

Disaster Recovery in a Data Processing Environment

Protecting Your Agencies' Assets

Prepared by: Stephen G. Tucker

Division of the State Chief Information Officer

South Carolina Budget and Control Board

Submitted: February, 2007

Introduction

The more our agencies' business relies on its information technology (IT) systems, the more we need to consider how unexpected disruptions would affect the mission of the agency. These disruptions could come in many forms, from fire and floods, theft, malicious attacks on our systems, such as hacking to areas we might never consider (see Appendix A).

Disaster recovery planning (DR/DRP) improves our agencies' ability to react to such disruptions. It describes how we will restart our operations in order to meet our agency-critical requirements. This paper will explain the importance of disaster recovery plans to the success of our agencies, and the stages we need to go through when developing them.

What is disaster recovery planning?

Disaster recovery planning is the process of planning for the unexpected. An effective plan will provide us with procedures to minimize the effects of unexpected disruptions. The plan should enable our agencies to recover quickly and efficiently, with the minimum disruption to our day-to-day activities.

Disaster recovery is a process developed to counteract systems failure. It is a management issue, not something that should just be considered by the IT department. If the IT systems fail or are unavailable, it is likely to have a significant impact upon the whole agency. Therefore we should take an active interest in establishing disaster recovery plans for our IT systems.

Disaster recovery supports the ability of the agency to recover. This includes:

- Providing facilities and services to enable the agency to continue to function;
- and

- Providing the critical IT applications and infrastructure necessary to support the recovery of agency processes

Once a disaster recovery plan has been written and implemented, it is the start of an ongoing commitment. Agencies constantly evolve, and recovery strategies must evolve with them. For example, as people join, transfer, retire or otherwise leave an agency, plans must be updated to reflect changes in recovery teams. Also, new IT systems could be introduced. These may be essential to the agency. If so, we must build their recovery into our plans. New legislation or reorganization could greatly change the missions of the agency.

Plans should be clear and concise; to ensure that people will read it. Make it available to all staff members responsible for any part of the plan. Summarize it for the rest of the staff so that they will know what to expect.

The benefits of disaster recovery planning

A disaster recovery plan minimizes the disruption to our agencies from any unexpected events or disasters. Staff will know their responsibilities in such situations, and will be able to respond to the events by following an agreed procedure. This will ensure that our agency-critical systems are up and running in the shortest possible time.

There are additional benefits of having a disaster recovery plan in place. First, there are regulatory requirements to have a recovery plan in place (see Appendix B). There are also additional Federal requirements pertaining to recovery of sensitive and time-critical data. In addition, an agency that can demonstrate an effective disaster recovery plan has a competitive advantage. For example, if we provide a service to a customer that is dependent upon the IT systems, like an Internet service provider, then evidence of a sound plan may provide us with an

advantage that can be used to win or retain customers. For instance, if our agency is a partner in a service delivery chain, disaster recovery planning may well need to be an integral part of our quality assurance.

Effective disaster recovery management will help agencies demonstrate that we are managing our business risks and so help to secure lower insurance premiums. In addition, drawing up a disaster recovery plan can help us assess what types of insurance we need the most, as identifying likely business risks is part of the planning exercise. This is because disaster recovery planning may help to identify potential business risks we were previously unaware of, but which we recognize that we now need to insure against. Therefore, we may decide to opt for lower insurance coverage across a broader range of risks - the original risks plus the recently identified ones - in order to remain within our budgeted insurance cost.

Risk assessment and impact analysis

The first step in disaster recovery planning is to do a risk assessment. This will help us to decide which threats on which to concentrate. It involves:

- Identifying the range of threats that the agency faces;
- Assessing their potential impact on the agency; and
- Assessing the likelihood of each threat occurring

Assessing the potential impacts of unexpected events is called impact analysis. We must consider how much our agency stands to lose because of each possible type of disaster or service disruption.

To assess potential impact we should identify the critical agency processes and the potential damage or loss that the agency would suffer if any of these services were disrupted. The damage can be measured in hard terms such as financial loss, or in soft terms such as political

embarrassment or loss of credibility to the agency. We must also consider how any damage or loss will increase if the disruption lasts a long time. For example, what would be the impact to our agency if our e-commerce site was down for a day rather than an hour? How about our Sexual Offender Registry or a social benefits site? For some agencies, this may mean the difference between a temporary loss of information and people being fired. Having determined the impact of each threat, we should decide how likely, each threat is to occur. This will help us decide which threats to prioritize in disaster recovery planning.

Components of a disaster recovery plan

We will use information on threats to our agencies to start our disaster recovery plan. These were gathered in risk assessment and impact analysis. The plan should aim to reduce the risks posed by disruption to our agencies' processes. Measures that may be needed include:

- A back-up and data recovery strategy, including off-site storage;
- The development of a resilient IT infrastructure with redundancies in case of failure. For example mirrored central server computers sited in different locations, each containing the same information, so that if one goes down the other one is available to ensure continuity of service and alternative storage facilities;
- The elimination of single points of failure, such as a single power supply; or
- The introduction of an uninterruptible power supply for our IT systems. This device allows the computer to keep running for a short time when the main power supply is lost. It uses a battery that takes over when power is lost and gives us time to save any data that we may be working on.

Even if such measures are adopted, things can still go terribly wrong. In the event of a disruption or disaster, the disaster recovery plan should specify when actions should begin and what actions are to be taken in order to recover from this event, covering such items as:

- People and accommodation;
- IT systems and networks;
- Services such as power and telecommunications; and
- Critical business processes

Methods of recovery might include:

- Carrying out activities manually until IT services are resumed;
- Staff at an affected building moving to another of the business' offices;
- Agreeing with another business to use each other's premises in the event of a disaster; or
- Arranging to use IT services and accommodation provided by a specialist third-party standby site

The disaster recovery plan should be kept short and readable. It should not duplicate other sources of information, and any other relevant documents should be referenced. Encourage staff to review the plan before it is formally issued.

