LinkResQ
A LEADER IN ENTERPRISE RISK MANAGEMENT

Staying In Business

A Business Continuity White Paper by

Paul O'Brien and Gerard Joyce

LinkResQ Limited

Contents:

Introduction

They say “Lightning never strikes twice in the same place”. There are two possible explanations for that conclusion: - the random nature of the process that causes lightning to come to earth in the first place, or God feels no need to waste a second bolt on the charred remains of something she has already burned to a crisp. If it does strike – is your enterprise ready?

What is Business Continuity?

The Basel Committee on Banking Supervision published a document outlining the principles of business continuity in which they define business continuity as “*the state of continuous, uninterrupted, operation of a business*.”

The Business Continuity Institute defines Business Continuity Management as “*a holistic management process that identifies potential impacts that threaten an organisation and provides a framework for building resilience and the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value creating activities*.”

Ideally business continuity is the ability of an enterprise to function normally, meet its objectives, and maintain **full** service to its customers and stakeholders despite **any** loss event.

Business Continuity has its roots in Enterprise Risk Management; establishing the risk context, determining the risk appetite, conducting a regular enterprise risk assessment, implementing mitigation strategies, analysing residual risks, accepting the loss event possibility, developing a continuity plan, testing the plan, applying the lessons of the testing, then repeating the cycle, regularly. The Business Continuity plan is informed by the whole Enterprise Risk Management Framework and is an outcome of the process.

Loss Events = Opportunities for Disaster

Loss events come in many guises: fire, flood, storm damage, utility outage, systems loss, people loss and many more. Any loss event is an opportunity for disaster. A loss event turns into a disaster for an enterprise if the Maximum Tolerable Outage (MTO) is exceeded or the Minimum Essential Service is lost. The MTO is the point in time at which the loss event begins to damage your business. It depends on a number of factors driven by the enterprise objectives and its commitments. How long can you be “away from the market” before the objectives are materially impacted? How long before permanent un-recoverable damage is done to your revenue, reputation, or the things that matter to your enterprise? The MTO is a function of time,

measured in minutes, hours, days, or weeks depending on the nature of your enterprise. The Minimum Essential Service (MES) is the degree to which the enterprise has to recover from a loss event in order to stem loss of revenue, reputation or the things that matter to your enterprise.

A *Business as Usual* sign in the window of your bakery in the local village is a plea to customers who might reasonably assume that business is far from *usual* given that the bakery now operates at the other side of a six foot deep trench at the end of a few very narrow planks. The "Denial of Access" caused by the trench is countered by the planks and business can continue. Most loyal customers will walk the plank the first day. Don't expect any incremental business other than from the guys digging the trench. By day three the plank novelty will have worn off and some of your loyal friends will be buying sliced and avoiding eye contact.

Awareness of an interruption or loss event by stakeholders and customers induces a period of understanding and empathy. This empathy has a shelf life. As soon as the loss of service or supply begins to materially affect customers the empathy evaporates. They begin to put deadlines on your recovery and begin to implement alternative arrangements if they have key service provider sections in their own business continuity plans. The ones who have no alternatives watch your disaster turn into their loss event and if they reach their MTO or lose their MES, they will consider you as the root cause!

Developing a Business Continuity Plan

It is important that business continuity plans cover all aspects of the operation. For years IT Disaster Recovery, Building Evacuation, and Insurance were the limit of many companies' "continuity" plans. However in these days of increased competitiveness, regulations, risk and stakeholder expectations, it is no longer enough. Enterprises must now also consider Crisis Management plans, Media Communication plans and Resource Recovery plans. (See side panel on 10 Steps To Business Continuity Planning) More significantly the time one can be "away from the market" is considerably reduced and this means that plans must be comprehensive, well communicated and tested.

