Ready for anything

Building your business resilience for the unexpected

Let's go forward

BARCLAYS

Contents

Introducing resilience to your business

Would you be ready if extreme weather, a cyber attack or terrorism disrupted your business?

Small and medium-sized businesses are often the most vulnerable to these types of threats. Issues affecting staff, customers and suppliers, or utilities and transport can have a severe impact on the success of a business.

SMEs have a lot to juggle, but alongside cashflow, recruitment and staff issues, the risks of disruptions from cyber crime, natural hazards and civil emergencies have become more important to think about than ever.

> "Disruptive events can happen anywhere, at any time, from natural disasters to cyber crime. Taking time to plan and prepare your business can save you time and money when something untoward happens. Business Emergency Resilence Group (BERG) is helping small business owners create resilience and recovery plans that will help guarantee future prosperity. Be resilient. Be prepared."
>
> **Lee Webb,** Director, Group Resilience, Barclays

Business owners often say they can't afford to spend time and money building resilience against risks, or that they are already doing enough to protect themselves. This mindset can be one of the biggest barriers to being prepared. Many SMEs also underestimate how long it would take to get back up and running if they were hit by an unexpected event.

Fewer than

one in five

(17%) SMEs has assessed their exposure to rising UK security threats, despite 44% expecting to face some kind of threat in the next 12 to 18 months.*

68%

of SMEs claim to be resilient to security crises, yet nearly half (43%) admit to having no business continuity, disaster recovery or crisis management plans in place.*

*Source: Arthur J. Gallagher – Understanding Security Risks report, 2017.

Taking action

While you can never protect your business from all the risks in today's world, you can certainly become more resilient to them. Business resilience needs to be firmly on the management agenda, as doing nothing can have serious consequences.

Fortunately, there are lots of worthwhile actions that can make your business more resilient and help you prepare for events that might jeopardise your future success.Taking time to plan and prepare your business can save you time and money when something unexpected happens.

We've produced this guide in partnership with Business in the Community's (BITC) Business Emergency Resilience Group (BERG), to raise awareness of resilience planning and to help your business get to grips with preparing for the unexpected.

This guide discusses the types of threats your business might face and how you can prepare for them. It includes lots of straightforward, practical steps you can take to lessen the impact on your business, as well as reducing insurance premiums and claims.

A successful business is ready for anything.

Identifying the threats to your business

To make your business more resilient, the first step is to think about some of the threats you may be vulnerable to and how they could impact your business.

Cyber attacks

Cyber crime hit **52%** of UK businesses in 2016, costing almost **£30 billion.**[1]

Supplier failure

75% of UK businesses experience at least one incident that disrupts their supply chain each year.[9]

Terrorism

Terrorist incidents in the UK are on the rise. They are not only a threat to lives but can cause major disruption to your business.

Criminal or industrial explosions

from gas pipelines or toxic chemical storage can cause damage to premises or prevent access to buildings.

Fraud

Scams that target small businesses are on the increase. The private sector lost an estimated **£144 billion** to fraud in 2016.[2]

World events

Political or economic events in other parts of the world can cause disruption to exchange rates, trade and financial transactions.

Power cuts

Technical failure or severe weather can cause loss of power at any time, without warning.

66% of UK manufacturers are vulnerable to this.[5]

Extreme weather

Nearly **60%** of UK businesses have no plans in place to deal with extreme weather.[3]

Flooding

Since 1998 there has been at least one serious flood every year.[4]

Illness and staff absence

An estimated **137.3 million** working days were lost due to sickness or injury in 2016.[7]

IT and Telecoms outages

British businesses suffered **3 DAYS'** internet downtime on average in 2016.[6]

Travel disruption

Industrial action or severe weather can disrupt road and rail networks. By 2030 this could cost the British economy as much as **£307 billion.**[8]

[1]www.beaming.co.uk/press-releases/cyber-security-breaches-cost-businesses-30-billion [2]www.nao.org.uk/wp-content/uploads/2017/06/Online-Fraud-Summary.pdf [3]Federation of Small Businesses and Climate Ready at the Environment Agency [4]Environment Agency: A guide to preparing your business for flooding. [5]Barclays Energy Resilience report, 2016 [6]https://www.beaming.co.uk/press-releases/british-businesses-lost7billion-internet-outages-2016/ [7]https://www.ons.gov.uk/employmentandlabourmarket/peopleinwork/labourproductivity/articles/sicknessabsenceinthelabourmarket/2016 [8]Centre for Economics and Business Research, Economic effect of UK road investment, February 2017 [9]Business Continuity Institute Supply Chain Survey.

