sbrcentre.co.uk

# Business Resilience

## Introductory Guide

Scottish Business Resilience Centre

# 1 SMEs - A Background

The SME sector is regarded as the backbone of the Scottish economy. The proportion of SMEs in Scotland is higher than in other areas of the UK, and their importance to the Scottish economy cannot be underestimated.

As of March 2018, there were an estimated 343,535 SMEs operating in Scotland, providing an estimated 1.2 million jobs. SMEs accounted for 99.3% of all private sector businesses in 2018, accounting for 54.9% of private sector employment and 41.5% of private sector turnover.

Within rural areas, SMEs account for a larger proportion of private sector employment than in urban areas. As of March 2018, SMEs accounted for 78.3% of private sector employment in remote rural areas; 69% in accessible rural areas; and 46.4% in the rest of Scotland.

Despite the above, SMEs are more susceptible to failure. Our research has identified the most common reasons why SMEs fail within their first year of operation. These include:

- Monetary concerns - poor record keeping, unrealistic expectations of growth, lack of initial research into pricing and costs, unexpected overheads, tax and insurances.
- Lack of market research - limited understanding of both industry competitors and customer base.
- Insufficient support - lack of mentors or impartial advice from industry experts.
- Location - overlooking the importance of location for business stability and growth.
- Lack of experience - no pre-existing working knowledge of the industry.
- Lack of business plan - inefficient promotion of the commodity through a sustainable business package.
- Poor administration - failure to implement basic administrative requirements or understand time constraints and subsequent impact on tasks.
- Ineffective management - no desire or capability to lead through change or motivate staff effectively.

In addition to the above concerns, there are also risks to SMEs falling victim to various forms of criminality, fire and other disasters that can have devastating and sometimes fatal consequences to the SME operation altogether.

Whilst some of these risk areas are supported through services delivered by other business support organisations, and remain out with the Scottish Business Resilience Centre's remit, focussing specifically at areas of criminality and their perceived threat to SMEs, we know that fraud, specifically cyber enabled fraud, is a key component of critical business failure.

For example, in the first six months of 2018, more than £503 million pounds worth of fraud was committed across the UK. Despite this figure, 75% of SMEs in Scotland have no cyber-fraud preventative measures in place, which is incidentally the highest figure across the UK.

Further research demonstrates that 60% of SMEs who are victims of cyber-attacks will not recover and are forced to close within six months of the attack. The British Continuity Institute also highlighted in its 2018 Horizon Scan Report that both cyber-attack and data breaches were the top two threats to both business continuity and resilience for the third year running.

# 2 The Scottish Business Resilience Centre

The Scottish Business Resilience Centre (SBRC) offers expert advice to SMEs on a broad range of topics, including personal safety and security, physical security, counter terrorism, fire risk mitigation, human trafficking awareness, crime prevention techniques, and cyber resilience.

This guidance relates to enhancing business resilience and can be applied to all companies across the varied spectrum of the SME sector. It provides both general resilience advice, whilst also concentrating on the primary risks identified for new SMEs. These risks can particularly impact on business within the first year of operation.

The guide is intended to provide SMEs with a strong foundation in business resilience, on which to build and expand their knowledge. This will, in turn, afford SMEs a greater chance of developing into a sustainable, profitable enterprise.

# 3 Business Continuity

Business continuity is a method of contingency planning to ensure there is sufficient resilience within a business to allow continued operation during a crisis or other eventuality. This is essential to allow continuity of service provision for customers, whilst protecting a brand from reputational damage.

A business continuity plan ensures long-term survivability following any unplanned, disruptive event, including accidents, fire, criminal activity, or natural disasters. To reduce physical and asset loss, it is of paramount importance that any plan can be instigated as soon as possible after the incident occurs.

This is especially important for a new business to consider, as it can often be overlooked. Businesses can, and do, suffer due to a lack of continuity planning – for example, as many as one in four businesses that experience a serious fire, never recover. This is especially the case for SMEs.

