CIRRO

Whitepaper
Understanding Business Continuity for Business Owners & Managers

Is Your Business in Good Shape?

Understand Measure & Reduce Risk

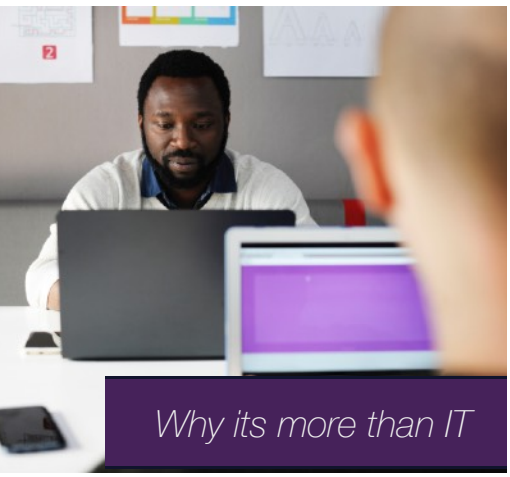
Questions You Need To Ask

Best Practise for Business Continuity

Table OF CONTENTS

What is Business Continuity?

Understanding Business Impact



Why its more than IT

Disaster Recover V Business Continuity

Best Practice Guide

What Is Business Continuity Anyway?

When you think of a major or disastrous event you might imagine a volcano, fire or criminal act. The reality of what constitutes a disaster for a lot of people today is the loss of connectivity or data, for others, it's when systems are slow.

We've got better at understanding our geographic and environmental risks, yet many businesses fundamentally don't understand business and technology risk.

On average, business has gone from 1% electronic data storage in 1986 to 98% in 2018 and the explosion of data only really began in the last few years

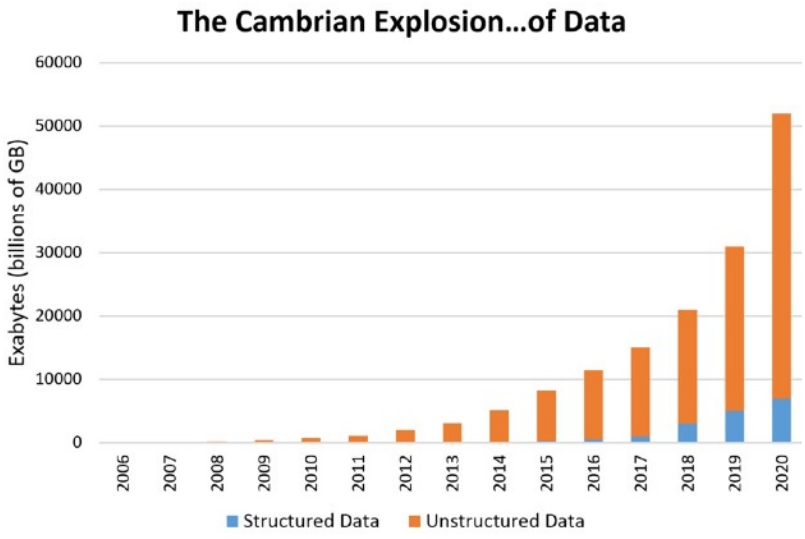
This paper is designed for business owners. So you can have the right conversation s about business objectives, outcomes and risk. This is not about technology. Those responsible for your technology need your guidance.

This paper will explore the business landscape and show how we got to this point of being so reliant on data. It will highlight the difference between Disaster Recovery and Business Continuity.

It will highlight successes and failures and importantly, it focuses on business outcomes and risk mitigation.

Unprecedented Growth

It is generally accepted that we have entered a period of significant data growth.



The Business Landscape of Today

Where Are We?

These are interesting times in human and business evolution. Never before have we relied so heavily on things we understand so little about. Our analogue heritage has been superseded by our digital present, which is predicted to be overtaken by an automated and robotic future.