Be prepared: protecting your people

Although there are numerous threats that could affect your business, there are many simple measures you can take to become better prepared. This includes looking at the resilience of your people, premises, suppliers and IT systems.

Develop a communication plan:

1. Make a list of employees' contact details and think about staff who may need special assistance in the event of an evacuation
2. Keep staff, customers and suppliers up-to-date about any disruption
3. Think about how you would communicate if staff needed to work securely from home or from another location
4. Monitor transport updates and check your local council's winter resilience plans, including which roads they will grit.

Small businesses are particularly vulnerable to staff absence, so it's vital to have well-tested systems in place that will allow you to carry on in the event of illness, travel difficulties or an incident affecting your premises.

Train staff to deal with disruption:

1. Ensure your staff understand their colleagues' job roles to cover for absences
2. Consider health and safety training for staff, including first aid
3. Brief your staff on evacuation routes, flood plans, chemical plans, safe spaces and how to secure your premises
4. Create a checklist of safety procedures to adopt in an emergency and ensure staff are fully briefed on what to do
5. Put security measures in place and make sure your staff understand them and their part in making them work
6. Show your staff the Government's 'Stay Safe' **video** for advice on what to do in the event of a weapons attack.

Be prepared: protecting your premises and supply chain

Safeguarding your premises

Business premises and equipment are vulnerable to a range of threats, from extreme weather and power outages to terrorism and industrial incidents.

Plan how you control access to your premises and whether you need to install CCTV.

Consider the risks to your premises:

- Work out where you are most vulnerable to decide on the level of security you require, plan how you control access to your premises and whether you need to install CCTV
- Check your flood risk, create a flood emergency plan and install flood protection products and flood-resistant materials if necessary
- If your premises are accessible to the public, think about measures you could take to minimise the risk of an attack, such as removal of waste bins or bag searches
- Think about where you could operate from if you couldn't access your premises.

Prepare for emergencies:

- Protect your business against crime, vandalism or unrest by testing fire alarms every week
- Make sure your security system has an uninterruptible and regularly tested power supply
- Store key documents, emergency plans, and contact information for staff, emergency services, customers and suppliers in a safe place
- Make sure your physical assets can be stored above flood level and identify anything that may need special protective measures
- Know how to shut off your gas, electricity and water supplies, and keep a contact list of your suppliers on a hard copy in a safe place. Make copies of your contacts, in case one record fails
- Keep mobile phones, laptops and tablets fully charged
- Put together an emergency kit, including a battery-operated or wind-up torch and radio.

Supplier resilience

Your suppliers are just as vulnerable to unexpected threats as your own business. Understanding your supply chain and developing resilience to any weaknesses can help you react more quickly to adverse events and could even give you an advantage over your competitors.

Understand the importance of your key suppliers:

- Be aware of how much you depend on your suppliers to run your business. Look at your most profitable product or service and the potential profit impact if the supplier failed
- Think about how you will keep customers up-to-date in the event of supplier failure.

Build resilience into your supply chain:

- Think about diversifying your suppliers and reassess contracts when they are renewed
- Consider using suppliers that operate from multiple or low-risk locations
- Discuss your contingency plans with your suppliers and assess the effectiveness of their own business continuity plans
- Find out more about how Cyber Essentials certification can help demonstrate that you and your supply chain take cyber security seriously.

Understanding your supply chain and developing resilience to any weaknesses can help you react more quickly to adverse events.

Be prepared: beating the fraudsters

Cyber security

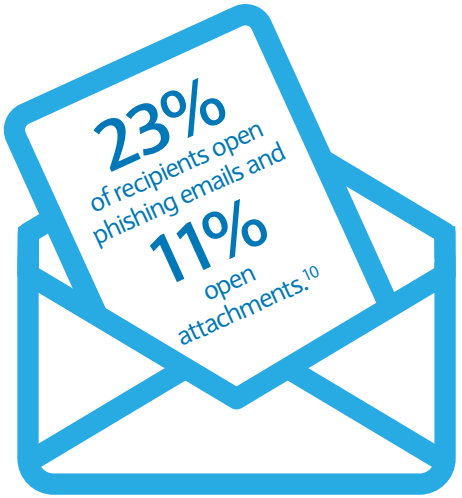
If you use IT systems to sell, deliver your services, manage your finances or communicate with customers you could be an easy target for cyber criminals. Lack of cyber security poses a threat to your profitability, cashflow and reputation. Our Digital Eagles are on hand to support if you would like to talk about how the following applies to your business.