A business continuity plan should be clear, concise, and tailored to each specific business. It should include, but not be limited to, the following:

- Guidance for management
- Identification of business-specific risk
- Prioritisation of key operations which must be maintained
- Designated disaster teams, if appropriate
- A complete inventory of the business
- Instructions for seeking help from other agencies
- An annual review with key personnel
- Employee awareness training
- Contact information for any suppliers who may be impacted
- Detailed plans for managing a loss of IT services

Further information on business continuity can be found on the Ready Scotland website: **www.readyscotland.org**

# 4 10 Steps to Business Resilience Toolkit

One in five businesses suffer a major disruption at some stage of their operations, which inevitably has a detrimental effect on the business. The innovative 10 Steps to Business Resilience toolkit developed by the SBRC is a self-assessment tool which can be used by SMEs to understand their specific risk profile and thereafter create a resilience plan. This will cover key areas of risk such as cyber security, information management and fraud prevention.

The online toolkit consists of a series of questions designed to prompt internal thought about risk and risk appetite. It is quick and easy to navigate, and will provides SMEs with an automated resilience report, detailing proportionate level of operational risk and suggestions for mitigation of those identified risks.

The toolkit can be accessed via the following link:
**http://bit.ly/SBRC10Steps**

# 5 Physical Security: Buildings

For those who trade or work in a physical setting, building security is one of the most important aspects when it comes to ensuring the stability and growth of your business. There are several measures which should be considered in making your building more secure for you, your staff and your customers.

## Doors and windows

In order to be adequately secure against potential break-ins, ensure that all doors on your building 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.

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.

## Insurance

The vast majority of insurance companies now ask that businesses have a specified level of physical security. These specified details are often detailed within your policy; check the small print of your policy and if in doubt, write to your broker before any break in your business experiences. Some insurance companies even offer a discount to secure premises or security surveys to ensure you obtain appropriate advice.

## CCTV

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 is owned predominantly by local authorities and private businesses.

To find out more information about the use CCTV visit the Centre for the Protection of the Na-tional Infrastructure website **https://www.cpni.gov.uk/cctv**

CCTV Advice for Business Premises:
**http://bit.ly/34Z6nK0**

CCTV Advice for Licensed:
**https://www.sbrcentre.co.uk/media/4560/cctv_licensed-1853-psm-16.pdf**

## Alarms

Choosing the right alarm system, whilst quite difficult due to a wide variety of features available, is beneficial. 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.

Essentially, there are two types of alarm systems:

- Remote Signalling
- Audible Only

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

## Remote Signalling Alarms

A monitored alarm system, commonly known as a 'remote signaling' system or 'police call', is monitored by a private central station 24 hours a day.

Upon activation, this alarm system automatically notifies an approved monitoring station, which, on a dedicated line, will inform the police.

Unlike monitored alarms at domestic properties, these alarms at commercial premises do not make any audible sound at the premises for ten minutes. This allows time for police or security personnel to attend and apprehend the trespassers.

This type of alarm is particularly suitable for buildings removed from residents, or where you cannot benefit from natural surveillance or do not wish to depend on the support of neighbouring buildings or individuals.

## Audible Only Alarms

If an individual, either you via a personal attack button or the potential thief, sets off this alarm it will ring instantly outside, whether in a commercial or domestic property. The system relies on an individual hearing the noise from the alarm, as it does not send a signal to a monitoring station or the police.

The cost of this alarm should be for installation only, although you may choose to take out a service and maintenance contract at your own expense.

If you do consider fitting an alarm yourself, you should also be fully competent in working with electricity and ensure that someone else is familiar with the alarm system for the occasions when you are not opening, closing or on the premises yourself. Many individuals prefer to choose an alarm company recognised by their insurance company.

When looking for an alarm and company to install it, business owners should take into account that the police will only attend alarm calls installed by companies that are approved by the two main regulatory bodies:

- National Security Inspectorate (NSI) and the
- Security Systems and Alarm Inspection Board (SSAIB)

Both the NSI and SSAIB publish lists of authorised alarm fitting companies in your local areas.