When IT systems became accessible to the masses during the 80's, computing was simple, things were proprietary, and everything was siloed. In reality, we didn't have much data, storage, connectivity or interoperability. As a result, many industries have evolved very slowly. Legal requirements, guidelines, best practice and certification standards also evolved slowly over his 25-year period.

Take data protection as an example, the Data Protection Act was enacted in 1998, the same year Google launched, and its been protecting only data since GDPR came into play in 2018, 20 years later.

Data Protection Act 1998

Since the launch of GDPR in early 2018, Google have been hit with a €50m fine in France for not disclosing how it collects and uses data* (BBC News, 2019). Just before GDPR launched, a major data scandal hit the US and UK, which resulted in around 1bn fake news ads influencing the US election and Brexit, it even has its own Wikipedia page and has been made into a documentary called Brexit: Britain's Great Escape. The result was Mark Zuckerberg in front of Congress and Facebook losing over $100bn in value.

While it's hard to directly link these types of events, as well as continued 'strange' and unpredictable events, from Drones over Gatwick, to NHS ransomware attacks, to our own day to day business. What is does show is the need for change in how we think of data and how we prepare for the unexpected.

The ISO standard for Information Security (27001) was launched in 2005 and the standard for Business Continuity (22301) was launched in 2012.

Data Protection Act 1998

Implication of DPA 1998

If you lose someone's personal data, THEY have a problem.
UK only.
Maximum fine was £500,000

Implications of GDPR

If you lose someone's personal data YOU have a problem.
EU wide.
Maximum fine is 4% global annual revenue or £20m

The focus on data and system has fundamentally changed in the last few years.

All this must be balanced with the reality that the new world currency is data. Many businesses are held to random by this 'monster' the world has created. Without access to data and the necessary applications and tools, many businesses simple can't operate. The concept of Disaster Recover is not new, but Business Continuity is. It differs in mentality, thought process and preparation.

Whats the Difference Between Disaster Recovery & Business Continuity?

Disaster Recover (DR) assumes that you may, at some point in the future, have a disaster event from which you need to recover. Disasters have traditionally been considered and dealt with as force majeure events or Acts of God.

Business Continuity (BC) assumes that you will experience impairments, degradation or loss of normal operations or aspects of them. It then provides the framework that your business has considered, designed, planned, tested and documented, to continue to operate in a way that will have limited or no impact to your normal operations.

The mentality aspect comes into play here as most organisations, especially SME's, don't see the relevance, the context or the need for Business Continuity. The reason is simple; there is a lot of scaremongering, miss-information and a real lack of understanding, especially when it comes to fundamentals. It's also true that it's so hard to contextualise. Some of events you hear and read about seem far fetched and are deemed as highly unlikely by most business.

The view of many business owners is

'Why Would Anyone Want To Attack Us?' Or 'We Test our Back-Up Annual, Everything Works Just Fine'.

Disaster Recovery

A set of policies for recovering from a Disaster Event

Event Types:

- Fire & Flood
- Lose of Power
- Lose of Connectivity
- Data Lose
- Lose of service or outage
- Outage with 3rd party provider

V

Business Continuity

Policies, plans & guidelines for dealing with unexpected or difficult situations

Event Types:

- Degraded Service (application/connectivity)
- Virus, infection, crypto, ransomeware
- System configuration or incident
- Accidental removal of data
- Lose of non-core system
- Lose/unavailability of key staff or password

Disaster Recovery is about the lights being on. Business Continuity is about knowing what to do when the lights start to flicker and how to measure the quality of light being produced. Clearly you need both.

By considering Business Continuity in more detail, organisations also understand their risk profile better and the need for good documentation for processes and systems, as well as having change control processes and a risk register.

More advanced organisations, and those that have understood the challenges around GDPR will also look to understand technology and system usage by asking basic questions, such as:

- What do you have (asset or system)
- Why do you have it (purpose)
- Is it fit for purpose (it's business value)
- Who has access to it and why (function)
- Its risk profile and availability requirements (impact)
- How it is managed & monitored (visibility)

The idea here is to start the conversations. If the answers are too technical, they aren't good answers. This needs to be simple.

