Futureproofing SMEs

Implementing a Business Continuity Management Programme

Purpose of this session...

- Introduction to Business Continuity Management (BCM)
- Looking at the threat landscape
- Benefits of BC management
- How to implement your organisation's BC programme
- Tools to use
- Helpful hints and tips
- Question and answers

What is Business Continuity Management? (BCM)

- Business Continuity Management (BCM) is an holistic process that identifies potential threats to an organisation and the impacts that those threats, if realised, might cause, and which provides a framework for building organisational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities.

(ISO 22301:2012)

Quick Quiz…

What is Organisational Resilience?

A) The ability of an organisation to absorb and adapt in a changing environment

B) The capability of the organisation to continue delivery of products or services at acceptable pre-defined levels following a disruptive incident

C) Yet another new-fangled word associated with Business Continuity Management

D) All of the above

What do we mean by “Threats”?

- Threats are identified and defined…
    - Nationally by the Government
    - Geographically in Scotland by Regional Resilience Partnerships
    - By business organisations, such as the...
        - Business Continuity Institute
        - National Cyber Security Centre
        - The Institute of Directors
        - Napier Meridian, in partnership with the National Cyber Resilience Leaders' Board and supported by the Scottish Government

Threats at a national level…

- Every two years, the Cabinet Office produces a National Risk Register of Civil Emergencies.
- The NRR considers events where there is evidence to suggest it could plausibly happen within the next five years and where the consequences of that event would cause a civil emergency.
- A civil emergency is an event which would have a serious effect on the security of the UK, its people or the environment in which we live.
- This is published online and available at https://www.gov.uk/government/collections/national-risk-register-of-civil-emergencies

An ever changing profile…

- The NRR evolves when improvements to risk modelling processes are adopted. It also evolves to reflect the changing world in which we live.
- Risks that have become more prevalent of late include:
  - Emerging infectious diseases – linked to climate change, increased world travel, greater movement and displacement of people from war, global transport of food and intensive food production methods
  - Antimicrobactical resistance (AMR) - AMR occurs when drugs are no longer effective in treating infections caused by micro-organisms, such as bacteria, viruses or parasites.

Other risks to consider...

- Natural
  - Extreme weather
  - Flooding
  - Space weather
  - Poor air quality
  - Wildfires
  - Volcanic eruptions
- Industrial
  - Widespread electrical failure
  - Systems failures
  - Transport accidents
  - Industrial and urban accidents
- People
  - Widespread illness
  - Key staff lose
  - Sabotage
  - Industrial action
  - Public disorder
- Commercial
  - Lawsuits
  - Governance failure
  - Regulatory non-compliance

And more…

- Infrastructure
  - Internal fire
  - Internal flood
  - Power outage
- Systems
  - Network failure
  - Equipment theft
  - System failure
- Information
  - Cyber attack
  - Data loss
  - Virus
- Product
  - Recall
  - Contamination

- Civil
  - Civil unrest and public disorder
  - Economic change
  - Industrial action
- Malicious Attacks
  - Attacks on crowded places
  - Attacks on transport systems
  - Attacks on infrastructure
  - Chemical, Biological, radiological and nuclear attacks

A focus on terrorism…

- “Today there is more terrorist activity, coming at us more quickly, and it can be harder to detect. It is multi-dimensional, evolving rapidly, and operating at a scale and pace we’ve not seen before.”
  - **MI5 Director General, Andrew Parker, October 2017**

- Threat levels are designed to give a broad indication of the likelihood of a terrorist attack.
  - **LOW means an attack is unlikely.**
  - **MODERATE means an attack is possible, but not likely**
  - **SUBSTANTIAL means an attack is a strong possibility**
  - **SEVERE means an attack is highly likely**
  - **CRITICAL means an attack is expected imminently**
- The current threat level for international terrorism in the UK is SEVERE.

Where does the terror threat come from?

International

The threat projected onto the UK by terrorist groups, principally Daesh & Al-Qaeda

Extreme Right-Wing

A growing area of threat and concern. Domestic extremism is poses as much threat as radicalised Islamic attacks, as sadly demonstrated last week in New Zealand

Northern Ireland Related

The threat from Dissident Republican groups in Northern Ireland remains at SEVERE but was reduced to MODERATE on the mainland, 1st March 2018

Animal Rights

Since Stop Huntingdon Animal Cruelty (SHAC) ended their 15-year campaign in 2014, AR activity has been on a much reduced scale.

Environmental

Anti-Fracking remains a topical environmental issue.