You can find further information on their websites:

NSI: **www.nsi.org.uk/** SSAIB: **http://bit.ly/2CHJOgx**

Before agreeing the installation of an alarm system, you should consider all aspects of the contract. Check all the details; including whether you own or rent the system, the maintenance contact, the cost, and the ease of use for your employees.

The alarm system you choose should cause no mess to your buildings décor since the wiring will be concealed. Many alarms operate wirelessly, and some alarms can operate by changes in air pressure which only require a free-standing detector unit.

Your neighbours should treat all potential alarm calls coming from your building as genuine, and they should be encouraged to call the police if they see something suspicious, regardless of whether the alarm has been triggered or not.

Remember that your employees who are responsible for opening and closing the premises must be fully conversant with the alarm system you choose. False calls will result in the police withdrawing the alarm response, which may affect your insurance.

Try to avoid false alarm calls; they can cause a loss of credibility with your neighbouring businesses and premises, who, as a result, may stop taking notice of your alarm.
Further advice can be found on the Secured By Design website:

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

## Keys

Akin to exterior doors, consider the strength of the wood in the door and how well the door frame is secured before deciding to fit it with any lock or bolt.

Do not leave any spare keys you may have for your windows or doors lying around your building. All keys that are used in the normal working day should be kept in a dedicated secure cabinet.

Retain a strict control of who borrows keys. It may be appropriate for your business to use only security keys; which can be copied only by a designated locksmith under authorisation.
Do not leave keys in door locks. Doing so makes it easier for unwanted individuals to unlock them and remove larger items from your premises.

## Safes

Check with your insurance company to see if they recommend a particular type of safe; especially if you wish to protect items of high value. Some safes are available to buy cheaply but are very difficult to actually fit. Discuss any needs you may have with a qualified locksmith, who may be able to help you.

Further information can be found on the Physical Security Advice and Measures | CPNI | Public Website. Available here: **https://www.cpni.gov.uk/physical-security**

## Banking procedures and cash in transit

If your business deals with cash transactions, here are some useful tips to ensure you are operating with a secure banking procedure:

- 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.
- Cash should be banked regularly and should not be allowed to accumulate on the premises.
- Due to their vulnerability, inexperienced, hesitant and new employees should not be used to transport cash. You need to carefully choose the right employee to undertake the banking.
- If staff are transporting cash, they are most vulnerable at the start or end of their journey. They should always be alert to suspicious people or vehicles.
- When carrying cash, a secure container should always be used - although it should not draw attention to itself. Where possible, do not use a canvas moneybag. Instead, use either a pocket or specifically designed carry case.
- The time you take and routes you follow whilst transporting cash should vary.
- If your staff are transporting cash on foot, they should always be accompanied. Furthermore, they should use the busiest roads and walk in the centre of the pavement facing oncoming traffic.
- Cash should never be transported on foot if an alternative method is available. With this being said, however, public transport should never be used for cash transport. If a car is being used, a second trusted employee should act as a driver, and accompany the person carrying the cash. Try and use a different car each time you transport cash.
- Ensure that all vehicles used for the transportation of cash are well maintained. All the doors should remain locked and there should be no unnecessary stops. The employees involved in the transportation of cash should not leave the vehicle until they are as close to their destination as possible.

- In the event that staff are attacked, they should surrender the cash they are carrying. They should never try to retaliate.
- Security briefcases, bags and other products designed for the movement of cash are beneficial, and some are available to include smoke, trackers or dye products.
- Car safes can be fitted in the boot of vehicles. Ringbolts can also be fitted to the secure cash carrying equipment.