17 Feb 2019 - Hackers wiped every server and every back-up of VFEmail, a secure email provider in the USA. With catastrophic loss of all data for 20 years.

The Hype, the Reality

Unfortunately, the hype is very real. Most organisations are blissfully unaware of the realities of the world they operate it.

The more you read the more scaremongering and hype you often find when it comes to Disaster Events. Especially around data breaches, hacks and cyber events. However, the old adage of 'failing to prepare is preparing to fail' is correct. While the scaremongering seems to be a focal point of many organisations providing these services, they are based on realities of what is happening in the real-world.

What is clear to us however, is that the vast majority (and we mean vast) are seriously unprepared for any serious event, have very limited means of recovery, very limited real-world testing and lack up to date documentation and processes. All this means that risk is not understand, managed or mitigated.

Why Aren't Businesses Well Prepared?

The main reason behind this behaviour is that organisations don't understand how to measure risk or how to mitigate it. The IT services industry is also very behind the curve in how it supports and educates customers. Essential IT Services companies have never really assumed much customer risk, they typically always 'win'. We say this because:

- The IT Provider sells a solution that has no guarantee, based on a customer's defined requirements
- The IT provider then sells a Support & Maintenance contract to 'fix' the issues that exist and manage the customer's investment they have made with them in the solution

- The IT industry makes less and less money from selling hardware and makes more out of selling ongoing services, such as support contracts
- Because customers own the risks, the investments and the ongoing issues, the IT services industry has devalued its offering to focus on price at the cost of quality. The result is a high churn of suppliers

This behaviour decreases the perceived value of ICT which is often seen as a cost or overhead and is therefore treated as such. It's not usually seen as a function that can create value, improve agility and simplify operations, however that is its exact purpose.

Suppliers won't and can't assume customer risk, however they should help customers reduce risk by working with them to understand and mitigate it. Additionally, the revenue model needs to change. The focus needs to be on operational excellence and quality. For example, Cirro doesn't charge for support when it comes to our Cloud Services because we are responsible for them. We are also very well placed to work with customers to understand and mitigate risk.

Have IT Service Providers devalued themselves? They offer no guarantee, they sell systems and then charge for fixing them

Benefits of a New Approach

For Customers

When this approach is applied the following number of things happen:

1. The provider owns the assets and can therefore control the quality and assume more responsibility for risk
2. The solution becomes more about end-to-end user experience and delivering outcomes rather than selling a product or a service
3. The solution incorporates security, performance monitoring, business continuity and data protection at the core

For Suppliers

Interestingly, for suppliers, we also see a number of benefits:

1. Lower number of support staff – dealing with fewer issues
2. Almost zero customer churn – they have no compelling reason to leave
3. Profitable customers, generally you need customers to be with your for longer due to your upfront investment in them
4. Move to a recurring revenue model rather than chasing cash-flow

3, 2, 1, Rule For Data Backup

3 Copies of your Data

2 On at least 2 different media

1 copy off-site at least

How To Understand Risk

Understanding risk isn't that easy, that's why many business haven't done it, or kept up to date with reviewing risks.

A question to ask yourself as you read this - When was the last time you had an internal meeting that reviewed risk? If it wasn't in the last 6 month - then that's a risk!

To better understand risk, let's look at common events and high profile events. That way we can look at what is behind them and where the risk comes from. Keep in mind that different industry types have different external threats and levels of potential exposure.

Feb 2019 - Crypto boss dies with only password to £145m

This is incredibly poor planning. A simple password management tool like 1pass or Dashline should have been used.

Feb 2019 - Able & Cole fail to deliver due to fire affect a major warehouse

This affected a high %age of customers. No communication went out, so all customers tried to call in, swamping staff.

Talk Talk suffers major UK wide broadband outage. o2 major outage.

Many UK business and home workers were affected. by these incidents.