Back up your data:

- Take regular backups of your important data and test whether it can be restored, and how long this takes
- Ensure the device containing your backup is not connected to the device holding the original copy, neither physically, nor over a local network
- Consider backing up to a secure and legally compliant cloud server so that your data is stored in a safe location and you are able to access it quickly from anywhere.

Prevent malware damage:

- Install approved antivirus software on all computers and laptops
- Make sure that all software and operating systems are updated regularly to protect against known threats. Turn on automatic updates where possible
- Control access to removable media such as SD cards and USB sticks
- Consider disabling ports or limiting access to unreliable media and encourage staff to use secure file transfer methods instead. Remember that emails are unsecure, so when sending sensitive data make sure it is encrypted.



Avoid phishing attacks:

- Make sure staff are aware of scams, such as emails asking for sensitive information like bank details or containing rogue links
- Ensure staff don't browse the web or check emails from an administrator account to reduce the impact of an attack
- Watch out for emails that offer financial rewards, ask you to act urgently or use scare tactics
- Check that you know the person or organisation sending an email – make sure the email address is legitimate and not trying to mimic someone you know
- Look out for emails and websites containing poor spelling or grammar, or low quality versions of logos
- Be wary of clicking on links or entering details on login pages – if it looks suspicious, it is best to delete or mark as junk mail.

Take care when using mobile devices:

- Switch on the PIN or password protection and recognition on all smartphones, laptops and tablets
- Configure devices so they can be tracked, remotely wiped or remotely blocked
- Do not connect to public Wi-Fi hotspots when sending sensitive data – use 3G, 4G or VPN instead, and check that your devices are not automatically connecting
- Replace devices that are no longer supported by manufacturers.

Use strong passwords to protect your data:

- Avoid predictable passwords, such as family and pet names that can be found easily, and common passwords that can be easily guessed such as passw0rd
- Make passwords as long as possible – at least eight characters and a combination of letters, numbers and symbols, or use a memorable sentence or phrase
- Do not reuse passwords on different sites
- Consider the use of a password manager to securely store passwords
- Get protection beyond passwords, such as two-factor authentication
- Make sure all devices use encryption products that require passwords and that security measures, such as passwords or fingerprint recognition, are switched on
- Control access levels across your workforce, ensuring staff only have access to information necessary for their roles.

[10]Data Breach Investigations Report.

Insurance – are you covered?

Although you can take various steps to make your business more resilient, unforeseen events may still occur. The only way to protect your business against loss of stock or damage to buildings is through insurance.

Check your insurance

Consider your insurance limits, excess and coverage terms and conditions; read the small print and ensure that the coverage is sufficient for your needs. On top of your mandatory insurance requirements (such as public liability and employment insurance), make sure you are also insured against threats that could impact your business, including extreme weather and flood damage, business interruption and lost revenue, cyber crime fraud and other losses.

Respond quickly

Call your insurance company as soon as possible after an incident. Make sure you know what information your insurer will require to support a claim. Take photos and video as evidence of any loss or damage.

Think about using a loss adjuster

You can appoint your own Chartered Loss Adjuster to look after your interests as a claim proceeds, prepare the claim and negotiate settlement on your behalf.

To discuss your insurance, please call 0330 102 1849,* arrange a call back or visit us at barclays.co.uk/business-banking/manage/business-insurance

Responding to an emergency

There are many sources of advice and support for businesses in the event of a serious disruption, including the emergency services, local authorities, local resilience forums, regional resilience partnerships and the voluntary sector.

Remember that it can take several months to get your business back on its feet after a major disruption, and don't underestimate the emotional stress on your staff and their families who are affected by a crisis.

Immediately after an incident there are a number of actions you could take:

1. Call 999 if people or property are in danger
2. Assess the impact on your business and how long it will last
3. Contact your insurance company and record photos and videos as evidence of any loss or damage
4. Contact staff, suppliers and customers to let them know what has happened
5. If you are comfortable that it would work for your business, consider using social media to share information about the disruption
6. Identify what business activities can continue and which may need to be put on hold
7. Speak to neighbouring businesses to see if they can help
8. Contact your local council to see what help it can offer.

