

## Power Outages and Business Continuity Planning this Winter

*This article is intended for insurance brokers only and has been written in collaboration with Arch Business Protection, our risk management partners.*

### Introduction: what businesses may be impacted?

There has been talk in the press of utility outages this winter. Not every eventuality is covered by commercial insurance policies. Deliberate decisions to cut or restrict supply by utility companies is one of these. This can have several serious implications for businesses. These may include;

- Frozen and chilled stock such as food, through to temperature-controlled raw materials and even medicines can be affected.
- The ability to run night shifts may be impacted.
- Some trade processes and manufacturing and engineering systems may need be shut down and re-energised in a controlled manner to prevent damage to the equipment (e.g., furnaces, injection moulding machines), failure of equipment (such as high intensity discharge lights) and loss of product/work in progress.
- Security systems - CCTV systems, Intruder and Fire Alarms installed to the relevant BS/EN standards will have an uninterruptable power supply, normally by battery back-up which steps in automatically when an electrical power outage occurs. Battery backup varies by the grade of system which in most circumstances is decided by a Risk Assessment/Risk Analysis of the site by the system installer, but which is generally a minimum of 4 hours.

### Policyholders should consider:

- Check with the Alarm Installer/Maintenance Company the minimum period the back-up power supply is expected to maintain the system in full operation.
- Ensure the back-up power supply is healthy and performing as intended – batteries decline with age and need to be replaced periodically.
- Where any planned power outage may exceed the capacity of the back-up power supply, consider alternative risk control strategies such as manned security or periodic visits to the site by a security company or senior company staff.

Please note, at time of writing in December 2022, it is becoming increasingly difficult to hire a generator to deal with potential power-outs, with limited supply and suddenly a significant demand.

### What should businesses do to protect themselves?

Businesses may want to consider having a plan in place for if the worst happens. An effective Business Continuity plan is a living document which needs to be constantly reviewed and updated considering the changing challenges that businesses face.



Winner

Broker Partner of the Year



Commercial Lines  
Arch Insurance

Winner

Commercial Lines  
Gold



Small Commercial  
Combined  
Arch Insurance

Winner

Small Commercial Combined  
Gold

## Power Outages and Business Continuity Planning this Winter

### What is business continuity planning?

Business Continuity Planning is not the same as a Disaster Recovery Plan, as the two phrases are sometimes used interchangeably but they are not the same. The risk management discipline that is known variably as Business Continuity Planning or Business Resilience Planning started life as Disaster Recovery Planning.

The concept of the Disaster Recovery Plan (DRP) is simple. If you experience a major event such as a fire, then you have information available and identified actions to take that help you shorten the reinstatement of your operations. The information you might see in a DRP;

- List of key contacts
- Information or its whereabouts for emergency services
- Details of suppliers for assets/resources, such as your utilities
- Emergency procedure steps that you need to take.

But as the name implies, it deals with disasters, rather than the loss of a specific asset or resource, such as electrical supply. During the '90s, Disaster Recovery Planning evolved into Business Continuity Planning (BCP) with the emphasis on minimising the likelihood of disruption, thus maintaining "continuity within the business" and also planning more proactively to recover the business, reducing the focus on Disaster Recovery to Incident Response.

### The difference between Disaster Recovery Plan and Business Continuity Planning

A BCP will have many elements of a Disaster Recovery Plan in its Incident Response Plan, but there are significant differences between the two. One of the most important is Understanding the organisation's Tolerance for Disruption – in simple terms, "if we cannot deliver our products or services, how long will it be before our customers seek alternatives elsewhere, perhaps to avoid disruption to their own business".

This information shapes the whole Business Continuity process as this timeframe is how quickly the business needs to reinstate the supply of its products or services regardless of the cause of disruption; it's the whole purpose of the BCP. And not most importantly in the event of a Disaster, but through partial damage (loss of utilities) or loss of use or access.

Business Continuity Planning also identifies the recovery times of individual Assets and Resources through a process known as Business Impact Analysis (BIA).

This is one of the significant differences between Business Continuity and Disaster Recovery as it protects the business from a range of events rather than a disaster. It is focussed on the timeframes in which the Business' functionality is restored, regardless of the cause for its loss or loss of use.

### Putting in place Business Continuity Arrangements – in broad terms, these will:

1. Reduce the likelihood of an incident (i.e. Sprinkler system, cyber risk controls, Health and Safety arrangements, Environmental controls, etc); these would be widely recognised as risk management controls.
2. Allow the assets/resources to be recovered (or their functionality to the business process) within their recovery time objectives (i.e. duplicate tooling, pre-agreed outsourcing arrangements, certain Business Interruption covers that pay out for additional expenditure (air freighting product rather than sea freight), data back-ups, etc) and pre-agreed contracts for the supply of Generators (as opposed to a list of possible generator suppliers). We refer to these as Recovery Measures as they allow the business to recover functionality well within its Tolerance for Disruption.
3. The Incident Response Plan – the step-by-step playbook for how the organisation manages an incident. This may also detail "Continuity Phase" - reinstating its activities and a "Recovery Phase" reinstating its infrastructure.
4. Recovery Resources – these are resources the Business specifically needs to support its Incident Response assuming the loss or loss of availability of its primary infrastructure. This would include an incident response centre, key business data, and a Communications Plan.

Business Continuity Planning also includes maintenance, testing, and exercising of the BCP and continuity arrangements to ensure they are in a state of readiness if required and all those with a role or responsibility can work an Incident Response.