### 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 on SBRC's website:
**https://www.sbrcentre.co.uk/news/2019/september/how-to-spot-a-counterfeit-note/**

You can also refer to these other links:

Scottish Banknotes:
**https://www.scotbanks.org.uk/polymer-banknotes.html**

Bank of England banknotes:
**https://www.bankofengland.co.uk/banknotes**

Northern Irish banknotes:
**http://bit.ly/34WSwUj**

## 5 Physical Security of IT Equipment

Computers and laptops are often very attractive to potential thieves. The theft of a computer, however, can have far reaching implications for a business. Although the replacement of the hardware itself will be costly, and there will be disruption to the daily business activity until it is replaced, perhaps the overriding problem with theft of a computer is the loss of business data contained within the machine.

Thieves may not always steal the entire computer, instead opting to steal the valuable components within it; such as the RAM, processors and hard drives.

Laptops are a valuable piece of property. They are, however, easily identifiable on being carried in a public place. If laptops must be carried in public view, consideration should be given to disguising this fact by carrying it in a non-distinctive bag or case, making the laptop less identifiable.

Computer accessories, such as printers, may not be as essential to a business, but they are also very appealing to thieves. Leaving these assets in plain view can also attract unwelcome attention.

The file server is the heart of any computer network and is usually critical to core business functions. It is extremely expensive to replace therefore it is worth taking extra precautions to safeguard this particular piece of equipment.

Physical solutions should always be a consideration for any business who wishes to protect their IT equipment. There is a vast array of options available to safeguard equipment. These range from low-cost, easily obtained solutions such as lockable cases, security screws and cable ties, to more high-tech options such as lock down plates, entrapment devices, security cabinets, and a variety of alarm systems.

Network monitoring can also be implemented if there are numerous computers used within the business.

## 6 Cyber Resilience

Cyber-crime, or computer-oriented crime, is generally understood as crime that involves a computer and a network. Computers can either be used in the commission of a crime (cyber-enabled crime) or they can be the direct target (cyber-crime) but both are becoming increasing commonplace, as technology advances and more businesses move towards a virtual presence.

A survey of 1000 SMEs across the UK found that poor password management was the main area of risk for businesses. SMEs need to consider the level of system access which is permitted on computer systems for all employees. This should lessen the possibility of unauthorised persons within an organisation accessing confidential information or carrying out an act of criminality via the business network.

Effective cyber resilience should incorporate a variety of measures that are used to detect, deter and delay any attack from occurring. The cyber security measures for a business should form part of a multi-layered strategy that includes physical security and personal security. All businesses rely on the availability, confidentiality and integrity of data in order to maintain the day-to-day distribution of services; therefore, cyber resilience is a necessity for every business.

There is a wealth of information available for businesses who wish to improve their cyber resilience. For example, The National Cyber Security Centre provides an online cyber resilience training package. This is free of charge, easy-to-use, and can be completed in under 30 minutes. It explains the importance of cyber resilience training and also demonstrates how cyber-attacks can be carried out. It then covers four key areas of cyber resilience, namely:

- Defence against phishing and spear-phishing
- How to secure all types of devices
- Creation of strong passwords
- How to report incidents

The training can be applied to any business and/or organisation within the SME sector. It has been deliberately designed for individuals who have little knowledge of cyber security and contains tips which can complement any existing policies and procedures already in place. The training package can be accessed via the following link:

**https://www.ncsc.gov.uk/blog-post/ncsc-cyber-security-training-for-staff-now-available**

## Cyber Essentials

Cyber Essentials is a simple and effective Government-backed scheme, supported by industry experts, that will help protect your organisation against a range of the most common internet borne cyber-attacks. Cyber-attacks come in many shapes and sizes, but the vast majority are very basic in nature and can be prevented.

The scheme has been carefully designed to guide organisations of any size in protecting themselves against cyber threats which include malware, ransomware and phishing, through the use of five technical controls and implementing basic cyber hygiene. It offers two levels of certification, Cyber Essentials (basic) and Cyber Essentials Plus which provides a greater level of assurance following additional verification of your cyber security by independent professionals.