Threats identified by the West of Scotland Resilience Partnership include...

- Influenza type diseases – pandemic
- Severe weather
- Flooding
- Industrial site accidents
- Pollution and contamination
- Transport disruptions
- https://www.readyscotland.org/my-community/ready-in-your-area/west-rrp/

On a more business focused level, the 2019 Horizon Scan report from the BCI…

1. Cyber attack or data breach
2. IT or telecoms outage
3. Adverse weather/natural disaster
4. Critical infrastructure failure
5. Reputational incident
6. Regulatory changes
7. Lack of talent/key skills
8. Supply chain disruption
9. Interruption to utility supply
10. Political change

The past versus the future...

- Adverse weather was previously 5th rated but has increased to 3rd for perceived future threats. An increase in weather related incidents such as the snowstorms affecting Europe and heat waves in Australia have heightened concerns.
- Global political uncertainty was previously 2nd from bottom of the league table but uncertainty in the US and challenges that Europe faces around Brexit have increased its profile

- https://www.thebci.org/uploads/assets/uploaded/331c286c-e7dd-41da-8e8c551bd22c07cf.pdf
- https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

The past versus the future... (cont')

- Cyber attacks have increased in profile from 4th greatest disruption to 1st place.

- The concern of HM Government over cyber security is so severe that they have developed a National Cyber Security Strategy 2016-2021 with DEFEND, DETER and DEVELOP as the core actions.

- There are many educational seminars designed to teach SME's about the risks of cyber breach. You are encouraged to undertake further investigation.

- https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

Developing Business Continuity Management

Actions to take

The many benefits of BCM…

- It has the potential to save lives
- It builds confidence amongst your customers
- It builds confidence amongst your employees
- It ensures compliance with industry standards
- It preserves brand value and reputation
- It cultivates a resilient organisational culture
- It provides valuable business data
- It helps mitigate financial risk
- It protects your supply chain
- It can save you money on insurance premiums
- It may be a prerequesite if applying for a tender

BCM does not need to be a complex thing although you can make it complex, if you wish.

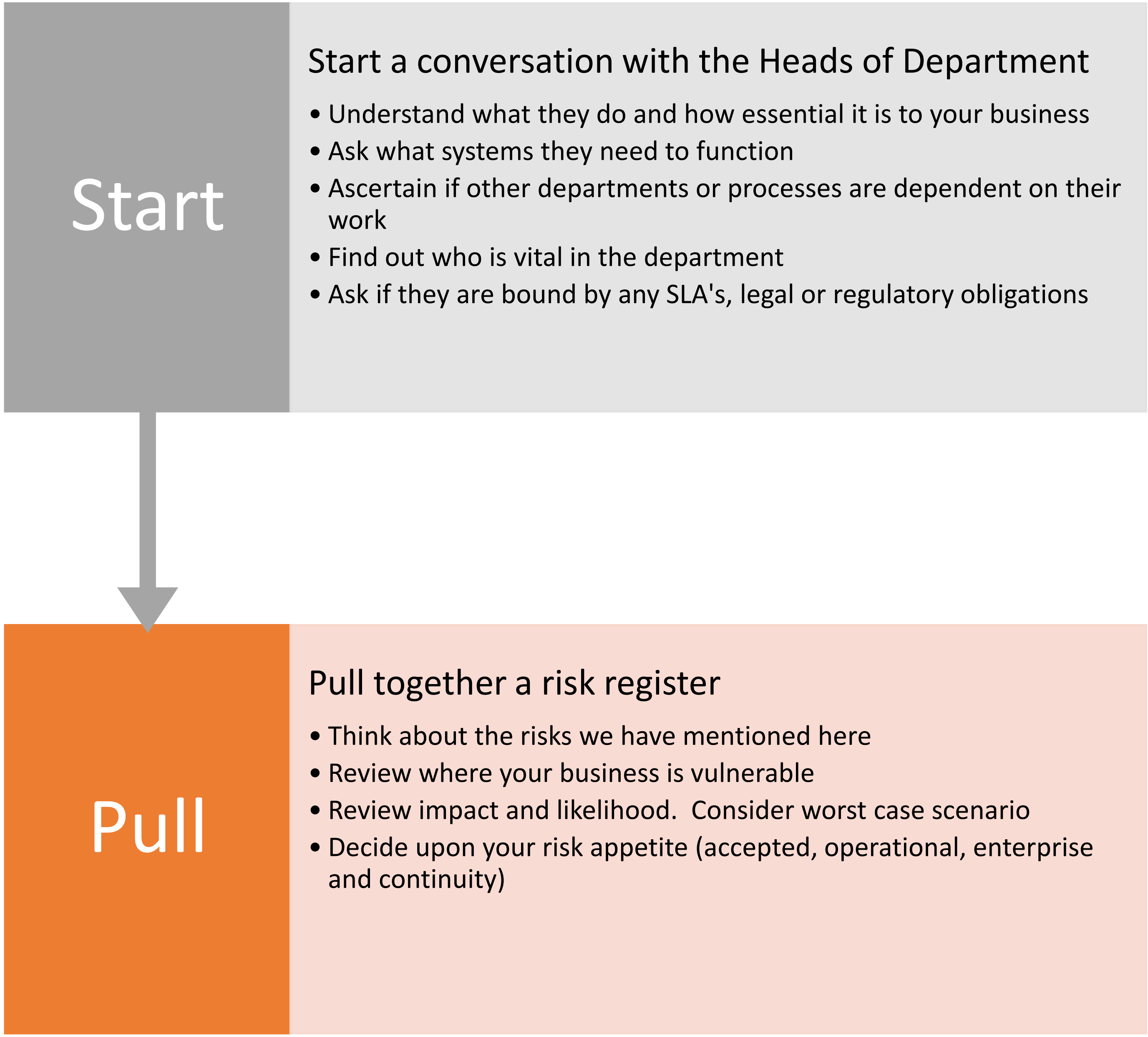
There is an ISO standard (22301) and a BCM life cycle to follow..