Testing the IT disaster recovery plan

Testing a disaster recovery plan can be difficult. Simulating potential threats to our agencies can be time consuming, expensive and possibly disastrous to our data. However, testing our disaster recovery plans will help show whether we have covered all angles, and whether our plan is achievable. In addition, it can increase our served citizens and other agencies' confidence in our business' ability to recover from disruption. Tests are also useful to raise staff awareness of the

plans. We can test whether staff can function without access to data cheaply and easily. Such tests can also help to check that other sources of data, such as back-ups or archives that are held off-site, are sufficiently up-to-date.

At some point, usually around 12 months after the plan has been developed, we should carry out a real restore of data - use data that has been backed up to get our system fully operational again - and attempt to work without premises or files. This will help to establish:

- Whether the expected timescales for recovering key business applications are realistic;
- How prepared the staff is for putting the plan into action; and
- Whether any third parties or service providers who are integral to the plan are ready to respond

We also should ensure that any test we undertake, whether technical - relating to the operation of the IT systems - or non-technical - relating to all associated activities - has clear objectives. For example, to measure the time needed to get our main IT systems running following a disruption or to test how long it takes to contact all key personnel in the event of a disaster. This will enable us to measure the success, or otherwise, of each exercise, and highlight areas in need of further attention. Any initial testing should be followed by further tests on a regular basis. In particular, details of any changes to IT systems should be included in the plan and tests should be undertaken on the new systems.

Education and training in IT disaster recovery

All staff members must be aware of the importance of disaster recovery planning. Training and awareness are important to make sure that the staff fully understands the plan and the role they will play in it. Awareness can range from simple knowledge of the assembly points should the

building have to be evacuated; through to the exact role each member of staff will have in the event of a disaster or unexpected event. Awareness training should be undertaken on a regular basis, and included in any staff induction programs. Staff who will have specific responsibilities in the recovery of IT systems should be given further technical training. This will ensure that they are able to recover systems and applications quickly and efficiently.

Any third parties who have a critical role in the disaster recovery plans should be part of this awareness training. If, for example, we have set up office-sharing arrangements with another agency, then they need to know the procedures that will be followed if our office becomes unavailable. We will also wish to include training for any member of staff who may need to talk to the media in the event of a disruption or incident. This is particularly important as the reputation and public perception of our agency is key to its ongoing success.

Key steps in developing a disaster recovery plan

There are five key stages in developing and maintaining a disaster recovery plan.

Stage 1-Understanding our Business

- Project initiation and management - get support from senior managers. Establish a management structure to develop and carry out the plan.
- Risk evaluation and control - identify the threats and the best defense. For example, with e-commerce, computer viruses might be a major threat - the appropriate defense might be regularly updated anti-virus software. See the page in this guide on risk assessment and impact analysis.

- Business impact analysis - establish the business' critical processes and identify the impact of any failures. For example, if our e-commerce website is critical to our operation, what would it cost our agency if it were down for 24 hours?

Stage 2-Disaster Recovery Management Strategies

- Develop an organizational disaster recovery strategy, identifying areas on which to concentrate. Focus on the critical operating requirements of the business, as identified above.
- Develop a process-level strategy - a documented framework clearly stating how critical processes will be restarted following an incident or failure. For example, if the payment system for our e-commerce website goes down, we will need a specific strategy for resuming operations.

Stage 3-Developing and Implementing a Disaster Recovery Response

- Emergency response and operations - establish a crisis management process to respond to incidents. Find out about crisis management at the Continuity Central website.
- Develop and implement a disaster recovery plan. This describes specifically how we will deal with incidents. Focus on the priorities of the overall disaster recovery strategy.
- Put in place business unit plans for each department. For example, detail the actions that the IT department will have to carry out if IT services are lost.

Stage 4-Developing a Disaster Recovery Management Culture

- Awareness and training plans - ensure all staff are aware of the importance of disaster recovery and can operate effectively following an incident.

- Review the effectiveness of awareness training periodically. Identify any further training needed.

Stage 5-Exercising, Maintenance and Audit

- Test the disaster recovery plans. Test any technical aspects - for example if we plan to use backed-up data to restore operations. Carry out full live exercises to establish how the plans work in a disaster situation.
- Maintain the plans - ensure that the documentation remains accurate and reflects any changes inside or outside the business.
- Regularly audit the plans - do they meet the needs of our strategy? Act on the findings.

Summary

I have an opportunity to meet with a number of the larger agencies on a regular basis. While exact data is hard to come by, most agree that they are in the infancy stages on the development of a true Disaster Recovery Plan. Most claim to have some form of backup and recovery. But, when asked if they have tested that plan, all reply "NO". If asked if their data was stored offsite, most replied "I think so" or "I don't know". I sincerely hope that thru my job at the Division of the State Chief Information Officer, I can promote the writing of Disaster Recovery Plans and the full implementation of these plans. The functions performed by most agencies, especially in the health and safety areas, are much too critical to the citizens of South Carolina to be left to the false hope that a disaster will never happen to them. Trained professional at the State CIO's division are available to assist any governmental agency with the development and implementation of a Disaster Recovery Plan.

Please understand that this paper was written to show the importance of having a Disaster Recovery Plan in place. It was not designed to be a template for that Plan. Actual creation and

implementation of a DR plan requires time, money, people and above all, senior management commitment. By reviewing some of the referenced documents, we can decide which options we wish to choose, how much we wish to spend and how much Disaster Recovery we need.