For more information on Cyber Essentials visit: **http://bit.ly/54356ce**

The following organisations can provide further information on cyber resilience:

The Scottish Business Resilience Centre
**https://www.sbrcentre.co.uk/services/cyber-services/**

Police Scotland
**https://www.scotland.police.uk/keep-safe/keep-secure-online/cybercrime**

Online safety for businesses with Get Safe Online
**www.getsafeonline.org**

The Advisory, Conciliation and Arbitration Service offer the following advice on their website
**http://www.acas.org.uk/index.aspx?articleid=3375**

The National Business Crime Centre – Little book of big scams
**http://bit.ly/2KlMRzo**

The National Business Crime Centre – Little book of cyber scams
**http://bit.ly/351Mcea**

The National Business Crime Centre – Little leaflet of cyber mistakes
**http://bit.ly/33M5AvN**

The National Cyber Security Centre
**https://www.ncsc.gov.uk/**

The National Crime Agency
**https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime**

Centre for the protection of the national infrastructure
**https://www.cpni.gov.uk/cyber-security**

# 7 Fraud

Every year, tens of millions of pounds are lost in the UK as a result of fraud. Scotland's SMEs, however, are less likely to be targets of fraud when compared to the rest of the UK; where the national average is 44%.

**Despite this, 31% of SMEs in Scotland surveyed said they had been targeted by fraudsters, of which one in five fell victim.**

Fraud is the use of deception with the intention of either obtaining personal gain, avoiding an obligation, or causing loss to another party. The term 'fraud' covers a wide variety of dishonest behaviour: including forgery, false representation and the concealment of material facts. Scotland also has the offence of 'uttering', wherein a person presents a fabricated writing falsely intended to pass as the genuine writing of another.

The impact of fraud on a business cannot be underestimated. If a business falls victim to fraud, it could suffer serious financial loss, damage staff morale, cause disruption to daily business function and generate adverse publicity for the business.

Businesses must be aware of the risk of fraud and ensure policies and procedures are implemented to prevent and detect this type of crime. Fraud is usually committed due to a lack of sufficient security procedures, whereby access to assets and information can be freely gained at any given opportunity.

CEO fraud and mandate fraud are particularly damaging to SMEs, as they can severely impact the cash flow of a business. CEO fraud involves the impersonation of a senior company executive in order to divert payment for goods and services into a fraudulent bank account.

Fraudsters will typically target the finance department of a company, either via email or by telephone. This type of fraud is more typical in larger SMEs, with CEOs under the age of 25 more likely to be targeted.

Mandate fraud is similar; however, this is where a business is deceived into changing a regular payment mandate such as a direct debit or standing order and payments are then rerouted into a fraudulent bank account. More information on mandate fraud can be found at the following link:

**http://bit.ly/2Of90jS**

Further advice on all aspects of fraud prevention can be found on the Police Scotland website, at the following link:

**http://bit.ly/2XclwVu**

# 8 General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) came into force on the 25th May 2018. GDPR will continue to apply to the UK after the Brexit process is complete and the UK formally leaves the European Union. This will allow for continued collaboration in terms of business between the UK and the EU.

A reform of data protection law in Europe was instigated due to the increased use (and abuse) of sensitive personal information. This reform has transferred the control of personal data – removing it from the organisations that collect, analyse and use such data; and returning control to the individuals to whom the personal data belongs.

All SMEs that handle personal sensitive information, must consider what actions need to be taken in order to protect that data under the GDPR legislation. The key changes outlined in the legislation include:

- Increased rights of access to an individual's personal data, as well as portability and deletion
- Organisations being held more accountable for what, why and how they process information
- An increase in fines for data breaches

It is now mandatory to report significant breaches of data to the Information Commissioner within 72 hours of being made aware of the breach. This is especially relevant if the breach is likely to result in a risk to people's rights and freedoms.

A breach of customer data could result in penalties of up to £20 million, or 4% of turnover, depending on which is higher. GDPR must be regularly reviewed to ensure that any business remains compliant with the new legislation.