*Calls to 03 numbers use free plan minutes if available; otherwise they cost the same as calls to 01/02 prefix numbers. Calls may be monitored or recorded in order to maintain high levels of security and quality of service.

Case study: Vivida Productions

Simeon Quarrie, owner of Vivida Productions, a visual storytelling business using video as well as virtual and augmented reality, recalls an IT failure in the early days of his business that threatened its survival.

Learning the hard way

Early on in the business, Vivida Productions mainly produced high-end videos of weddings and other family events. Simeon Quarrie recalls: "My team was working away on video edits when our hard drives suddenly went down. Initially we didn't panic because we knew we had backups off-site. But when we tried to use the backups they went down too."

"It's really important that businesses focus not just on growth but on what could go wrong."

It turned out that the servers were exceeding their recommended operating temperature during a heatwave, due to lack of ventilation. Fortunately, the company had another backup of the source data, but still lost a lot of work. "I had to pay my staff overtime to get the business back to where it had been. It had a huge impact.

> "The incident could have been devastating for our reputation and pipeline of new business, as well as financially if we'd had to refund clients."

"The incident could have been devastating for our reputation and pipeline of new business, as well as financially if we'd had to refund clients. And there is the impact on staff morale of having to repeat completed work.

"I think it's really important that businesses focus not just on growth but on what could go wrong. Keep looking for potential weaknesses in your business and be prepared. We've learned that you need to be aware of the limitations of the technology your business depends on."

The company has since invested in sophisticated hard drives with built-in analytics that can be rebuilt in a matter of hours and makes sure it provides source data files to clients, as well as using cloud backup for all its documentation. It is also vigilant about planning for hot weather and has increased its insurance cover.

Having survived and recovered from the incident, the business has since doubled in size and business resilience has become a factor in winning bigger contracts. "We've learned our lessons and emerged as a stronger business, trusted by some of the biggest brands in the world for our visual storytelling," says Simeon.

VIVIDA

Simeon Quarrie
Owner of Vivida Productions

Case study: Glorious Spa

Stephanie Ridge, owner of Glorious Spa, a chain of high-street spa and beauty salons in West Sussex, explains the lessons she has learned about resilience and preparing for emergencies after suffering a flood to her premises.

Planning for the unexpected

Stephanie Ridge opened Glorious Spa in 2010 in Chichester. She now has three salons in West Sussex, with a fourth on the way and a training school launching in 2018.

In late October 2013 the ground floor of the salon was flooded following flash storms, and Stephanie had to close for three days. She explains: "The electrics were compromised, and we had to repaint and refurbish. It was chaotic, and it cost us a lot of money. Cashflow was vital as we'd opened during the recession and sunk every penny into the business.

"At the time we had just one shop so it was our only source of income, and we had a substantial payroll to meet. It was also the last busy week before November, which is the quietest time of year for us as people are saving for Christmas. It was a major incident for us."

> "We've grown our social media presence so we can communicate quickly with customers, and we have a directory of tradesmen who we trust and who would be ready to assist in emergencies."

After the flood, Stephanie worked with Barclays to improve the company's emergency plan and make sure it is easy to put into action.

"We now have an up-to-date list of staff phone numbers, contact details for neighbouring shops and our booking system is online so all the senior team have access to it," she says. "We've also grown our social media presence so we can communicate quickly with customers, and we have a directory of tradesmen who we trust and who would be ready to assist in emergencies.

"I would always advise other businesses to make sure they have a robust plan in place to contact tradesmen, staff and, of course, customers."

the glorious spa company

Stephanie Ridge
Owner of Glorious Spa

Case study: in Your Face Advertising

Arthur Chirkinian, founder and CEO of in Your Face Advertising (iYFA), explains what he has learned about making his business more resilient to cyber crime from his involvement in Barclays B:Resilient events.

Be resilient and carry on

Launched in 2015, iYFA offers businesses a new platform to advertise their products or services in an eco-friendly way to their local community. Arthur explains: "Companies can use our custom-built online software to design and create adverts and promotions that can be put on ecologically sustainable eBins and eBags."

"The B:Resilient events have been incredibly helpful and inspiring."

Having been invited to a B:Resilient event on cyber security for SMEs, iYFA has since attended several other events, which Arthur says have also been useful for networking with other SMEs, as well as showcasing the company's products.