If you think it could not happen here, visit the SC Department of Archives and History. This site has a wealth of information for State agencies:
<http://www.state.sc.us/scdah/disaster.htm>

For further information, contact:

Steve Tucker
Manager, Level II Support Center
Division of the State Chief Information Officer
(803) 896-0139

REFERENCES

Business Continuity Planning / Disaster Recovery Planning -- An Online Guide
<http://www.yourwindow.to/business-continuity/>

Business Continuity Planning Model, By Disaster Recovery Institute, International
<http://www.drj.com/new2dr/model/bcmodel.htm>

National Fire Protection Association, NFPA1600 Standard on Disaster/Emergency Management and Business Continuity Programs, 2004 Edition
<http://www.nfpa.org/assets/files/PDF/NFPA1600.pdf>

South Carolina Enterprise Architecture, Business Continuity, Disaster Recovery Best Practices, V1.0 – January 24, 2007
<http://www.cio.sc.gov/cioContent.asp?pageID=539>
<http://www.cio.sc.gov/SCEA/sms/sms-DisasterRecoveryBestPracticesa.pdf>

Appendix A

Environmental Disasters

The DR Project Team will need to examine each potential environmental disaster or emergency situation. The focus should be on the level of business disruption potentially likely to result from each situation. Potential emergencies include business disruption caused by one or more of the following environmental disasters.

*** Tornado**

Tornadoes are tight columns of circling air creating a funnel shape. The wind forces within the tornado can reach over 200 miles per hour. Tornadoes can often travel in excess of 50 miles per hour. They can cause significant structural damage and can also cause severe injuries and death.

*** Hurricane**

Hurricanes are storms with heavy circular winds exceeding 60 miles per hour. The eye or centre of the hurricane is usually calm. The hurricane contains both extremely strong winds and torrential rain. Hurricanes can cause flooding, massive structural damage to homes and business premises with associated power failures, and even injury and death.

*** Flood**

Floods result from thunderstorms, tropical storms, snow thaws or heavy and prolonged rainfall causing rivers to overflow their banks and flood the surrounding areas. Floods can seriously affect buildings and equipment causing power failures and loss of facilities and can even result in injury or death.

*** Snowstorm**

Snowstorm conditions can include blizzards, strong winds, freezing temperatures with significant amounts of snow. Snow and ice can impact power and communications and employees may be unable to travel to work due to the impact on public transport or road conditions. It is possible for buildings to collapse under the weight of snow and injuries or even death could occur through freezing temperatures and icy conditions.

*** Drought**

Droughts are caused through lack of rainfall and can have a devastating affect on human life, animal life and plant life. These conditions are often seasonal and some regions of the world are more prone to these extreme conditions. Severe droughts can cause considerable loss and suffering to human life. There can also be significant affects on businesses that depend on the availability of water for their products or processes.

*** Earthquake**

Earthquakes are caused by a shifting of the earth's rock plates beneath its surface resulting in violent shaking and movement of the earth's upper surface. Severe earthquakes can destroy power and communication lines and disrupt gas, water and sewerage services. Significant damage to structures can occur including total collapse of buildings, bridges or other elevated structures. Earthquakes can also bring landslides, damage to dams, and aftershocks and resulting damage can hinder rescue efforts. In addition to being trapped in a collapsing building, of particular danger to human life is the possibility of falling glass or other objects.

*** Electrical storms**

The impact of lightning strikes can be significant. It can cause disruption to power and can also cause fires. It may also damage electrical equipment including computer systems. Structural damage is also possible through falling trees or other objects.

*** Fire**

Fires are often devastating and can be started through a wide range of events which may be accidental or environmental. Deliberate fires caused through arson are dealt with in topic BC 020102. The impact on the business will vary depending on the severity of the fire and the speed within which it can be brought under control. A fire can cause human injury or death and damage can also be caused to records and equipment and the fabric or structure of premises.

*** Subsidence and Landslides**

Subsidence and landslides are often caused through a change in the composition of the earth's surface. This change can often result from flooding, where flowing water can create cavernous open areas beneath structures. Subsidence or landslides can cause structural damage and can also disrupt transport services and affect travelling conditions.

*** Freezing Conditions**

Freezing conditions can occur in winter periods and the effects can be devastating. Where temperatures fall in excess of - 30(Centigrade they can create conditions which significantly disrupt businesses and even cause death or injury. Businesses and homes can be seriously affected through burst pipes, inadequate heating facilities, disruption to transportation and malfunctioning equipment. Work undertaken outside of buildings in the open environment will obviously be seriously affected.

*** Contamination and Environmental Hazards**

Contamination and environmental hazards include polluted air, polluted water, chemicals, radiation, asbestos, smoke, dampness and mildew, toxic waste and oil pollution. Many of these conditions can disrupt business processes directly and, in addition, cause sickness among

employees. This can result in prosecution or litigation if more permanent damage to employees' health occurs.

*** Epidemic**

An epidemic can occur when a contagious illness affects a large number of persons within a country or region. This can have a particularly devastating short term impact on business through a large number of persons being absent from work at the same time. Certain illnesses can have a longer term effect on the business where long term illness or death results. An example of this extreme situation is occurring in certain third world countries where the Aids virus is considered to be of epidemic proportions.

Each of the above scenarios to be used within the planning process needs to be developed and examined in detail and an analysis prepared of the consequences of each potential threat. Each scenario should also be assessed for possibility of occurrence (probability rating) and possible impact (impact rating).

Organised and / or Deliberate Disruption

The DR Project Team will need to examine each potential disaster or emergency situation caused through activities which can be described as "organised disruption". The focus should be on the level of business disruption likely from each situation. Potential emergencies include business disruption caused by one or more of the following organised disruptive events.

*** Act of terrorism**

Acts of terrorism include explosions, bomb threats, hostage taking, sabotage and organised violence. Whether this is perpetrated through a recognised terrorist organisation or a violent protest group, the effect on individuals and business is the same. Such acts create uncertainty and fear and serve to de-stabilise the general environment.