Public sector organisations are now required to 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.

The ICO has created a Data Protection Toolkit for SMEs which can be used to ensure that a business is GPDR complaint. This can be accessed via the following link:

**http://bit.ly/2QhsdUD**

# 9 Insider Threat

Insider threat can be accidental or malicious and is not restricted to cyber-related crimes. This type of criminality arises as a result of actions by employees trusted to manage some aspect of the business.

These employees will exploit their legitimate position within a company and will ultimately be responsible for losses against the business. These offences can be committed by employees at any level within an organisation.

Generally, there are three different categories of insider threat:

- Deliberate insider - individuals who obtain employment for the sole purpose of deliberately abusing the access they are given by a business
- Volunteer/Self-initiated insider - individuals who obtain employment for genuine reasons, but who at some stage personally decide to abuse their access to the business. This can also refer to a careless employee who fails to adhere to policies and procedures for risk mitigation.
- Exploited/Recruited insider - vulnerable employees who are being exploited or recruited by a third party to provide information on the business. These individuals are more susceptible to either exploitation or recruitment by criminals due to a stressful component of their lifestyle, such as a secret addiction, crippling debt or previous criminal activity.

Despite the risk of insider threat, many businesses demonstrate weakness in the creation of policies regarding recruitment and dismissal of staff. This leaves a business potentially vulnerable to infiltration by criminals. Recruitment processes should be stringent and designed to deter criminals from applying for roles within the business.

A robust vetting system should be implemented, with consideration given to disclosure checks. Referees should always be contacted to confirm that they know the applicant, and to verify the information provided, which should also assist in detecting any potential criminals.

More information on the risk of insider threat can be found on the following websites:

**http://bit.ly/2QsPZ0n**

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

10

# Fire Safety Awareness and Risk Mitigation

Fire does not discriminate and the potential for a fire situation to occur and develop can happen at any time. However, an effective fire safety strategy and good management attitude can considerably reduce the risk of fire affecting your staff, customers, premises and business.

There are a number of legal obligations placed upon the 'duty holder' of a premises under the Fire (Scotland) Act 2005 which must be maintained.

Effective planning and preparation can have a hugely positive impact on increasing your business resilience and keeping everyone within your premises safe. Non-domestic premises present some unique, potential fire safety risks. The following guidance and advice should assist you in that pre-planning and preparation.

Ensure you have carried out a Fire Safety Risk Assessment (FSRA) for your premises. If you have five or more employees, you must document and record the findings of the FSRA. It should be reviewed regularly, including when any changes occur that could impact upon fire safety within your premises.

Testing and maintenance of fire safety measures should be carried out at the appropriate intervals and it is good practice to document and record the details. Your Automatic Fire Detection (AFD) system should be tested weekly and serviced by a competent person on a six-monthly basis. Ensure this is appropriate for use - don't have detectors incorrectly located or use the wrong type of detector.

The use of multi-sensor detection can significantly reduce instances of false alarms within your premises. Other items such as fire extinguishers, fire doors and emergency lighting should also be part of a testing regime.

Staff should be trained in what actions to take in the event of a fire. This training should be refreshed regularly as well as documented and recorded. Staff should also take part in regular fire evacuation drills which should also be recorded. It's also beneficial to carry out a short debrief after a drill to discuss what went well or any issues arising from the drill.

For more information on Fire Safety guidance and legislation, visit: **http://bit.ly/34YbLNk**

## Unwanted Fire Alarm Signals

Ask your local legislative fire safety enforcement officer for information on our 'TAKE 5' and 'Be Aware' UFAS/false alarm activation reduction initiatives. Find out more:

**http://bit.ly/32Kg7pV**

11

# SBRC and helping SMEs

At the Scottish Business Resilience Centre (SBRC) we work with SMEs to help them become more resilient and raise awareness of potential threats which could cause a devastating impact to their business. If you'd like to learn more about SBRC's work visit, www.sbrcentre.co.uk or send one of our team an email at enquiries@sbrcentre.co.uk

## Other useful organisations

- **The Scottish Business Resilience Centre** - **https://www.sbrcentre.co.uk**

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

- **Association of Convenience Stores** - **https://www.acs.org.uk**

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

- **Federation of Small Businesses** - **https://www.fsb.org.uk**

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

- **The Health and Safety Executive** - **http://www.hse.gov.uk/scotland/**

For a variety of advice and guidance in the workplace relevant to health and safety.

