Business Continuity Overview

V0.3 2021-11-15



Copyright © 2021 Real World Technology Solutions

All rights reserved.

Contents

[1 Introduction 4](#_Toc88124130)

[1.1 What is Business Continuity? 4](#_Toc88124131)

[1.2 Why is Business Continuity Necessary? 4](#_Toc88124132)

[1.3 Is Business Continuity Expensive? 5](#_Toc88124133)

[1.4 Essential Preparation 5](#_Toc88124134)

[2 General Approach to Business Continuity 6](#_Toc88124135)

[2.1 Infrastructure 6](#_Toc88124136)

[2.2 People 6](#_Toc88124137)

[3 Additional Business Continuity Information 7](#_Toc88124138)

# Introduction

Business Continuity is fundamental to the continuing success of every organisation, not just commercial businesses. Every organisation conducts its business for the benefit of the organisation and those who are its beneficiaries, be they paying customers, clients or recipients of the organisation’s patronage in some form. It is important, therefore, to recover from unexpected events as quickly as possible.

If an organisation cannot conduct its normal business, it and the people to whom it provides goods or services suffer. The potential for the organisation to “go out of business” if it cannot conduct its business for any given time is real.

## What is Business Continuity?

Business Continuity is being prepared for the unexpected. It is understanding what might cause the normal operations of an organisation to be reduced or stopped for a period of time. It is about having plans to deal with such circumstances so that normal operations can be restored as quickly as possible, whilst providing essential functions during the incident, if at all possible.

Business Continuity involves:

* Understanding the “normal operations” of the organisation
* Identifying all the resources (people, equipment, facilities, etc) needed for normal operations to work as intended
* Deciding what are essential functions that can be considered as “mission critical”
* Identifying risks, threats and vulnerabilities that can affect normal operations
* Having Plans to manage incidents that reduce or stop normal operations, designed to provide at least the mission critical activities of the organisation, if possible
* Regular testing, reviewing and revising of Business Continuity Plans to ensure they remain effective as IT environments and cyber security environments evolve.

Business Continuity is about being proactive. When a major disruption to normal operations happens, good Business Continuity helps protect the organisation and those who benefit from it!

## Why is Business Continuity Necessary?

When a major incident happens, organisations with good Business Continuity Plans tend to survive much better than those that do not have such preparation. Various statistics put the number of business closures within six months of a significant cyber attack at 60%. Putting good Business Continuity in place is both good business practice and sheer common sense.

The impact to an organisation when it suffers a cyber attack can include:

* Financial loss
* Damage to reputation
* Loss of customers and clients
* Disruption of the organisation’s assistance to beneficiaries, particular for non-profits
* Loss of data, including sensitive and private data
* Damage to equipment and facilities
* Consequential damage claims from customers, clients and beneficiaries

While it is crucial to plan for the unexpected from a cyber security perspective, the plans put in place will also be of value when there are disruptions due to other types of events, including power grid failures, fire, flood, criminal activity, etc.

## Is Business Continuity Expensive?

Business Continuity should be made possible in ways that are appropriate and manageable for the organisation. That means doing what is achievable with the resources available (people, equipment, finances, etc) to try to ensure an explicit set of essential functions and services is available during disruptions.

It will almost certainly involve some financial expenditure. The cost will depend on the decisions listed in Section 1.1 above (What is Business Continuity?).

Things to consider include:

* Preventive and protective infrastructure such as network equipment strengthened to minimise risks of cyber attack
* Redundant equipment that could handle “primary” equipment being compromised
* Protective software such as antivirus and malware protection
* Additional personnel, possibly with on-call arrangements
* Time and effort to prepare and manage Business Continuity Plans

Every organisation must weigh the financial cost of Business Continuity against the overall cost (financial and non-financial) of damage done during a disruption, and plan accordingly.

## Essential Preparation

Business Continuity is both preparation and, if needed, execution during an incident. The overall approach looks like this:



**Prevent**: Risk Management activities to reduce the likelihood and impact of incidents

**Prepare**: Business Impact understanding and ways to mitigate impact during an incident

**Respond**: Manage an active incident to minimise its scope and impact

**Recover**: Recover and restore essential and non-essential functions, services and activities

All these are part of good Business Continuity. They should be regularly reviewed, rehearsed and revised.

# General Approach to Business Continuity

Business Continuity will be different for each organisation. Nevertheless, there are some common aspects that all organisations must address. Reducing risks makes it more likely that a Business Continuity Plan will not need to be invoked, providing greater resilience to a potential interruption to normal operations. If the Business Continuity Plan is invoked, various preparations and expenditure in advance will help to reduce the impact of the incident. These include preventive measures as well as ways to mitigate the impact of any incident and recover more quickly. Good preparation is key!

## Infrastructure

Providing good Business Continuity will almost certainly mean some changes in IT infrastructure. This includes hardware (equipment, generally) and software.

Some things to consider to minimise the risk of successful cyber attacks include:

* Making network equipment as secure as possible – this involves the right network devices being used and being configured well
* Configuring IT systems securely
* Installing and running effective antivirus and malware software
* Preventing risks associated with the use of portable devices
* Configuring equipment so that there is redundancy that could make recovery quicker
* Use of off-site resources such as cloud-based storage to separate data from local equipment

Investment in IT infrastructure should be balanced against the available resources, primarily finances, so that expenditure for continuity planning is based on a good understanding of the potential costs of damage from an incident. This is part of the overall risk management investment of the organisation.

## People

Business Continuity planning is not just about technology, as important as that is. People are at the heart of good Business Continuity planning. The best technology in the world can still be vulnerable to failure during disruptive events if people are not prepared and practised in handling such incidents.

Some things to consider to try to ensure personnel can respond well during cyber attacks include:

* Give personnel regular, up-to-date Cyber Security Training
* Teach personnel to recognise and report cyber security events that may indicate a cyber security incident is in progress
* Define, document, test and practice Business Continuity Plans – plans must be familiar to personnel so that their actions are effective and appropriate, always following the Plan
* Encourage feedback from personnel on the rehearsals of Business Continuity Plans and incorporate useful insights as a means of continual improvement of plans

Above all, make personnel aware that eventually something will disrupt normal operations and it is part of the culture of the organisation to “be prepared”!

# Additional Business Continuity Information

Many organisations have useful information about Business Continuity. A selection of these is provided here for additional reference.

* Wikipedia – Business Continuity Planning: <https://en.wikipedia.org/wiki/Business_continuity_planning>
* Australian Government – Risk Assessment and Planning:

<https://business.gov.au/risk-management/risk-assessment-and-planning>

* QLD Government – Business Continuity Planning:

<https://www.business.qld.gov.au/running-business/protecting-business/risk-management/continuity-planning>

* NSW Government – Prepare for the unexpected - Build a Business Continuity Plan:

<https://www.smallbusiness.nsw.gov.au/BCP>

* WA Government – Dealing with unexpected events:

<https://www.smallbusiness.wa.gov.au/business-advice/insurance-and-risk-management/dealing-unexpected-events>

* APRA – Business Continuity Management:

<https://www.apra.gov.au/business-continuity-management-1>

* US Government – Business Continuity Plan:

<https://www.ready.gov/business-continuity-plan>

* Investopedia – Business Continuity Planning (BCP):

<https://www.investopedia.com/terms/b/business-continuity-planning.asp>

* Manchester City Council, UK – Business Continuity Planning:

<https://www.manchester.gov.uk/info/200039/emergencies/6174/business_continuity_planning>

* International Standards Organisation (ISO) – ISO 22301 - Business Continuity (An Introduction):

<https://www.iso.org/publication/PUB100442.html>