*** Act of Sabotage**

An act of sabotage is the deliberate serious disruption of an organisation's activities with an attempt to discredit or financially damage the organisation. Business will often be immediately and seriously affected by successful acts of sabotage. This can affect the normal operations and also serve to de-stabilise the workforce. An internal attack on the IT systems through the use of malicious code can be considered to be an act of sabotage.

*** Act of war**

An act of war is the commencement of hostilities between one country and another. This could take the form of air strikes, ground strikes, invasion or blockades. Business could be immediately

affected where they are either located near the outbreak of hostilities or where they are dependent upon imports or exports for survival. Many businesses do not survive a prolonged outbreak of war.

*** Theft**

This hazard could range from the theft of goods or equipment to the theft of money or other valuables. In addition to possibly financially damaging the organisation, theft can cause suspicion and uncertainty with the workforce where it may be believed that one or more of them could have been involved.

*** Arson**

Arson is the deliberate setting of a fire to damage the organisation's premises and contents. As this can cause both loss of premises and loss of goods and other assets, this can be highly disruptive to the organisation.

*** Labour Disputes / Industrial Action**

This disruptive threat is the withdrawal of labour or working to rule usually organised by a union to which employee groups may belong. It can follow a dispute between the workers and the management of a company which has not been resolved. A withdrawal of labour is often accompanied by picketing across the entrance of the company's premises to try to discourage anyone from entering. This sort of action is highly disruptive to the business and normally results in a shutdown of the business until the dispute is resolved.

Each of the above scenarios needs to be developed and examined in detail and an analysis prepared of the consequences of each potential scenario. Each scenario should also be assessed for possibility of occurrence (probability rating) and possible impact (impact rating).

Loss of Utilities and Services

The DR Project Team will need to examine each potential disaster or emergency situation. The focus here should be on the level of business disruption likely from each loss of utilities or public services. Potential emergencies include business disruption caused by the loss of one or more of the following utilities or services.

*** Electrical power failure**

All organisations depend on electrical power to continue normal operations. Without power the organisation's computers, lights, telephones and other communication medium will not be operational and the impact on normal business operations can be devastating. All organisations should be prepared for a possible electrical power failure as the impact can be so severe. Data can be lost, customers can be lost and there can be a serious impact on revenue. Pre-planning is

essential as a regional outage can cause a shortage of back up electrical generators. Consideration should be given to installing UPS systems to avoid brownouts.

*** Loss of gas supply**

The loss of gas supply can be extremely serious where the business relies on gas to fuel either its production processes or provide heating within its premises. The impact that a loss of gas supply can have on the production process can result in the whole process shutting down. The impact on the organisation will also be particularly acute where the loss of gas-fired heating could render the premises unusable during periods of low external temperatures.

*** Loss of water supply**

The loss of the water supply is likely to close down a business premises until the supply is restored. Where the water is used in the production process this is particularly serious. The loss of water supply is also a health and safety issue as minimum sanitary needs cannot be met. This is often caused through a fault in a water supply route or as a result of a particularly severe drought.

*** Petroleum and oil shortage**

For most countries in the world, a petroleum shortage can occur at any time. This has a serious impact on businesses as rationing is likely to be imposed immediately affecting transportation and the normal operations of diesel or petrol fuelled machinery. For example, this type of shortage can be caused by a sudden reduction in production output imposed by one of the OPEC members. It could also be caused through the short-term failure of a refinery, thereby affecting output of particular grades of fuel.

*** Communications services breakdown**

Most businesses are fully dependent upon their telecommunications services to operate their normal business processes and to enable their networks to function. A disruption to the telecommunications services can result in a business losing revenue and customers. The use of cell-based telephones can help to alleviate this but the main reliance is likely to be on the land based lines.

*** Loss of drainage / waste removal**

The loss of drainage or waste removal is likely to cause a serious sanitation and health issue for most businesses. This is likely to impact on the business through the possible loss of its workforce during the period where drainage services are not available. This, in turn, will have an immediate impact on revenue. A large number of businesses also rely on waste removal for its production processes and this will be impacted also.

Each of the above scenarios needs to be developed and examined in detail and an analysis prepared of the consequences of each potential scenario. Each scenario should also be assessed for possibility of occurrence (probability rating) and possible impact (impact rating).

Equipment or System Failure

The DR Project Team will need to examine each potential disaster or emergency situation. The focus should be on the level of business disruption potentially likely from each equipment or system failure. Potential emergencies include business disruption caused by one or more of the following equipment or system incidents:

*** Internal power failure**

An internal power failure is an interruption to the electrical power services caused through an internal equipment or cabling failure. This type of fault will need to be repaired by a qualified electrician and delays will inevitably impact on the business process. Where particularly serious faults have occurred, such as damage to main cables, the repairs could take some time and could have a severe effect on the business.

*** Air conditioning failure**

An air conditioning (AC) failure could have serious consequences where the AC unit is protecting particularly sensitive equipment such as a main computer processing unit, and the rise in temperature could cause the equipment to fail and be damaged. It can also affect the workforce as conditions in buildings can become extremely uncomfortable with a significant rise in temperatures and where the staff are adversely affected. Portable AC equipment may possibly be used as back up.

*** Production line failure**

Mechanical or electronic failure on an organisation's production line can have serious financial consequences. This is a particularly critical problem where the equipment needs to be replaced and is not easily repairable. The workforce may need to be laid off until the problem is rectified and sales and customers lost. Particularly vulnerable are the fully automated processes being used with the automotive and other industries.

*** Cooling plant failure**

Businesses that rely on cooling equipment for their production processes are particularly severely affected when the cooling plant fails. Dairy product processing and ice cream manufacturing are just two examples of a huge frozen and refrigerated food industry which is fully dependent upon cooling plants. Good back up arrangements are normally essential to avoid serious loss or damage to foodstuffs and deliveries.