An enterprise must know its MTO and MES to develop a Business Continuity Plan. Like any good plan it has stated objectives and operational alignment around those objectives. In the details, tasks are assigned and command and control established. (The leaders in a crisis situation are not necessarily the same people who lead/manage in normal circumstances.) In a loss event the MTO and the MES become the Enterprise Primary Objectives. The functional primary objectives must align with these new enterprise objectives ensuring a harmonised approach to the recovery. If the MTO is not exceeded and the MES is met the loss event is not a disaster.

Getting the essential services up quickly enough to satisfy your dependencies allows the enterprise to communicate to stakeholders from a position of control, and confidently predict full recovery from an informed perspective. Getting back to full service assures them of your competence and can win you business. It also assures your people that you plan on their behalf.

The appetite of the enterprise for risk is reflected in its preparedness for disaster. High risk companies typically are less prepared for loss events. Having a business continuity plan is not enough. The management needs to own the issue and regularly answer "what would happen if" questions. Most people see themselves in the role of superman when confronted with a loss event, but it does not work that way. Untested plans historically fail, whereas tested plans serve to increase awareness and train individuals in how to respond, thereby increasing the likelihood of a successful recovery. Key to a successful handling of a loss event is the clear separation of responsibilities. Two distinct teams are required, one to deal with the crisis and the communication to stakeholders and one to focus on the recovery. Good people will do extraordinary things to prevent a loss event becoming a disaster if they know the goals, MTO and MES, have a plan, tools and training in the loss event environment.

10 Steps To Business Continuity Planning		
Buy-In	1	Confirm Stakeholder buy-in
Resource	2	Put together a Business Continuity team ⇒ Representatives from each key function ⇒ Agree budget and resources
Assess	3	Conduct an Enterprise wide Risk Assessment ⇒ Aligned with Enterprise Objectives ⇒ Agree the Maximum Tolerable Outage (MTO)
Align	4	Carry out a Business Impact Analysis. ⇒ Focus on events that can cause a significant interruption ⇒ Identify Recovery Priorities ⇒ Define Recovery Time Objective (RTO) ⇒ Define Recovery Point Objective (RPO) ⇒ Define Minimum Essential Service (MES)
Develop	5	Develop Plans ⇒ Incident Assessment ⇒ Specific incident responses ⇒ Escalation procedures ⇒ Various Strategies (e.g. alternative site, remote working) ⇒ Crisis Management Plan ⇒ Resource Recovery Plan ⇒ Communications Plan
Communicate	6	Communicate Plans ⇒ Awareness Training ⇒ Policies and Objectives
Exercise	7	Test Plans ⇒ Test procedures ⇒ Exercise plans ⇒ Rehearse roles
Inform	8	Media Management Plans ⇒ Identify Stakeholders ⇒ Identify Spokesperson ⇒ Script Responses
Include	9	Key Supplier BC plans ⇒ Identify Mission Critical Suppliers ⇒ Review their plans
Maintain	10	Maintain Plans ⇒ Change Management ⇒ Update after Tests

The Experience of Others

In the 1993 World Trade Centre bombing, 150 out of 350 businesses affected failed to survive the event. Conversely, following the September 11 terrorist attack, businesses that had tested BCPs were operational within three days of the disaster.

A major factor in the effectiveness of the response by the Civil authorities in the Buncefield Oil Storage Depot incident in Dec 2005, was Hertfordshire County Council's Crisis Communications Plan. The plan had already been well and truly tested due to the Potters Bar and Hatfield rail incidents and had undergone a testing exercise during October 2005.

Planning takes the fun out of panic. When NASA heard the words "Heuston …….we have a problem" ---- one that wasn't in the BCP- the primary objective, the MTO and the MES changed and the enterprise had to deal with the loss event. You may well ask, what were they doing up there in the first place in a spacecraft with a number 13 painted on the side of it.

Planning informs the art of the possible and trains organisations to perform miracles under pressure.