Interestingly, our business had an issue, see below*

Feb 2019 - FSEmail suffer catastrophic loss of 20 years of data

This is poor design. To have all your live and back-up data accessibly and online is shockingly bad, see our best practice guide.

Areas To Measure

Risk can be measured and calculated as follows:

1. **Business Impact** - If a service were to fail, how significantly would that impact the business?
2. **Likelihood of Failure** - This can be very hard to measure, you need to consider historic data, age of equipment, test results and any other information you have
3. **Likelihood of Detection** - Services that fail might not be immediately detected, so what measures are in place for early detection (Service Impairment) or actual failure - how do you know?

Calculate risk by multiplying the three areas;
Impact X Likelihood X Detection = Risk Score

* Our own business had a rare lease line outage at a key office. We had a Business Continuity plan whereby we had an o2 4G fail-over. Unfortunately, the only time we needed this, o2 also had a rare outage. This caused us a major issue as we have VoIP, so it affected all our communications.
* Fortunately we were able to get a Vodafone 4G SIM very quickly and were back-online. We now have both o2 and Vodafone SIM's for back-up.
* We also use a remote answering service if no users are logged in to our phone system. So call were answered.
* When we reviewed this event, the consensus was that having our primary lease line down and two mobile operators down is unlikely and a low (acceptable) risk. Because of the nature of our business, all our users can work from home and a full DR plan would takes 45min to implement.

What to Measure, How To Identify Risk

Understanding risk and threats use to be fairly simple as the majority or risk was localised. It may come from the environment, or politics or technology. However even then, risk events were fairly localised. In today's global economy, where everything is connected, local now means planet Earth. Anyway who is connected is therefore connected to everyone. That was how the Internet was design.

Many IT systems and networks are however, still designed with the view that local, means local, and local means trust. Here we look at where the risks and the threats come from.

Internal

- Human error
- Victim of Cyber Attack
- Mis-configured system
- Virus on external device
- Reliance on key individual(s)
- Stolen data sets

External

- 3rd party provider
- API's or application configurations
- Customer or supply chain
- Disgruntled ex-employees
- Competitors - industrial espionage

Cyber

- A targeted attack - device or network
- A virus, bug, malware - generic attack
- An engineered attack - human or behaviour level

Prevention Is Better Than Cure

When you look at the risk areas, you can see a lot of this is easily preventable. You can take the following sets and massively reduce 'risk'. We suggest some steps you can take:

Audit, what do you have? How do you work? Get every department head to put this together. It should include every device and application used

Understand your process for managing those systems. Who administers them, how up to date are they. How are they backed-up.

Document and measure your risk profile. Understand and define 'normal' operations.

How educated and aware are your staff.

Areas of Business Impact

Business Impact needs to be measured against how you operate normally. The level of service you expect or are contracted to provide, the level of output you want / need to maintain. You should also incorporate and understand of your Customer Experience.

Depending on your business, this will also include:

- Loss of revenue or impact on cash-flow
- Increased expenditure
- Decrease in customer satisfaction or delivery timescales
- Lower quality of product or service
- Regulatory fines or loss of trust
- Impact on deliveries or supply chain
- Inability to communicate effectively

By understanding what 'normal' looks like, you can better measure Impact, which is the difference between Normal and how you perform during or after an Event.

CIRRO

Business Continuity for most business is Important but urgent. Until they have an event that makes it urgent.

Cirro is certified to ISO 22301 for Business Continuity, ISO 27001 for Information Security and ISO 9001 for Quality and ISO 14001 for Environmental Management.

If you'd like to reduce your technology and operational risk, we'd love to help you.

You can find more advice, guides and tools on our website, including how to get in touch.

bsi. ISO 9001 Quality Management

bsi. ISO/IEC 27001 Information Security Management

bsi. ISO 22301 Business Continuity Management

bsi. ISO 14001 Environmental Management

You can find more advice, guides and tools on our website,
Need more help? Get in touch.