*** Equipment failure (excluding IT hardware)**

All businesses rely on a whole range of different types of equipment in order to run their business processes. In many cases, it is possible to move to alternative processes to enable the business

processes to continue but this requires considerable planning and preparation. See BC 020105 below for computer systems failure.

Each of the above scenarios needs to be developed and examined in detail and an analysis prepared of the consequences of each potential scenario. Each scenario should also be assessed for possibility of occurrence (probability rating) and possible impact (impact rating).

Serious Information Security Incidents

The DR Project Team will need to examine each potential disaster or emergency situation. The focus in this section should be on the level of business disruption likely from each serious information security incident. Potential emergencies include business disruption caused by one or more of the following serious Information Security incidents:

*** Cyber crime**

Cyber crime is a major area of information security risk. It includes attacks by hackers, denial of service attacks, virus attacks, hoax virus warnings and premeditated internal attacks. All cyber crime attacks can have an immediate and devastating affect on the organisation's normal business processes. The average cost of an information security incident has been estimated at US\$30,000 and over 60% of organisations are reported to experience one or more incidents every year.

*** Loss of records or data**

The loss of records or data can be particularly disruptive where poor back up and recovery procedures result in the need to re-input and re-compile the records. This is normally a slow process and is particularly labour intensive. This can result in an increase in costs through additional working hours and a great deal of embarrassment where information is unexpectedly not available.

*** Disclosure of sensitive information**

This is a serious information security incident which can result in severe embarrassment, financial loss, and even litigation where damage has been caused to someone's reputation or financial standing. Further types of serious disclosure involve secret patent information, plans and strategic directions, secret recipes or ingredients, information disclosed to legal representatives etc. Deliberate unauthorised disclosure of sensitive information is also referred to as espionage.

*** IT system failure**

With the almost total level of dependence on IT systems within the vast majority of businesses, a failure to these systems can be particularly devastating. The types of threats to computer systems are many and varied, including hardware failure, damage to cables, water leaks and fires, air

conditioning system failures, network failures, application system failures, telecommunications equipment failures etc.

Each of the above scenarios needs to be developed and examined in detail and an analysis prepared of the consequences of each potential scenario. Each scenario should also be assessed for possibility of occurrence (probability rating) and possible impact (impact rating).

Other Emergency Situations

The DR Project Team will need to examine each potential disaster or emergency situation. The focus should be on the level of business disruption likely from other emergency situations not already covered above. Potential emergencies include business disruption caused by one or more of the following incidents:

*** Workplace violence**

Acts of violence in the workplace can affect morale, absenteeism, create fear and uncertainty and increase the rate of turnover of employees. This can have a significant affect on productivity and could also result in claims for workers compensation, harassment claims and a need for increased security measures. Statistically, this type of incident is especially prevalent at organisations which have recently merged or are being re-sized or restructured, where there are regular threats of industrial action, or where permanent employees have been replaced with temporary employees.

*** Public transportation disruption**

Disruption to public transport has a major effect on businesses through the inability of employees to get to their normal place of work. This disruption can be caused through major accidents, industrial action, equipment failure, bad weather conditions and major preventative repairs. Difficult travelling conditions increase absenteeism as well as lower morale and productivity.

*** Neighbourhood hazard**

A neighbourhood hazard is defined as a disruptive event in the close vicinity which directly or indirectly affects your own premises and employees. An example would be a seepage of hazardous waste from a neighbouring factory or the escape of toxic gases from a local chemical plant. Health and safety regulations require that the organisation take suitable action to protect its employees. This may have severe disruptive implications for the business particularly where it can take some time to clear the hazard.

*** Health and Safety Regulations**

For organisations that do not properly and fully observe all the necessary Health and Safety Regulations, a complaint or an inspection can result in the operation being completely closed down until the situation is corrected. This could result in substantial delays on major projects with

significant financial implications. Organisations should ensure that they meet the necessary regulations and requirements at all times.

*** Employee morale**

A large number of internal or external factors can have a direct impact on the level of employee morale. This can often arise where there is a combination of poor management, uncertainty and difficult working conditions. Productivity will be affected and employee turnover is likely to rise.

*** Mergers and acquisitions**

Mergers and acquisitions can be extremely de-stabilising on the employees of both businesses involved. Employees may be uncertain about how they will be affected or even whether they are about to lose their jobs. Unless well managed, the effect on the staff could be considerable with a dramatic lowering of morale and productivity.

*** Negative publicity**

Unfavourable press comments can result in a lowering of employee morale or a loss of customers. Any company can suffer from negative publicity and an internal crisis is best resolved from within, prior to the media feeding of the uncertainties and disputes. Reports may also be inaccurate, particularly where reliable information is not available, and therefore, well-worded press statements may be issued to quieten down adverse reports. Information can be leaked to the press from disgruntled employees and industry competitors.

*** Legal problems**

Legal problems are both time consuming and expensive. Organisations can experience a wide range of legal issues including sexual harassment, contract disputes, copyright disputes, health and safety regulations and discrimination. It is important that organisations are fully aware of their legal duties and the rights of their employees.

Each of the above scenarios needs to be developed and examined in detail and an analysis prepared of the consequences of each potential scenario. Each scenario should also be assessed for possibility of occurrence (probability rating) and possible impact (impact rating).

Reference: Business Continuity Planning / Disaster Recovery Planning -- An Online Guide. Sections BC 020101 thru BC 020106

<http://www.yourwindow.to/business-continuity/>

Appendix B

SECTION 1-11-435. Protection of critical information technology infrastructure and data systems.