Business Continuity Things That Only Cost You A Thought

1 Invite the local fire brigade to tour your premises.
2 Identify alternate contacts for each function in an emergency
3 Know your fax numbers, they may be the only phones that work in a power failure
4 Use your web-site as a notice board to communicate in an emergency
5 Keep a list of contact names and numbers in the glove box of your car.
6 Take your laptops home each day, but back 'em up before you go.
7 Restore from your backups periodically.
8 Set up contact SMS groups in your mobile phone.
9 Talk to the security people.
10 Keep a waterproof cover in your comms room.

Practice Best Practice

Avoiding Disaster – 3 Views

Consider loss events in three ways: Prior to the event occurring, Upon the event occurring and Post event. All mitigation initiatives need to be put in place before any loss event occurs, but each mitigation will have an impact either before, during or after the loss event occurs. Where enterprises have a low risk appetite the focus will be on preventing the event occurring. During the loss event, actions focus on minimisation and containment and post loss event tests the effectiveness of the Business Recovery Plan.

Plan before a loss event occurs.
Plan to make it not occur.
Plan to contain it when it does occur.
Plan to recover fully if you survive.

Plan for Prior	Plan for During	Plan for Post
Minimise likelihood	Ensure early detection	Have a BRP
Implement good policies and procedures for all activities	Ensure that all detection systems are regularly maintained/ serviced	Store copies of critical data offsite.
Train staff well	Monitor operation of key process systems continually	Determine membership of recovery teams
Ensure there is no over-dependency on any individual	Plan "courses of action" for key specific events	Test recovery plans regularly
Install resilient systems	Train staff in how to respond to specific events	Ensure that Insurance cover is appropriate for your activity
Build in redundancy	Put a clearly defined communication plan in place.	Have an offsite IT Disaster recovery plan in place
Build and operate to recognised standards where appropriate	Ensure appropriate "response times" are in place with suppliers	Have a Work Area Recovery plan in place for employees
Record and investigate incidents	Rehearse emergency response plans on a regular basis	Ensure an appropriate level of product / stock is maintained
Monitor and respond to changes in staff morale	Ensure that "response plans" take time of occurrence into account	Establish alternative suppliers for critical components / service
Measure key performance indicators and review results	Involve 3rd parties in response planning so they understand their role. E.g. fire department	Keep up-to-date records of all system configurations.

Plan to be the last one standing and the first one up!

	Business Continuity Checklist	✓
1	Do you have a documented and approved BCM policy?	
2	Do you have a clearly defined telecommunications recovery plan?	
3	Do you have a clearly defined IT recovery plan?	
4	Do you have a documented Crisis Management Plan?	
5	Are people's roles in an emergency clearly defined and approved?	
6	Have you got the telephone numbers of all key staff and a Call Cascade plan in place?	
7	Do you have the contact details for all key-suppliers documented in your plan?	
8	Has a Work Area Recovery strategy for Mission Critical Applications, their support activities and operators been developed and documented within the BCP?	
9	Do you know how long your UPS will supply power in the event of a power outage / generator failure?	
10	Do you have back-ups of all key data off-site?	
11	Have you tested your data restore procedure in the past 12 months?	
12	Do you have a procedure for bringing all servers down in a controlled fashion?	
13	Are all insurance policies reviewed annually for relevance and adequacy?	
14	Have you conducted an evacuation drill in the past 6 months?	
15	Have you conducted a Business Impact Assessment in the past year?	
16	Do you control all work done by contractors on your premises using Work Permits?	
17	Do key systems transmit alarms to individuals in the event that they develop a fault, whatever the time of day?	
18	Do you have a policy that ensures that there is no over-dependence upon single individuals for any key task?	
19	Do the users of key systems have emergency plans in the event of a system outage?	
20	Does the organization have a clearly defined change control process to ensure BCM requirements and selected BCM solutions are maintained in an up-to-date and fit-for purpose status?	
21	Does the organization have a clearly defined, documented and approved BCM exercising cycle and programme?	

LinkResQ Ltd., 4200 Atlantic Avenue, Westpark, Shannon, Co Clare, Ireland
Tel: +353-61-477 888, email: @linkresq.ie, web: .linkresq.ie