Week 09 Assignment 9-3

William Slater

CYBR 625 – Business Continuity Planning and Recovery

Bellevue University

Business Continuity Planning and the Small Business

Sue Sampson, M.S. - Professor

October 28, 2012

Business Continuity Planning and the Small Business

Mr. Seger's brief article, that was written and published in October 2012, BUSINESS CONTINUITY PLANNING FOR SMALL BUSINESSES first makes the point that a Business Continuity Plan (PCP) is not the same thing as a Disaster Recovery Plan (DRP, and that a BCP is required to get a business back up and in operation (Seger, 2012).

The first step that Mr. Seger is necessary is to understand how many BCP plans will be necessary or if there will be one central umbrella plan that will be available for use to reconstitute business operations. The next step is to understand the critical business functions that must be documented and then use a standard template to document these business functions. For accuracy, quality and integrity, Mr. Seger suggests getting the buy-in from each employee by telling them that these are critical business functions required for the business to operate, and that since the business is their livelihood, it is essential to have accurate and quality inputs from each employee. I believe that this is especially true in a small business where things often are so fast moving and chaotic that people rely on "tribal knowledge" with which to operate the business (Seger, 2012).

One method Seger uses to capture the most important critical business functions is to have employees write down every task they would need to perform within the first 48 hours after a disaster. He believes that this exercise helps put employees in the mindset of the urgency to understand the most essential tasks to start reconstituting the business operations of a small business (Seger, 2012).

Mr. Seger also uses the BCP to capture and categorize all the necessary resources to reconstitute a business. The idea here is that a planner wants to be as thorough as possible to ensure that the business's operations will not be impeded by lack of the necessary resources (Seger, 2012). In this section, however, he is vague and states that not all vendors must be contacted, and that whether or not they are contacted will be based on the seriousness of the event. In my estimation, more definitive structure and guidelines should be provided as to the different types of events that can occur and who should be called and when they should be called.

For purposes of simplicity and standard organization, Seger advocates organizing the BCP for each of the department into the following sections: Recovery Procedures, Departmental Overview, Critical Functions, and Key Resources. He also advocates providing cross functional documentation that provides the ways and order in which the people utilizing each of these plan sections may be required to interact and exchange information (Seger. 2012).

Finally, Seger advocates the use of testing exercises, maintenance, and after-action reports, as well as ensuring that all active participants have a personal copy of the plan, so that they will be prepared to act if and when a disaster should occur (Seger, 2012).

This short 1400+ word article provided some good general guidelines for the average small business. However, I believe that Seger should have also emphasized just how critical it is for even small businesses to have such BCPs, and the consequences when they fail to have such

plans. After two spectacular disasters, one in 1992 with the Great Chicago Loop Flood, and one in 1993 with the first World Trade center bombing, one survey showed that over 50% of all businesses, when denied access to the data and information required to operate their business, would be out of business in 12 months or less. This fact alone highlights the need for every business, no matter the size, to have a DRP and a BCP, and to keep it updated.

Dr. Susan Lincke, a professor from the University of Wisconsin at Milwaukee, working on a grant from the National Science Foundation in 2010 - 2011 completed the Small Business Information Security Workbook (SBISW). This free resource is a well-designed, well-written, easy to use 87-page document helps walk a small business through the essentials of understanding and applying sound principles and practices of Information Security. The SBISW uses three distinct structured processes and documents to complete a Business Continuity Planning:

- **"Business Impact Analysis**: An analysis of which business functions and finances would be most affected by a problematic event or disaster.
- **Business Continuity Plan**: A business plan for how the organization should resume service, following a disaster.
- **Disaster Recovery Plan**: A technical plan for how IT should resume service following a problematic event or disaster."

(Lincke, 2012)

What makes Dr. Lincke's approach particularly effective is the use of a process that lists the types of types of disasters that can impact a business showing the typical severity that they have on the business. See the table with Incidents and Impacts from the SBISW below:

Problematic Event or Incident	Affected Business Process(es)	Impact Classification and Effect on finances, legal liability, human life, reputation
Fire	Patient Treatment Patient Scheduling	Crisis: For 1-3 months
Hacking incident	Patient Treatment Patient Billing	Crisis: Human life, liability, rep. Minor
Network Unavailable **(E.g., ISP problem)**	Affects remote access: Patient Treatment Patient Billing Insurance Management	 Major (if at hospital) Minor Minor
Social engineering, fraud	May affect: Remote access, financial stability, reputation, insurance	Crisis: Could affect: Legal liability, human life
Medical Server Failure **(Disk/server)**	Patient Scheduling Patient Treatment Insurance Management	Major Major (Human Life) Minor
Server Failure **(Disk/server)**	Financial analysis, Personnel	Minor Minor
Power Failure	Patient Scheduling Patient Treatment Insurance Management	Major Major (Human Life) Minor

Table 3.3.1: Incidents and Impacts (Lincke, 2012)

Unlike Seger's brief article, Lincke's ***Incidents and Impacts*** table serves to help the management of a small business thin about the unthinkable, and I believe that this can be an effective motivator to act proactively and create the necessary BCPs.

In another useful table, Dr. Lincke has the planner address the methods with which the business would designate controls to minimize its downtime. See below.

