and never drive when it may put yourself or others at risk. If you are out partying, keep track of your alcohol consumption. Do not drink and drive.

The Scottish Business Resilience Centre has published advice to keep you, your home, and your business safe and secure this winter:

www.sbrcentre.co.uk/media/1954/sbrc-dec-2016.pdf

Police Scotland Xmas Safety Leaflet:

www.scotland.police.uk/assets/pdf/keep_safe/online-Xmas-safety-Leaflet?view=Standard

See Keeping safe

lxxv

Zero-Tolerance policies exist to eliminate undesirable behaviour amongst your employees. They can apply an automatic penalty for anyone who violates your businesses policy. Although perhaps being most commonly used in order to unwanted or unwelcome behaviour from employees, zero-tolerance policies can also be used in order to stop those who are in managerial roles from bending any rules you may have in order to apply for discretion. Zero-tolerance policies can be used to stop a number of behaviours, but they are most commonly used for issues such as sexual harassment and drug use.

lxxvi

Zero Waste Scotland aspires to create a society in which none of our resource are wasted and instead are valued. In order to achieve their mission of social change, Zero Waste Scotland motivates both individuals and businesses to engage in behaviours that help promote zero waste. They achieve this by providing tailored awareness programmes and the promotion of relevant brands, as well as direct interventions which effect change – these are often in terms of finance management, business sup-port, technical advice and forms of training.

More information on Zero Waste Scotland can be found on their website:

www.zerowastescotland.org.uk

A-Z

BUSINESS RESILIENCE
COMPENDIUM

Acknowledgement

We'd like to thank Abigail McLean, MSc Applied Social Research (Criminology), for her assistance in the development of this document.

References

Information, statistics and quotes used within this compendium were sourced from the following websites and documents and information rewritten for the sake of clarity and descriptive purposes. These websites can be accessed by clicking the links in this reference section. Each numeral corre-sponds to each section within the compendium.

i Wrexham.com (2018) http://www.wrexham.com/news/police-warning-over-fake-50-and-20-notes-being-circulated-in-wrexham-160196.html

ii Gambling Commission Betwatch toolkit (2018). Available: https://www.gamblingcommission.gov.uk/PDF/Betwatch-toolkit.pdf

iii Procedures for handling bomb threats. UK Government (2016). Available: https://www.gov.uk/government/publications/bomb-threats-guidance/procedures-for-handling-bomb-threats

iv Anti-bribery policy. Gov.uk. Available: https://www.gov.uk/anti-bribery-policy

v Information for this section was taken from the following blog published in 2007 http://rudyanto62.blogspot.com/2007/12/business-continuity-management.html

vi Information for this section was taken from Greater Manchester's Police A Guide to Security Booklet

vii National Neighbourhood Watch website. Available: https://www.nnw.org/business-watch

viii Police.uk: Vehicle Crime. Available: https://www.police.uk/crime-prevention-advice/vehicle-crime/

ix BSIA Website: https://www.bsia.co.uk/sections/cash-and-valuables-in-transit.aspx

x Cheshire Police Website: https://cheshire.police.uk/advice-and-support/business-safety-and-security/cctv/

xi The example of a plane crash was taken from here: https://en.wikipedia.org/wiki/Contingency_plan#cite_note-1

xii NPCC website https://news.npcc.police.uk/releases/counter-terrorism-police-announce-ground-breaking-insurance-initiative

xiii People Sense by Alitus. Article written by Stephen (2017): https://www.peoplesense.com.au/news/article/15122017-240/managing-a-critical-incident-in-your-workplace

xiv Revo Website Availbale: https://www.revocommunity.org

xv Nottinghamshire Police Website. Available: https://www.nottinghamshire.police.uk/site-page/cross-sector-safety-security-communications-cssc

xvi We are Cycling UK. Article by Hazael, (2019)https://www.cyclinguk.org/article/campaigns-guide/stop-bike-stolen

xvii CPNI Website: https://www.cpni.gov.uk/cyber-security

xviii Ontrack Website. Article written by Wiltshire (2015) https://www.ontrack.com/uk/blog/top-tips/writing-a-disaster-recovery-plan-for-your-small-business-free-template/

xix High Speed Training Website. Article by Spruce (2017). Available: https://www.highspeedtraining.co.uk/hub/drug-alcohol-policy-template/

xx Information for this section was taken from the HSE Government website: http://www.hse.gov.uk/event-safety/incidents-and-emergencies.htm

xxi Information for this section was taken from the Government of Western Australia's website: https://www.scamnet.wa.gov.au/scamnet/Scam_types-Threats__extortion.htm

References

xxii The ACG Website: https://www.a-cg.org/the-acg/about-us

xxiii West Mercia Police Website: https://www.westmercia.police.uk/article/13049/Farm-and-outbuilding-crime-prevention-advice

xxiv Police Scotland Website: https://www.scotland.police.uk/keep-safe/advice-for-victims-of-crime/fraud/

xxv Information for this section was retrieved from safer Scotland's (2008) Practical fire safety guidance for factories and storage premises

xxvi This information is drawn from the SBRC Website. Available: https://www.sbrcentre.co.uk/news/2019/may/get-yourself-covered-reduce-ufas-false-alarms-due-to-accidental-or-malicious-call-point-breakage/

xxvii AXA Website: https://www.axa.co.uk/make-a-claim/extreme-weather/flooding/

xxviii PSNI Police Leaflet. Available: https://www.psni.police.uk/globalassets/graphics/rp115--forecourt-security-leaflet.pdf

xxix BOSS Forecourt Watch Website: https://www.bossuk.co.uk/services/forecourt-watch/