To protect the state's critical information technology infrastructure and associated data systems in the event of a major disaster, whether natural or otherwise, and to allow the services to the citizens of this State to continue in such an event, the Office of the State Chief Information Officer (CIO) should develop a Critical Information Technology Infrastructure Protection Plan devising policies and procedures to provide for the confidentiality, integrity, and availability of, and to allow for alternative and immediate on-line access to critical data and information systems including, but not limited to, health and human services, law enforcement, and related agency data necessary to provide critical information to citizens and ensure the protection of state employees as they carry out their disaster-related duties. All state agencies and political subdivisions of this State are directed to assist the Office of the State CIO in the collection of data required for this plan.

Full and associated text can be located at the South Carolina Legislature Online website:
<http://www.scstatehouse.net/code/t01c011.htm>

Disaster Recovery in a Data Processing Environment

Protecting Your Agencies' Assets

Prepared by: Stephen G. Tucker

Division of the State Chief Information Officer

South Carolina Budget and Control Board

Submitted: February, 2007

Introduction

The more our agencies' business relies on its information technology (IT) systems, the more we need to consider how unexpected disruptions would affect the mission of the agency. These disruptions could come in many forms, from fire and floods, theft, malicious attacks on our systems, such as hacking to areas we might never consider (see Appendix A).

Disaster recovery planning (DR/DRP) improves our agencies' ability to react to such disruptions. It describes how we will restart our operations in order to meet our agency-critical requirements. This paper will explain the importance of disaster recovery plans to the success of our agencies, and the stages we need to go through when developing them.

What is disaster recovery planning?

Disaster recovery planning is the process of planning for the unexpected. An effective plan will provide us with procedures to minimize the effects of unexpected disruptions. The plan should enable our agencies to recover quickly and efficiently, with the minimum disruption to our day-to-day activities.

Disaster recovery is a process developed to counteract systems failure. It is a management issue, not something that should just be considered by the IT department. If the IT systems fail or are unavailable, it is likely to have a significant impact upon the whole agency. Therefore we should take an active interest in establishing disaster recovery plans for our IT systems.

Disaster recovery supports the ability of the agency to recover. This includes:

- Providing facilities and services to enable the agency to continue to function;
- and

- Providing the critical IT applications and infrastructure necessary to support the recovery of agency processes

Once a disaster recovery plan has been written and implemented, it is the start of an ongoing commitment. Agencies constantly evolve, and recovery strategies must evolve with them. For example, as people join, transfer, retire or otherwise leave an agency, plans must be updated to reflect changes in recovery teams. Also, new IT systems could be introduced. These may be essential to the agency. If so, we must build their recovery into our plans. New legislation or reorganization could greatly change the missions of the agency.

Plans should be clear and concise; to ensure that people will read it. Make it available to all staff members responsible for any part of the plan. Summarize it for the rest of the staff so that they will know what to expect.

The benefits of disaster recovery planning

A disaster recovery plan minimizes the disruption to our agencies from any unexpected events or disasters. Staff will know their responsibilities in such situations, and will be able to respond to the events by following an agreed procedure. This will ensure that our agency-critical systems are up and running in the shortest possible time.

There are additional benefits of having a disaster recovery plan in place. First, there are regulatory requirements to have a recovery plan in place (see Appendix B). There are also additional Federal requirements pertaining to recovery of sensitive and time-critical data. In addition, an agency that can demonstrate an effective disaster recovery plan has a competitive advantage. For example, if we provide a service to a customer that is dependent upon the IT systems, like an Internet service provider, then evidence of a sound plan may provide us with an

advantage that can be used to win or retain customers. For instance, if our agency is a partner in a service delivery chain, disaster recovery planning may well need to be an integral part of our quality assurance.

Effective disaster recovery management will help agencies demonstrate that we are managing our business risks and so help to secure lower insurance premiums. In addition, drawing up a disaster recovery plan can help us assess what types of insurance we need the most, as identifying likely business risks is part of the planning exercise. This is because disaster recovery planning may help to identify potential business risks we were previously unaware of, but which we recognize that we now need to insure against. Therefore, we may decide to opt for lower insurance coverage across a broader range of risks - the original risks plus the recently identified ones - in order to remain within our budgeted insurance cost.

Risk assessment and impact analysis

The first step in disaster recovery planning is to do a risk assessment. This will help us to decide which threats on which to concentrate. It involves:

- Identifying the range of threats that the agency faces;
- Assessing their potential impact on the agency; and
- Assessing the likelihood of each threat occurring

Assessing the potential impacts of unexpected events is called impact analysis. We must consider how much our agency stands to lose because of each possible type of disaster or service disruption.

To assess potential impact we should identify the critical agency processes and the potential damage or loss that the agency would suffer if any of these services were disrupted. The damage can be measured in hard terms such as financial loss, or in soft terms such as political

embarrassment or loss of credibility to the agency. We must also consider how any damage or loss will increase if the disruption lasts a long time. For example, what would be the impact to our agency if our e-commerce site was down for a day rather than an hour? How about our Sexual Offender Registry or a social benefits site? For some agencies, this may mean the difference between a temporary loss of information and people being fired. Having determined the impact of each threat, we should decide how likely, each threat is to occur. This will help us decide which threats to prioritize in disaster recovery planning.

Components of a disaster recovery plan

We will use information on threats to our agencies to start our disaster recovery plan. These were gathered in risk assessment and impact analysis. The plan should aim to reduce the risks posed by disruption to our agencies' processes. Measures that may be needed include:

- A back-up and data recovery strategy, including off-site storage;
- The development of a resilient IT infrastructure with redundancies in case of failure. For example mirrored central server computers sited in different locations, each containing the same information, so that if one goes down the other one is available to ensure continuity of service and alternative storage facilities;
- The elimination of single points of failure, such as a single power supply; or
- The introduction of an uninterruptible power supply for our IT systems. This device allows the computer to keep running for a short time when the main power supply is lost. It uses a battery that takes over when power is lost and gives us time to save any data that we may be working on.