But sometimes, it's good to keep it simple...

So, how do we do this?

Step one – Review the risks to your business.

This is called the "Business Impact Analysis" (BIA)



Start

Start a conversation with the Heads of Department

- Understand what they do and how essential it is to your business
- Ask what systems they need to function
- Ascertain if other departments or processes are dependent on their work
- Find out who is vital in the department
- Ask if they are bound by any SLA's, legal or regulatory obligations

Pull

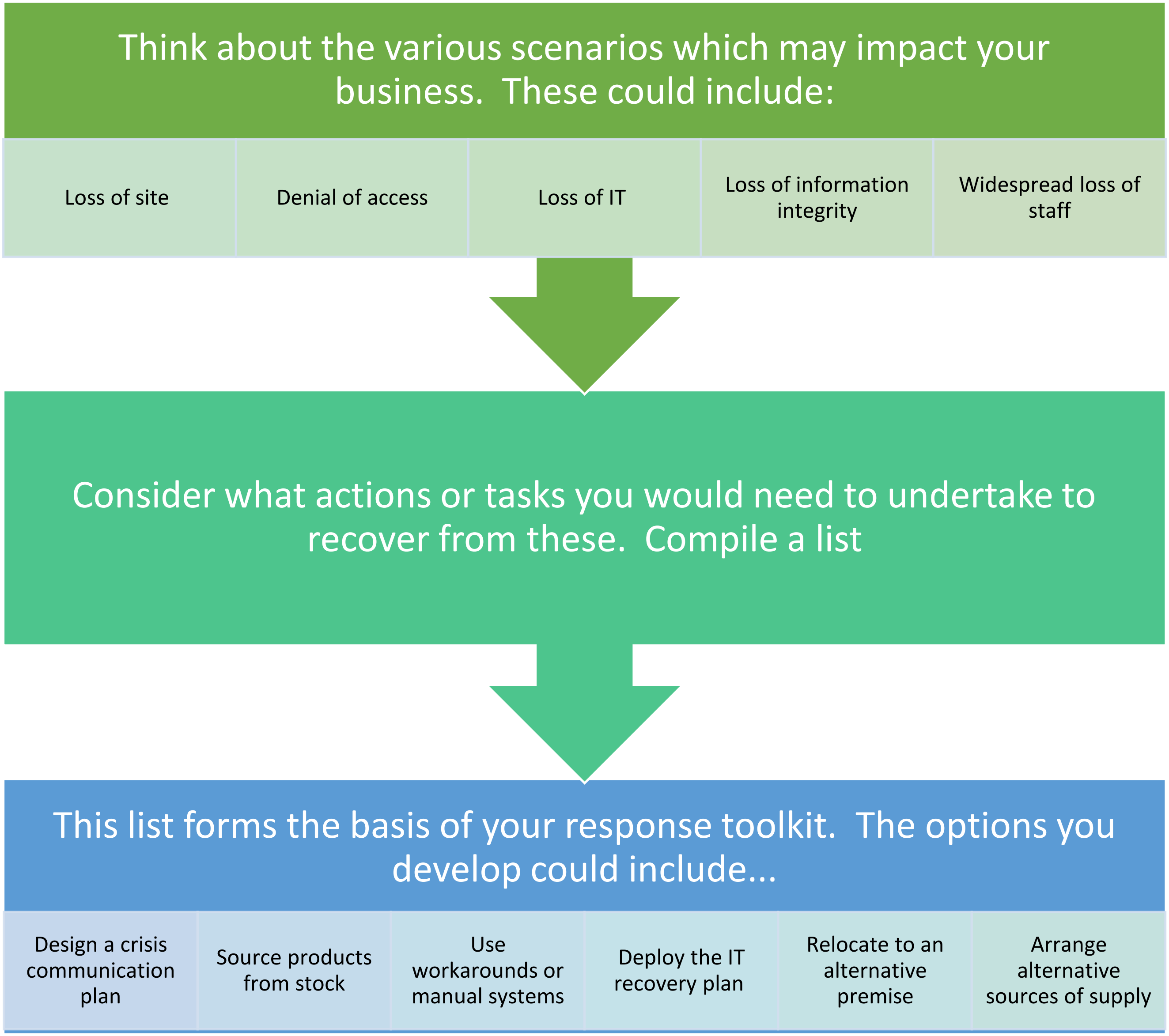
Pull together a risk register

- Think about the risks we have mentioned here
- Review where your business is vulnerable
- Review impact and likelihood. Consider worst case scenario
- Decide upon your risk appetite (accepted, operational, enterprise and continuity)

Step one – review the risk to your business

- Consider the impacts that an incident may have on your organisation
    - Financial – fines, penalties, missed opportunities, lost custom
    - Reputation – brand damage, poor PR
    - Productivity – quality of output inferior
    - Human welfare -
    - Regulatory and legal
- Impact is the pain felt by your business when it can't operate normally
- Set deadlines for the maximum tolerable period of disruption for each of the products/services within your business

Step two – Building your armoury



Think about the various scenarios which may impact your business. These could include:

- Loss of site
- Denial of access
- Loss of IT
- Loss of information integrity
- Widespread loss of staff

Consider what actions or tasks you would need to undertake to recover from these. Compile a list

This list forms the basis of your response toolkit. The options you develop could include…

- Design a crisis communication plan
- Source products from stock
- Use workarounds or manual systems
- Deploy the IT recovery plan
- Relocate to an alternative premise
- Arrange alternative sources of supply

