BUSINESS CONTINUITY AND THE CLOUD

Bruce Swallow
CPIT
Madras Street
Christchurch
+6439408000
Bruce.swallow@gmail.com

Alison Clear
CPIT
Madras Street
Christchurch
+6439408000
Alison.clear@cpit.ac.nz

ABSTRACT
This paper seeks to examine the concepts of Business Continuity Management, Disaster Recovery and Cloud Computing. It explains the theory behind each of these concepts and attempts to show how they are or can be related. The paper shows that business continuity management and disaster recovery are related insofar as disaster recovery is a subset of business continuity management practice. The paper relates cloud computing to disaster recovery and business continuity management by examining the implication, benefits and risks of adopting cloud computing from a continuity standpoint. This is considered from two sub-perspectives: issues in continuity management for cloud computing services and issues in using the cloud for continuity management services and tools. We begin with an examination of the reasons that organisations should consider continuity issues. To clarify these we examined the importance of ICT to organisations.

Categories and Subject Descriptors
K.3.1 [**Computers and Education]**: Computer Uses in Education – *collaborative learning, computer-assisted instruction (CAI), computer-managed instruction (CMI), distance learning.*

General Terms
Management, Documentation, Performance, Economics, Reliability.

Keywords
Cloud Computing, Disaster Recovery, Business Continuity Management.

1. INTRODUCTION
An organisation's Information and Communications Technology (ICT) infrastructure is now one of its most important assets. The prolonged failure of ICT systems or the extensive loss of data can determine whether an organisation is able to continue to operate with the same level of success, or continue to operate at all [2]. Organisations now rely on ICT systems to carry out tasks that were traditionally manual, meaning that even short periods of downtime can be disproportionately damaging [11]. These tasks range from the traditionally IT based, such as accounting functions to the traditionally analogue, such as telephony and customer communications. ICT systems are now integral to many, if not all, of the business processes in many organisations [6].This means that any ICT failure can have effects that spread throughout an organisation. The external parties that an organisation has dealings with, such as its customer, vendors and shareholders, all have expectations of organisational continuity. ICT disruption can have serious continuity consequences and these consequences can damage the organisation by affecting its relationship with external stakeholders [6]. Brandabur [5] argues that the current economic climate has led firms to look for accurate and reliable valuation data, to attempt to cut costs and to seek competitive advantage. These are areas in which ICT can be valuable, and as such ICT has become of even greater importance to organisations. Furthermore, the importance of ICT is borne out by the finding that some 90% of organisations that lose data in a disaster close within two years [2].

This poster paper appeared at the 4th annual conference of Computing and Information Technology Research and Education New Zealand (CITRENZ2013) incorporating the *26h Annual Conference of the National Advisory Committee on Computing Qualifications*, Hamilton, New Zealand, October 6-9, 2013. Mike Lopez and Michael Verhaart, (Eds).

2. BUSINESS CONTINUITY: AN OVERVIEW
The critical and vulnerable nature of ICT systems means that their preservation and continued operation in adverse conditions is essential to an organisation's efforts to remain viable. Business Continuity Management (BCM) and Business Continuity Planning (BCP) -the terms are frequently used interchangeably- attempt to provide organisations with the tools and concepts to enable this.

2.1 Possible Continuity Incidents
The broadness of possible causes of continuity incidents is illustrated in the literature. It identifies, at the very least, the following:

- Naturally occurring: events such as hurricanes, floods, earthquakes, wildfires, heat waves, blizzards and epidemics [8] [2]
- Man-made: crime, conflict, embargo, blockade, war, terrorism, sabotage, poor training, data destruction, data integrity, data security, transportation accidents and the like [10] [2]

The man-made causes can be further broken down into internal and external threats. Threats like arson and embargo usually result from actors external to the organisation, whereas human-error related threats, such as poor training leading to data loss, frequently come from within. External threats can be further broken down into conflict and non-conflict types [10]. Conflict types include war and war –like circumstances as well as riots, extreme political change or strikes. Non-conflict types include economic issues, corruption, attacks on reputation and so on.

Al Badi et al [2] report that 43% of disasters, as defined from an organisational perspective, are caused by human error, 39% by power failure, but only 9% are related to natural disasters.

ICT systems are vulnerable to a large number of possible "continuity incidents". These incidents can be man-made or naturally occurring, and can originate internally or externally to the organisation. They range from natural disaster to hacking and data theft.

3. THE CLOUD AS A BUSINESS CONTINUITY TOOL

The intention of this paper is to consider the suitability issues surrounding the use of cloud computing as a business continuity tool. As such it is important to gain an understanding of what we mean by "cloud computing" and what the key concepts are.

