Disaster Recovery

Submitted to

Diane Kinderwater, Instructor
Department of Office Administration
Grande Prairie Regional College

Prepared by

Alexandra Grosset
OA2081 EC
Department of Office Administration

January 24, 2014

DISASTER RECOVERY

Businesses need to face the fact that disaster can strike at any moment. It can be ugly, but it does not have to be disastrous. From losing revenue to going out of business, companies need to have a disaster recovery plan in place to deal with such situations. For a small or large business, it is rather like an information insurance policy. A disaster recovery plan refers to "a plan developed and implemented to provide guidance for protecting records and information and continuing business operations when emergencies and disasters occur"[1]. This plan usually is written in step-by-step format and is very detailed, but it can be a vital resource for a business on how to quickly recover after a devastating disaster. Alternative names for a disaster recovery plan may include "contingency plans, emergency plans, or disaster plans"[2].

There are two types of disasters: natural and manmade. A natural disaster results from the earth's natural hazards and usually displays hostile weather behavior. Some examples of natural disasters include "floods, tsunamis, tornadoes, hurricanes/cyclones, volcanic eruptions, earthquakes, heat waves, and landslides. Other types of disasters include the more cosmic scenario of an asteroid hitting the Earth"[3]. In contrast, manmade disasters can be intentional or unintentional consequences of technological or human hazards. Examples of intentional manmade disasters can include sabotage or terrorism, whereas unintentional manmade disasters can include accidents like the destruction of a manmade dam. Other examples of manmade disasters include "stampedes, urban fires, industrial accidents, oil spills, nuclear

[1] Read, Judith, and Mary Lea Ginn, "The Records and Information Management Program," *Records Management*, 2008, pg. 394
[2] Read, Judith, and Mary Lea Ginn, "The Records and Information Management Program," *Records Management*, 2008, pg. 394
[3] *Wikipedia.* Accessed January 22, 2014. <http://en.wikipedia.org/wiki/Disaster_recovery_plan>

explosions/nuclear radiation and acts of war. Other types of manmade disasters include the more cosmic scenarios of catastrophic global warming, nuclear war, and bioterrorism"[4]. Since we are living in an information era, computers are also vulnerable to attack. Information security experts tend to computer threats like viruses, cyber-attacks, and hacking, just to name a few.

When discussing the topic of disaster recovery, it is important to know the difference between an emergency and a disaster. An emergency is a sudden event that requires urgent attention. For instance, a broken water pipe, a bomb threat, or an unexpected storm would be described as an emergency. These events do not typically result in major damage or disturbance to the business. However, a disaster is an unforeseen emergency event that does typically result in major damage or disturbance to the business. Unfortunately, significant financial damage usually results. For instance, a fire, a flood, or a tornado would be identified as a disaster.

There are three phases of a disaster recovery plan: disaster prevention (also called criticality analysis), preparedness (or recovery plan development), and recovery (or active testing). In the first phase, actions are taken to decrease the chance of damage caused by an emergency. These actions diminish the possibility that they will turn into records information management disasters, should an emergency arise. Examples of such actions include determining what type of disasters you are planning for, deciding the goal of the disaster recovery plan, and recognizing which computer applications need to be recovered first. In the second phase, the business basically prepares to respond when an emergency happens. This is

[4] *Wikipedia.* Accessed January 22, 2014. <http://en.wikipedia.org/wiki/Disaster_recovery_plan>

so employees know what to do and who to call once an emergency is identified. "Responding to an emergency event means activating resources necessary to protect the organization from loss."[5] Examples of such actions include deciding roles and responsibilities, recording who does what, when, and how, and recording procedures for disaster recovery (constructing a plan of action). The third phase involves actions that are needed to restore the business quickly and testing them out. Basically, this phase determines what courses of action to employ that will keep the business actively producing products and services as well as keeping customers. Examples of such actions include "dehumidifying records, restoring data onto computers, and returning vital records from offsite storage"[6].

Risk assessment is a major part of the disaster recovery planning process. It is crucial to consider all types of probable incidents, as well as the effect each one may have on the company's ability to function normally. This step involves figuring out which incident is most likely to happen and prioritizing them in regards to risk (low, medium, or high). For instance, one company could rate a power outage as a higher risk than an earthquake. This would mean that it would be classified as a higher priority in their disaster recovery plan. As you can see, a disaster recovery plan is unique to its company.

In general, disaster recovery encompasses many different types of issues. Businesses need to create a complete and thorough disaster recovery plan, but also update it regularly. "An effective plan is a live plan and must be revised on an ongoing basis. At least once a year,

[5] Read, Judith, and Mary Lea Ginn, "The Records and Information Management Program," *Records Management*, 2008, pg. 394

[6] Read, Judith, and Mary Lea Ginn, "The Records and Information Management Program," *Records Management*, 2008, pg. 394

organizations should conduct a complete test to confirm that the plan is appropriate and workable."[7] It is better to be safe than sorry.

[7] *Certified General Accountants Association of Canada.* Accessed January 22, 2014. <http://www.cga-canada.org/en-ca/AboutCGACanada/CGAMagazine/2004/Nov-Dec/Pages/ca_2004_11-12_ft1.aspx>

Works Cited

Certified General Accountants Association of Canada – http://www.cga-canada.org/en-ca/AboutCGACanada/CGAMagazine/2004/Nov-Dec/Pages/ca_2004_11-12_ft1.aspx [January 22, 2014]

DevX – http://www.devx.com/security/Article/16390 [January 22, 2014]

How Stuff Works – http://money.howstuffworks.com/business-communications/how-disaster-recovery-plans-work.htm [January 22, 2014]

Read, Judith, and Mary Lea Ginn, "The Records and Information Management Program," *Records Management*, 2008.

The Disaster Recovery Guide – http://www.disaster-recovery-guide.com/risk.htm [January 22, 2014]

Wikipedia – http://en.wikipedia.org/wiki/Disaster_recovery_plan [January 22, 2014]