"The B:Resilient events have been incredibly helpful and inspiring. Cyber crime is a key threat for us, and we've already had two hacking attempts against our website.

> "We understand that building resilience is critical to our growth. Whether it's fire, flood or cyber threats, it's important to take steps to prepare yourself."

But we managed to successfully protect ourselves and our customers' data from the attacks by applying what we had learned at these events."

In 2017, the company was a finalist in BITC's Barclays Award for Building Resilient Business.

The company now has two backup cloud servers, customer data is secured using SSL certificates and they have a self-healing cloud infrastructure, which is monitored round the clock.

A keen believer in businesses building their resilience, Arthur says: "Our eProducts not only carry advertising from local businesses, they also promote the work that BITC and Barclays is doing to further promote resilience in local business communities.

"As a start-up, we understand that building resilience is critical to our growth. Whether it's fire, flood or cyber threats, it's important to take steps to prepare yourself. Be resilient and carry on is our motto – a resilient business means staying in business."

iN YOUR FACE ADVERTISING

Arthur Chirkinian
Founder and CEO of in Your Face Advertising

Business Emergency Resilience Group's 10-minute plan

BERG's 10-minute plan is designed to help small to medium-sized businesses prepare for, respond to and recover from emergencies, such as flooding, cyber crime and civil unrest.

Take 10 minutes to help prepare your business:

1 Emergencies

Consider the following impacts on your business	High	Med	Low
Access to site and premises is prevented, possibly for an extended period of time			
Disruption from external events such as a terrorist incident, flooding or a fire			
Critical equipment fails or a major supplier goes out of business			
Loss of electricity, water or gas			
Disruption to key transport networks			
Key staff are absent at the same time			
Burgled or vandalised office			
IT and telecommunications outages			

2 Plan ahead

What could you do to protect your business?	Yes	No
Check live alerts – sign up for Environment Agency and cross-sector safety and security messages		
Follow the advice on the official National Counter Terrorism Security Office (NaCTSO) website		
Download the British Red Cross Emergency app		
Check your flood risk on the Environment Agency website		
Show the government's 'Stay Safe' video to your staff for advice on what to do in the event of a weapons attack		
Consider how you might secure your premises to keep your staff and customers safe inside, and can you provide food, water and access to toilets?		
Consider insurance limits – excess and coverage terms and conditions, watch for small print and underinsurance		
Understand your site – evacuation routes, flood plans, chemical plans and safe spaces		
Consider back-up utilities – energy, water and communications		
Create checklist for new starters and leavers – new passwords, access codes, keys and emergency procedures		
Follow data protection guidance. Backup computers and key documents – keep copies safe/offsite		
Undertake weekly security checks – IT/fire alarm/safety system/burglar alarm		
Ensure staff understand colleagues' job roles to cover for absences		
Consider health and safety staff training, including first aid and Met Police Project Griffin training		
Create a contact list of current and alternative suppliers		
Check the Centre for the Protection of National Infrastructure (CPNI) website for information and advice on physical security, personnel security and cyber security		
Share resilience plans and identify ways to support neighbouring businesses		

3 Capture Business Emergency Contacts

How should you communicate?	Yes	No
Capture Business Emergency Contacts		
Detail important information and contacts, including staff, emergency, customers and suppliers		
Regularly communicate your plan to staff and ensure they have management's contact details		
Regularly review and update contacts (every three to six months)		
Keep contacts in a safe place/offsite		
Regularly test and check key elements of the plan (every three to six months)		
Create an emergency 'grab bag' – key documents, plans and contact details		

Useful contacts

Emergency

- **BERG**
  Offers practical help for businesses during a crisis and in the recovery period in the form of goods, services and advice.
  www.bitc.org.uk/berg/prepare
- **British Red Cross**
  Supports the police, ambulance and fire services, local and health authorities and utility companies to help those most affected by UK crises.
  www.redcross.org.uk
- **The Samaritans**
  Has a team of volunteers trained to provide emotional support in response to an emergency.
  www.samaritans.org

Insurance

- **Barclays**
  Working with Allianz, one of the UK's leading insurance providers, to help small businesses design insurance cover to suit their specific needs.
  www.barclays.co.uk/business-banking/manage/business-insurance
- **The Chartered Institute of Loss Adjusters**
  Can help you find a suitable loss adjuster.
  www.cila.co.uk