Business Process	**RPO (Hours)**	**Data File and System/Directory Location**	**Special Treatment (Backup period, RAID, File Retention Strategies)**
Patient Schedule	0 hours -1 day	Medical DB	Local RAID, Off-site backup to KSC daily. Encrypted backup at KSC.
Patient Treatment	0 hours - 1day	Medical DB	Local RAID, Off-site backup to KSC daily. Encrypted backup at KSC
Insurance	1 day	Medical DB	Local RAID, Off-site backup to KSC daily. Encrypted backup at KSC

Table 3.3.3. RPO Controls (Lincke, 2012)

Perhaps the most valuable visual in Dr. Lincke's write up on Business Continuity Planning is this diagram showing the Recovery Point Objective and the Recovery Time Objective associated with a business attempting to recovery from a disaster and resume its business operations:

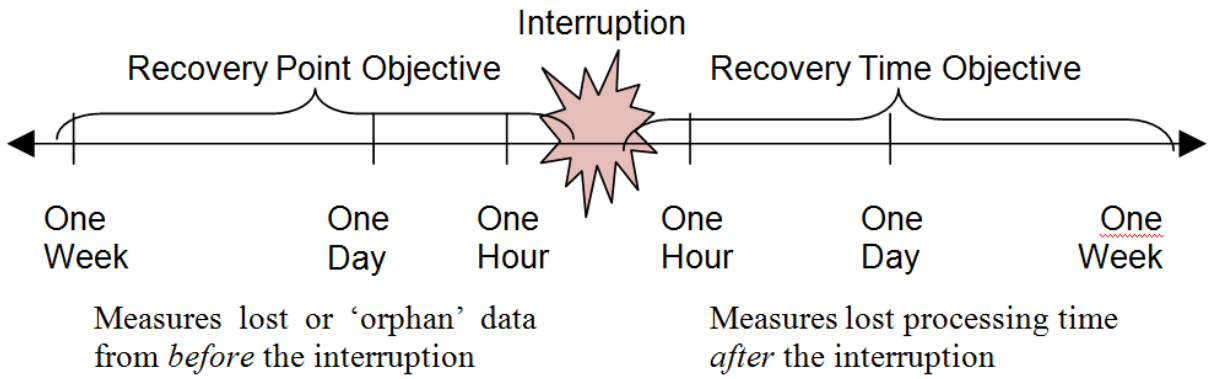

Figure 1 – Recovery Point Objective and Recovery Time Objective shown with a Business Interruption (Lincke, 2012)

Such visual diagrams help a small business owner start to understand a business interruption in the same ways that management and planners in medium and large companies have been dealing with these topics over the past 10 to 12 years.

Another free and useful resource for small business owners who seek to create BCPs is a document titled the Small Business Information Security: The Fundamentals, by Richard Kissel. This was published by NIST in 2009. While this is a useful reference, Mr. Kissel uses a general approach that is not as detailed as Mr. Seger's approach. He advises that businesses should be prepared for disasters and that they should categorize their essential data and information resources along with their locations in a table and then in another table, document how that those resources are protected (Kissel, 2009).

Implementing a Business Continuity Plan and the Small Business

On another note, I am presently at the beginning phase of an ISO 27001-based Information Security Management System implementation for a small software business. They generate about $7 million per year in revenue and they are required to go through this effort to enable a business relationship with a major online university. Annex A.14 of the ISO 27001 standard requires the development and regular testing of a Business Continuity Plan, so I will soon become part of the process of creating their Business Continuity Plan so that it will meet the requirements necessary to pass an ISO 27001 certification audit and achieve an ISO 27001 certification (ISO, 2005).

Conclusion

It is essential that every business needs to take business continuity seriously. From these three approaches, ranging from general high level advice (Seger and Kissel), to a structured detailed approach that includes scenarios, categorized impacts, as well as Recovery Point Objectives, Recovery Time Objectives and suggested controls, it is obvious that a quality solution can be identified and utilized without a lot of effort. It is therefore necessary for the owners and leaders in a small business to take seriously the responsibility of ensuring that business operations can continue in adverse situations, and take a mature approach to designing and building the best BCP and DRP solutions that it can afford. The very survival of a small business will depend on thinking about, planning for, and preparing the key members of the business for the unexpected disaster.

References

Gregory, P. (2008). IT Disaster Recovery and Planning for Dummies. Indianapolis, IN: Wiley Publishing.

ISO. (2005) "Information technology – Security techniques – Information security management systems – Requirements", ISO/IEC 27001:2005.

Kissel, R. (2009). Small Business Information Security: The Fundamentals. A document published in October 2009 by the National Institute of Standards and Technology. Retrieved from http://csrc.nist.gov/publications/nistir/ir7621/nistir-7621.pdf on May 3, 2012.

Lincke, S. (2012). Small Business Information Security Workbook, version 3.0. Retrieved from http://www.cs.uwp.edu/staff/lincke/infosec/notes/SecurityWorkBook.doc on August 25, 2012.

McCumber, J. (2008). Assessing and Managing Security Risk in IT Systems: a Technology-independent Approach. Retrieved from the web at https://buildsecurityin.us-cert.gov/swa/downloads/McCumber.pdf on August 31, 2011.

Seger, C. (2012). BUSINESS CONTINUITY PLANNING FOR SMALL BUSINESSES. An article published at the Continuity Central website. Retrieved from http://www.continuitycentral.com/feature1016.html on October 28, 2012.

Whitman, M. E. and Mattord, H. J. (2007). Principles of Incident Response & Disaster Recovery. Boston, MA: Course Technology – Cengage Learning.