Even if such measures are adopted, things can still go terribly wrong. In the event of a disruption or disaster, the disaster recovery plan should specify when actions should begin and what actions are to be taken in order to recover from this event, covering such items as:

- People and accommodation;
- IT systems and networks;
- Services such as power and telecommunications; and
- Critical business processes

Methods of recovery might include:

- Carrying out activities manually until IT services are resumed;
- Staff at an affected building moving to another of the business' offices;
- Agreeing with another business to use each other's premises in the event of a disaster; or
- Arranging to use IT services and accommodation provided by a specialist third-party standby site

The disaster recovery plan should be kept short and readable. It should not duplicate other sources of information, and any other relevant documents should be referenced. Encourage staff to review the plan before it is formally issued.

Testing the IT disaster recovery plan

Testing a disaster recovery plan can be difficult. Simulating potential threats to our agencies can be time consuming, expensive and possibly disastrous to our data. However, testing our disaster recovery plans will help show whether we have covered all angles, and whether our plan is achievable. In addition, it can increase our served citizens and other agencies' confidence in our business' ability to recover from disruption. Tests are also useful to raise staff awareness of the

plans. We can test whether staff can function without access to data cheaply and easily. Such tests can also help to check that other sources of data, such as back-ups or archives that are held off-site, are sufficiently up-to-date.

At some point, usually around 12 months after the plan has been developed, we should carry out a real restore of data - use data that has been backed up to get our system fully operational again - and attempt to work without premises or files. This will help to establish:

- Whether the expected timescales for recovering key business applications are realistic;
- How prepared the staff is for putting the plan into action; and
- Whether any third parties or service providers who are integral to the plan are ready to respond

We also should ensure that any test we undertake, whether technical - relating to the operation of the IT systems - or non-technical - relating to all associated activities - has clear objectives. For example, to measure the time needed to get our main IT systems running following a disruption or to test how long it takes to contact all key personnel in the event of a disaster. This will enable us to measure the success, or otherwise, of each exercise, and highlight areas in need of further attention. Any initial testing should be followed by further tests on a regular basis. In particular, details of any changes to IT systems should be included in the plan and tests should be undertaken on the new systems.

Education and training in IT disaster recovery

All staff members must be aware of the importance of disaster recovery planning. Training and awareness are important to make sure that the staff fully understands the plan and the role they will play in it. Awareness can range from simple knowledge of the assembly points should the

building have to be evacuated; through to the exact role each member of staff will have in the event of a disaster or unexpected event. Awareness training should be undertaken on a regular basis, and included in any staff induction programs. Staff who will have specific responsibilities in the recovery of IT systems should be given further technical training. This will ensure that they are able to recover systems and applications quickly and efficiently.

Any third parties who have a critical role in the disaster recovery plans should be part of this awareness training. If, for example, we have set up office-sharing arrangements with another agency, then they need to know the procedures that will be followed if our office becomes unavailable. We will also wish to include training for any member of staff who may need to talk to the media in the event of a disruption or incident. This is particularly important as the reputation and public perception of our agency is key to its ongoing success.

Key steps in developing a disaster recovery plan

There are five key stages in developing and maintaining a disaster recovery plan.

Stage 1-Understanding our Business

- Project initiation and management - get support from senior managers. Establish a management structure to develop and carry out the plan.
- Risk evaluation and control - identify the threats and the best defense. For example, with e-commerce, computer viruses might be a major threat - the appropriate defense might be regularly updated anti-virus software. See the page in this guide on risk assessment and impact analysis.

- Business impact analysis - establish the business' critical processes and identify the impact of any failures. For example, if our e-commerce website is critical to our operation, what would it cost our agency if it were down for 24 hours?

Stage 2-Disaster Recovery Management Strategies

- Develop an organizational disaster recovery strategy, identifying areas on which to concentrate. Focus on the critical operating requirements of the business, as identified above.
- Develop a process-level strategy - a documented framework clearly stating how critical processes will be restarted following an incident or failure. For example, if the payment system for our e-commerce website goes down, we will need a specific strategy for resuming operations.

Stage 3-Developing and Implementing a Disaster Recovery Response

- Emergency response and operations - establish a crisis management process to respond to incidents. Find out about crisis management at the Continuity Central website.
- Develop and implement a disaster recovery plan. This describes specifically how we will deal with incidents. Focus on the priorities of the overall disaster recovery strategy.
- Put in place business unit plans for each department. For example, detail the actions that the IT department will have to carry out if IT services are lost.

Stage 4-Developing a Disaster Recovery Management Culture

- Awareness and training plans - ensure all staff are aware of the importance of disaster recovery and can operate effectively following an incident.

- Review the effectiveness of awareness training periodically. Identify any further training needed.

Stage 5-Exercising, Maintenance and Audit

- Test the disaster recovery plans. Test any technical aspects - for example if we plan to use backed-up data to restore operations. Carry out full live exercises to establish how the plans work in a disaster situation.
- Maintain the plans - ensure that the documentation remains accurate and reflects any changes inside or outside the business.
- Regularly audit the plans - do they meet the needs of our strategy? Act on the findings.

Summary

I have an opportunity to meet with a number of the larger agencies on a regular basis. While exact data is hard to come by, most agree that they are in the infancy stages on the development of a true Disaster Recovery Plan. Most claim to have some form of backup and recovery. But, when asked if they have tested that plan, all reply "NO". If asked if their data was stored offsite, most replied "I think so" or "I don't know". I sincerely hope that thru my job at the Division of the State Chief Information Officer, I can promote the writing of Disaster Recovery Plans and the full implementation of these plans. The functions performed by most agencies, especially in the health and safety areas, are much too critical to the citizens of South Carolina to be left to the false hope that a disaster will never happen to them. Trained professional at the State CIO's division are available to assist any governmental agency with the development and implementation of a Disaster Recovery Plan.