Cyber crime and fraud

- **Cyber Essentials**
  Cyber Essentials certification allows your organisation to advertise that it meets a Government-endorsed standard.
  www.cyberaware.gov.uk/cyberessentials
- **National Cyber Security Centre (NCSC)**
  A part of GCHQ, NCSC is the UK's authority on cyber security. Further guidance for small businesses can be found on their website.
  www.ncsc.gov.uk
- **Action Fraud**
  The UK's national fraud and cyber crime reporting centre.
  www.actionfraud.police.uk

*Calls to 03 numbers use free plan minutes if available; otherwise they cost the same as calls to 01/02 prefix numbers. Calls may be monitored or recorded in order to maintain high levels of security and quality of service.

Extreme weather

- **The Environment Agency**
  Provides lots of information, warnings and advice on floods.
  www.gov.uk/flood and a 24hr Floodline is 0345 988 1188*
- **The National Flood Forum**
  Has advice for before, during and after flooding.
  www.nationalfloodforum.org.uk
- **The Association of British Insurers**
  Produces a guide to resistant and resilient repair after a flood.
  www.abi.org.uk
- **Aviva**
  Gives guidance on what to expect, who can help and where to start with cleaning up.
  www.aviva.co.uk/news-and-guides

Terrorism and world events

- **The National Counter Terrorism Security Office**
  Provides information on preparing for a terrorist attack, with detailed information on protecting your business's assets.
  www.gov.uk/government/organisations/national-counter-terrorism-security-office
- **The Centre for the Protection of National Infrastructure (CPNI)**
  Website gives advice on physical security, personnel security and cyber security.
  https://www.cpni.gov.uk

Illness and staff absence

- **Government information and advice on flu pandemics**
  www.gov.uk/guidance/pandemic-flu
- **NHS England**
  Has produced an operating framework for managing the response to pandemic influenza.
  www.england.nhs.uk/ourwork/eprr/pi/
- **Highways England**
  Has information on traffic disruptions.
  www.highways.gov.uk

Supplier resilience

- **The Business Continuity Institute (BCI)**
  Runs supply chain resilience courses and produces the Supply Chain Resilience Report, which tracks the origins, causes and consequences of supply chain disruption.
  www.thebci.org/

Key takeaways

- Think about some of the threats you may be vulnerable to and how they could impact your business. Filling in BERG's 10-minute plan (page 12) is a great way to begin
- If your business could be hindered by staff absence, it's vital to have well-tested systems in place that will allow you to carry on in the event of illness, travel difficulties or an incident affecting your premises
- Plan how you control access to your offices, and how you can protect your technology and locations from all instances – whether that's as common as a power outage or something more severe like weather damage
- Evaluate any dependencies in your supply chain and identify contingency plans for any weaknesses that could arise
- Cyber crime is on the rise, so it's important for all businesses to be prepared. Following the five quick and easy steps on page 7 could save time, money and even your business's reputation
- Consider taking out business insurance, or – if you are already insured – review your level of cover to ensure that you would be protected if the worst were to happen
- Make a note of any key contacts – both inside your business and external support networks – that can help in a time of crisis.

About Barclays and BERG

Getting your business ready for future challenges has never been more important. Our sincere thanks to the Business Emergency Resilience Group for partnering with us to create this report.

About Business Banking at Barclays

Barclays has been working with business owners, organisations and company executives for over 327 years, helping and inspiring those that rely on local connection, insight and know-how to move forward.

Your business plays a crucial role in the success of the UK economy, and we believe that the more knowledge you have, the more successful your business can be.

We hope this report will prove useful when future-proofing your business's operations and upcoming plans.

About Barclays Group Resilience team

Barclays Group Resilience team has developed an initiative which brings together the skills and experience of its team of experts, the wider Barclays community and external partners on business resilience. It helps SMEs to share experiences and learn from real-life examples of businesses that have been affected by cyber crime, floods, fire and other disruptions, and what they now do differently. Barclays is a member and supporter of the Business Emergency Resilience Group programme.

About the Business Emergency Resilience Group

Part of Business in the Community (BITC), an initiative of His Royal Highness The Prince of Wales, the Business Emergency Resilience Group (BERG) helps businesses and communities across the UK to prepare for, respond to and recover from emergencies such as flooding, cyber attacks and civil unrest.

Find out more at
www.bitc.org.uk/berg

April 2018. BD05915-02.