3.1 Definition

Even a cursory examination of the extant literature will reveal a large number of definitions for the term "cloud computing". A number of these are presented below:

- "the essential characteristics of cloud computing: on-demand self-service, broad-network access, resource pooling, rapid elasticity, and measured service" [1]
- "both the applications delivered as services over the internet and the hardware and systems in the data centres that provide those services" [3]
- "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" [9]
- "Cloud computing is the use of computing resources, hardware as well as software, that are delivered as a service through a network, typically the Internet" [7]

3.2 Cloud Computing Benefits

Wood et al identify a number of benefits of using the cloud for Disaster Recovery [11]. Cost savings may accrue for applications that require only warm site levels of functionality. Applications that only require a loose Recovery Point Objective will accrue even greater savings. Cost savings may be realized through the pay-as-you-go model, with the elasticity of the cloud meaning that users can gain access to and pay for resources only as they need them, rather than traditional models that involve provisioning for the greatest expected load [11]. It may also lead to lower management and maintenance costs, with these functions being handled externally by the cloud provider.

Adoption of cloud services for everyday functions may have the benefit of "warming" any recovery site that an organisation may need. By utilizing cloud administration applications, such as word processing and email services, an organisation may be able to maintain the appearance of "business as usual" despite being forced from their regular premises by a localized event like a fire. It is possible that many operations could continue with as little as a computer and internet connection, allowing the organisation to at least maintain contact with stakeholders.

Many large organisations already use thin clients and data centres to gain cost advantages. The expansion of cloud services has the potential to spread this to smaller organisations, not only reducing their capital costs but reducing the cost of continuity by necessitating the replacement of much less expensive equipment.

The cheapest way to utilize the cloud for DR/BC is simply to use it for data backup. Backup can be done to local drives, and then these drives can be mirrored to cloud storage. This is especially useful if the disaster situation is a localized one, and not a region-wide situation. The procedure can also be automated, and done at off-peak hours, at no extra labour cost [4].

Furthermore, organisations may be able to generally reduce their RTOs through the ability to rapidly provision in the face to mounting needs. If a live local server is affected they may be able to rapidly, if not automatically, failover to a cloud service that already contains their backed-up data, rendering their RTO mere minutes.

4. CONCLUSION

Cloud computing is, briefly, the provision of computing resources via the internet. These resources can be provided on a private or public basis, or a combination thereof. A number of benefits and risks are argued to accrue from cloud computing adoption. The benefits range from cost reduction to management effort simplification. The risks encompass issues from performance to security to data lock-in. These risks and benefits have significant consequences for business continuity planning.

5. REFERENCES

1. Alali, F., Yeh, C., "Cloud Computing: Overview and Risk Analysis" *Journal of Information Systems,* Fall 2012; 26, 2
2. Al-Badi, A., Ashrafi, R., Al-Majeeni, A., Mayhew, P., "IT disaster recovery: Oman and Cyclone Gonu lessons learned" *Information Management & Computer Security,* 2009; 17, 2.
3. Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I., Zaharia, M, "A View of Cloud Computing" *Communications of the ACM,* April 2010; 53, 4
4. Beckman, M., "Using the Cloud for Business Continuity", System iNEWS, Jan 2012, pg. 9
5. Brandabur, R.E, "IT Outsourcing – A Management-Marketing Decision", *International Journal of Computers, Communications & Control,* April 2013; 8, 2
6. Calderon, T. G., Dishovska, M., "Transitioning from Disaster Recovery Management to Business Continuity Management" *Internal Auditing,* Mar/Apr 2005; 20, 2
7. Catherine, M. R., Edwin, E. B., "A Survey on Recent Trends in Cloud Computing and its Application for Multimedia" *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)* Volume 2, Issue 1, January 2013
8. Kadlec, C., Shropshire, J., "Best Practices in IT Disaster Recovery Planning Among US Banks" *Journal Of Internet Banking and Commerce,* April 2010; 15, 1
9. Mell, P., Grance, T., "The NIST Definition of Cloud Computing" *NIST Special Publication 800-145,* National Institute of Standards and Technology, September 2011
10. Shaluf, I. M., Ahmadun, F., Said A., M., "A review of disaster and crisis" *Disaster Prevention and Management;* 2003; 12, 1; ProQuest Central pg. 24
11. Wood, T., Cecchet, E., Ramakrishnan, K.K., Shenoy, P., van der Merwe, J., Venkataramani, A., "Disaster Recovery as a Cloud Service: Economic Benefits and Deployment Challenges" http://static.usenix.org/event/hotcloud10/tech/full_papers/Wood.pdf, retrieved on 03/03/2012 at 11:35am