Step three – Draft strategies for recovery

A strategy is a high-level response plan we adopt when faced with a scenario.

Think hard about the various scenarios and actions we have considered

Consider any additional assumptions, goals, options and deadlines and resilience measures in place.

Work up a number of recovery strategies that can be adapted to use in any incident that requires a business continuty response

Planning the Plan

Translating our work into a living document

The BC Plan is the instruction manual for the management of an incident. It should include:

- A list of all locations within use in the business
- Key staff names and contact details (inc next of kin)
- Critical customer, supplier and emergency responder details
- Organisational chart and details of the roles allocated to each person
- Procedures detailing workarounds and recovery plans
- Procedures for securing the site
- Instructions for IT service recovery, including details of cloud based applications

It should also include...

- Who is the plan sponsor
- Under what circumstances can the plan be invoked
- Who can invoke the plan
- Who is in the crisis team
- What to do within the first 4 hours of an incident
- What should be considered to help support the longer term recovery

Tools for managing and storing your plan

- BC plans need to be accessible to all at the time of an incident
- ✗ A large ring binder of instruction is not likely to be a useful tool
- ✓ There are various cloud-based software providers that offer BC software products aimed at SME's, which are reasonably priced
- A MS Word version of the plan saved on a password protected 'phone gives ready access during an incident
- Log sheets and document records are part of the plan and should be used to record actions during an incident

Helpful hints and tips

The more you can think about and decide in advance of an incident, the easier the management of the incident becomes.