- **National Federation of Retail Newsagents** - **https://nfrnonline.com**

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

- **Scottish Grocers Federation** - **http://bit.ly/sgf324**

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.

- **Scottish Enterprise** - **http://bit.ly/scotenterprise**
- **Secured By Design** - **https://www.securedbydesign.com**

SBD is a police initiative that improves the security of buildings and their immediate surroundings to provide safe places to live, work, shop and visit.

- **National Fire Chiefs Council (NFCC)** - **https://www.nationalfirechiefs.org.uk/**

The National Fire Chiefs Council is the professional voice of the UK fire and rescue service. NFCC drives improvement and development throughout the UK FRS.

## Acknowledgement

We'd like to thank Greater Manchester Police for their assistance in the development of this guide.

## Appendices

- SMEs in Scotland:

**https://www2.gov.scot/Topics/Statistics/Browse/Business/Corporate/KeyFacts**

**http://bit.ly/2rI9asJ**

- Reasons for failure of business start ups:

**https://www.forentrepreneurs.com/why-startups-fail/**

**https://techround.co.uk/business/why-start-ups-fail-in-the-uk/**

**http://bit.ly/2NMuvK5**

- Fraud in Scotland 2018:

**https://www.insider.co.uk/news/smes-fraud-barclays-scotland-percentage-12420191**

- Cybercrime:

**https://fleximize.com/articles/011275/cyber-threats-facing-smes**

**http://bit.ly/2CGZDnI**

**http://bit.ly/34Yr1Ke**

- Financial fraud:

**http://bit.ly/2CRcaFv**

**https://www.ukfinance.org.uk/wp-content/uploads/2018/09/Fraud-Report-FINAL.pdf**

# Disclaimer

This material has been compiled for general information purposes only. Whilst every effort has been made to ensure that the information is accurate; no warranty, express or implied, is given as to its accuracy, and the SBRC do not accept any liability for error or omission. The information reflects a wide range of experiences and may not be suitable for everyone. Any decision to follow the advice contained in this material lies with the individual. The SBRC cannot guarantee that following the advice will lead to any reduction in crime or increase in resilience and shall not be liable for any damage (including, without limitation, damage for loss of business or loss of profits) arising in contract, delict or otherwise from the use of, or inability to use, material contained in it, or from any action or decision taken as a result of using this material.

This material includes links to third party websites over which the SBRC has no control. Any link made to or from a third-party website is made at the own risk of the individual. Any use of the third-party website will be subject to, and any information provided will be governed by the terms of that website, including those relating to confidentiality, data privacy and security. The SBRC are not responsible or liable for the goods and services offered by any third party mentioned in these materials nor does the SBRC endorse or approve or make any warranty, representation or undertaking relating to the content of any third party website to which any individual may link through these materials.

In particular the SBRC disclaim liability for any loss, damage and any other consequence resulting directly or indirectly from or relating to an individual's access to any such third party website or any information that may be provided or any transaction conducted on or via the third party website or the failure of any information, goods or services posted or offered at the third party website or any error, omission or misrepresentation on the third party website or any computer virus arising from or system failure associated with the third party website.

Scottish Business
Resilience Centre

Oracle Campus
Blackness Road
Linlithgow
West Lothian
EH49 7LR

☎ 01786 447 441
✉ enquiries@sbrcentre.co.uk
www.sbrcentre.co.uk
@SBRC_Scotland

A Company Limited by guarantee and registered in Scotland
No. SC170241 | VAT Registration Number: 717 2746 27