xxx SBRC Website: https://www.sbrcentre.co.uk/news/2018/january/get-ready-for-new-gdpr-regulations/

xxxi IRCA Website. Article written by Parker (2017) https://www.quality.org/knowledge/importance-good-governance

xxxii HSE Website: http://www.hse.gov.uk/simple-health-safety/index.htm

xxxiii Cheshire Constabulary Website: https://cheshire.police.uk/advice-and-support/heritage-crime/

xxxiv Immobilise Website: https://www.immobilise.com/about

xxxv Devon County Council Website: https://www.devon.gov.uk/informationsharing/information-sharing-protocols

xxxvi CPNI Website (2013): https://www.cpni.gov.uk/system/files/documents/63/29/insider-data-collection-study-report-of-main-findings.pdf

xxxvii AXA website: https://www.axa.co.uk/business-insurance/

xxxviii Health Safety Emirates Website: https://healthsafety.ae/jesip/

xxxix Avyud Consultancy Website: https://avyud.in/formation/firm/partnership-firm/

xl Europol Website (2013): https://www.europol.europa.eu/publications-documents/prevention-and-coping-strategies-kidnapping-hostage-taking-extortion

xli Premises licence (Scotland) Gov.uk website: https://www.gov.uk/premises-licence-scotland

xlii Lyco Website. Article written by Harper (2014) https://www.lyco.co.uk/advice/protecting-your-premises-with-reliable-security-lighting/

xliii Secured by Design (2009)

xliv ACAS Website https://www.acas.org.uk/index.aspx?articleid=1900

xlv Gangmasters and Labour Abuse Authority report. Available: https://www.gla.gov.uk/media/3178/spot-the-signs-glaa.pdf

xlvi Information from this section also came from the SBRC Website. Available: https://www.sbrcentre.co.uk/media/2918/sbrc-issue-12.pdf

xlvii National Crime Agency Website: https://www.nationalcrimeagency.gov.uk/404

References

xlviii Ready Scotland Website: https://www.readyscotland.org/ready-government/national-centre-for-resilience/

xlix NBCC Website: https://nbcc.police.uk/?id=d62625150154bdeee2e912ea4be64e5b

l Ready for Scotland Website: https://www.readyscotland.org/ready-government/national-centre-for-resilience/

li Nottingham Police Website: https://www.nottinghamshire.police.uk/advice/prevention/worship

lii Crescent Learning Website: https://www.felp.ac.uk/taxonomy/term/671

liii National Buisness Crime Centre: https://nbcc.police.uk/guidance/purple-flag-scheme

liv Quality Assurance Wikipedia: https://en.wikipedia.org/wiki/Quality_assurance

lv Quote taking from: http://asq.org/data/subscriptions/sqp_open/1999/june/sqpv1i3vanveenendaal.html

lvi Chron Website. Article by Linton https://smallbusiness.chron.com/business-recovery-strategies-42682.html

lvii Metropolitan Police Website: https://www.met.police.uk/cp/crime-prevention/miscellaneous-theft/protect-your-restaurant/

lviii Simply Business Website. Article by Delves (2016) https://www.simplybusiness.co.uk/knowledge/articles/2016/09/top-ten-shoplifting-prevention-tips-to-protect-your-retail-business/

lix Information for this section was also sourced from the SBRC website: https://www.sbrcentre.co.uk/about-us/our-focus/retail-and-tourism/

lx Information for this section was taken from Greater Manchester's Police A Guide to Security Booklet

lxi Age UK Website: https://www.ageuk.org.uk/information-advice/money-legal/scams-fraud/postal-scams/

lxii Kisi blog website. Article by Mehl (2018). https://www.getkisi.com/blog/physical-security-assessment-problems-it-can-uncover

lxiii Information for this section was taken from Greater Manchester's Police A Guide to Security Booklet

lxiv The Scottish Government Website: https://www.gov.scot/policies/crime-prevention-and-reduction/serious-organised-crime/

lxv Gov.uk website: https://www.gov.uk/government/publications/crowded-places-guidance

lxvi Healthy Working Lives website: https://www.healthyworkinglives.scot/workplace-guidance/mental-health/Pages/stress-at-work.aspx

lxvii Metropolitan Police Website: https://www.met.police.uk/cp/crime-prevention/vandalism/property-vandalism/

lxviii Information for this section was also sourced from the Metropolitan Police Website: https://www.met.police.uk/cp/crime-prevention/vandalism/

lxix HSE Website: http://www.hse.gov.uk/violence/

lxx Information in this section was sourced from Police Scotland's report for visitor attractions https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/375180/VisitorAttractions_Reviewed.pdf

lxxi CIPHR Website. Article written by Chignell (2013). Available; https://www.ciphr.com/advice/prepare-your-business-for-winter/

lxxii ACAS Website: https://www.acas.org.uk/index.aspx?articleid=1361

References

lxxiii Department for Business Innovation and Skills (2015) document. Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/415175/bis-15-200-whistleblowing-guidance-for-employers-and-code-of-practice.pdf

lxxiv Police Scotland website: https://www.scotland.police.uk/keep-safe/festive-safety/

lxxv Study.com https://study.com/academy/lesson/zero-tolerance-policy-in-the-workplace-definition-examples-quiz.html

lxxvi Zerowaste Scotland Website: https://www.zerowastescotland.org.uk/content/who-we-are

Disclaimer

A-Z BUSINESS RESILIENCE COMPENDIUM

Scottish Business Resilience Centre

@SBRC_Scotland Scottish Business Resilience Centre enquiry@sbrcentre.co.uk