Deciding on policies for home working and staff salary payments during an incident, in advance means that this is clear cut at a time when everything else may not be

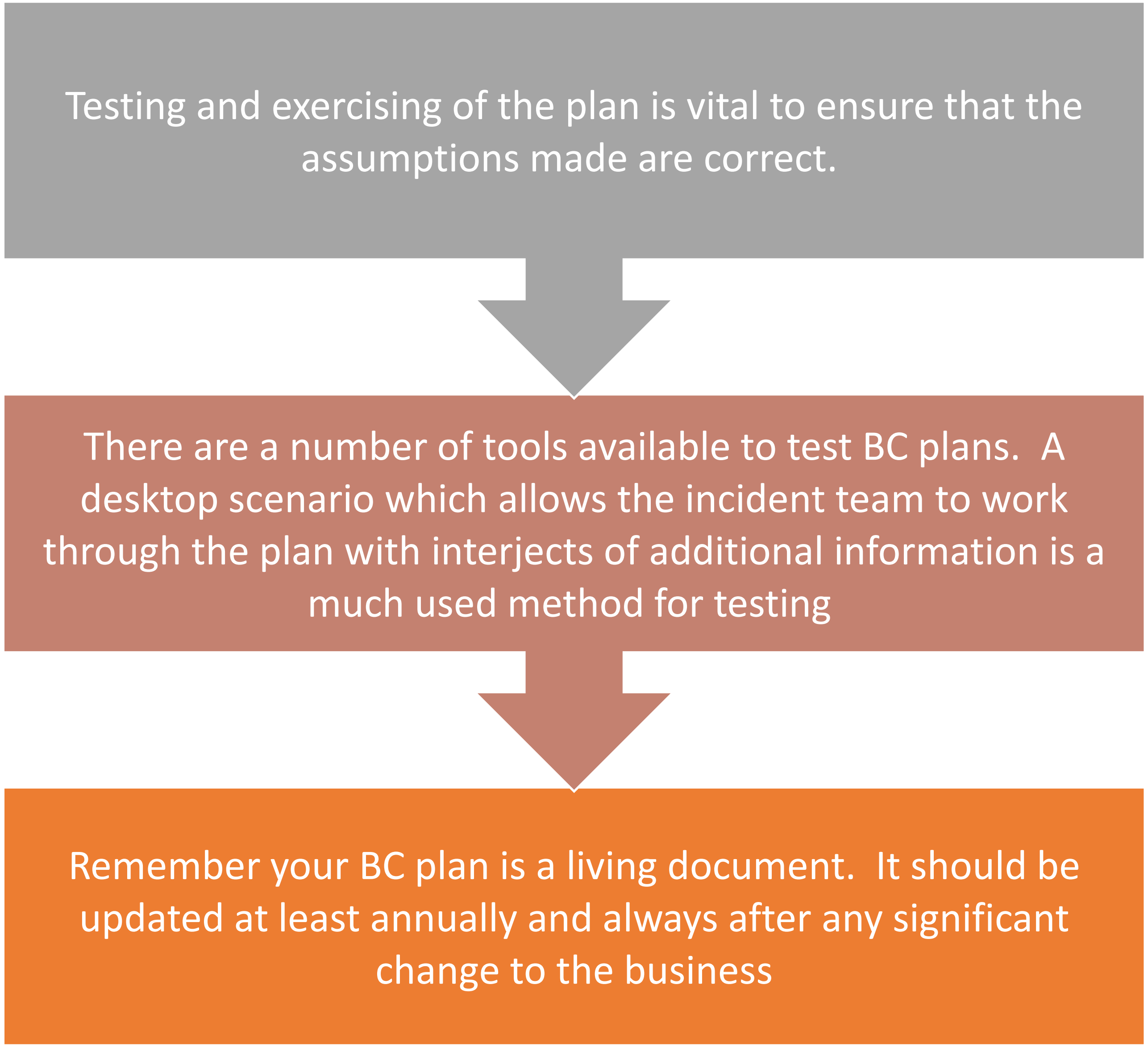
Consider the use of technology for incident communications.

Set up Whatsapp groups or Text anywhere facilities in advance to be used for communication of requirements

Consider a "grab bag" which various support items available.

Include wind- up radios, first aid kit, schematics of the building, IT network diagrams, insurance policy details and a copy of your BC Plan

Going forward…



Testing and exercising of the plan is vital to ensure that the assumptions made are correct.

There are a number of tools available to test BC plans. A desktop scenario which allows the incident team to work through the plan with interjects of additional information is a much used method for testing

Remember your BC plan is a living document. It should be updated at least annually and always after any significant change to the business

It is hoped that you will never need to use a BC plan

However, statistics state that 93% of businesses without a recovery plan who suffer a major incident are out of business within one year of the incident.

Don't let that be your organisation.

Questions?

Thank you for listening

3 minutes to MIDNIGHT