Please understand that this paper was written to show the importance of having a Disaster Recovery Plan in place. It was not designed to be a template for that Plan. Actual creation and

implementation of a DR plan requires time, money, people and above all, senior management commitment. By reviewing some of the referenced documents, we can decide which options we wish to choose, how much we wish to spend and how much Disaster Recovery we need.

If you think it could not happen here, visit the SC Department of Archives and History. This site has a wealth of information for State agencies:
<http://www.state.sc.us/scdah/disaster.htm>

For further information, contact:

Steve Tucker
Manager, Level II Support Center
Division of the State Chief Information Officer
(803) 896-0139

REFERENCES

Business Continuity Planning / Disaster Recovery Planning -- An Online Guide
<http://www.yourwindow.to/business-continuity/>

Business Continuity Planning Model, By Disaster Recovery Institute, International
<http://www.drj.com/new2dr/model/bcmodel.htm>

National Fire Protection Association, NFPA1600 Standard on Disaster/Emergency Management and Business Continuity Programs, 2004 Edition
<http://www.nfpa.org/assets/files/PDF/NFPA1600.pdf>

South Carolina Enterprise Architecture, Business Continuity, Disaster Recovery Best Practices, V1.0 – January 24, 2007
<http://www.cio.sc.gov/cioContent.asp?pageID=539>
<http://www.cio.sc.gov/SCEA/sms/sms-DisasterRecoveryBestPracticesa.pdf>

Appendix A

Environmental Disasters

The DR Project Team will need to examine each potential environmental disaster or emergency situation. The focus should be on the level of business disruption potentially likely to result from each situation. Potential emergencies include business disruption caused by one or more of the following environmental disasters.

*** Tornado**

Tornadoes are tight columns of circling air creating a funnel shape. The wind forces within the tornado can reach over 200 miles per hour. Tornadoes can often travel in excess of 50 miles per hour. They can cause significant structural damage and can also cause severe injuries and death.

*** Hurricane**

Hurricanes are storms with heavy circular winds exceeding 60 miles per hour. The eye or centre of the hurricane is usually calm. The hurricane contains both extremely strong winds and torrential rain. Hurricanes can cause flooding, massive structural damage to homes and business premises with associated power failures, and even injury and death.

*** Flood**

Floods result from thunderstorms, tropical storms, snow thaws or heavy and prolonged rainfall causing rivers to overflow their banks and flood the surrounding areas. Floods can seriously affect buildings and equipment causing power failures and loss of facilities and can even result in injury or death.

*** Snowstorm**

Snowstorm conditions can include blizzards, strong winds, freezing temperatures with significant amounts of snow. Snow and ice can impact power and communications and employees may be unable to travel to work due to the impact on public transport or road conditions. It is possible for buildings to collapse under the weight of snow and injuries or even death could occur through freezing temperatures and icy conditions.

*** Drought**

Droughts are caused through lack of rainfall and can have a devastating affect on human life, animal life and plant life. These conditions are often seasonal and some regions of the world are more prone to these extreme conditions. Severe droughts can cause considerable loss and suffering to human life. There can also be significant affects on businesses that depend on the availability of water for their products or processes.

*** Earthquake**

Earthquakes are caused by a shifting of the earth's rock plates beneath its surface resulting in violent shaking and movement of the earth's upper surface. Severe earthquakes can destroy power and communication lines and disrupt gas, water and sewerage services. Significant damage to structures can occur including total collapse of buildings, bridges or other elevated structures. Earthquakes can also bring landslides, damage to dams, and aftershocks and resulting damage can hinder rescue efforts. In addition to being trapped in a collapsing building, of particular danger to human life is the possibility of falling glass or other objects.

*** Electrical storms**

The impact of lightning strikes can be significant. It can cause disruption to power and can also cause fires. It may also damage electrical equipment including computer systems. Structural damage is also possible through falling trees or other objects.

*** Fire**

Fires are often devastating and can be started through a wide range of events which may be accidental or environmental. Deliberate fires caused through arson are dealt with in topic BC 020102. The impact on the business will vary depending on the severity of the fire and the speed within which it can be brought under control. A fire can cause human injury or death and damage can also be caused to records and equipment and the fabric or structure of premises.

*** Subsidence and Landslides**

Subsidence and landslides are often caused through a change in the composition of the earth's surface. This change can often result from flooding, where flowing water can create cavernous open areas beneath structures. Subsidence or landslides can cause structural damage and can also disrupt transport services and affect travelling conditions.

*** Freezing Conditions**

Freezing conditions can occur in winter periods and the effects can be devastating. Where temperatures fall in excess of - 30(Centigrade they can create conditions which significantly disrupt businesses and even cause death or injury. Businesses and homes can be seriously affected through burst pipes, inadequate heating facilities, disruption to transportation and malfunctioning equipment. Work undertaken outside of buildings in the open environment will obviously be seriously affected.

*** Contamination and Environmental Hazards**

Contamination and environmental hazards include polluted air, polluted water, chemicals, radiation, asbestos, smoke, dampness and mildew, toxic waste and oil pollution. Many of these conditions can disrupt business processes directly and, in addition, cause sickness among

employees. This can result in prosecution or litigation if more permanent damage to employees' health occurs.

*** Epidemic**

An epidemic can occur when a contagious illness affects a large number of persons within a country or region. This can have a particularly devastating short term impact on business through a large number of persons being absent from work at the same time. Certain illnesses can have a longer term effect on the business where long term illness or death results. An example of this extreme situation is occurring in certain third world countries where the Aids virus is considered to be of epidemic proportions.

Each of the above scenarios to be used within the planning process needs to be developed and examined in detail and an analysis prepared of the consequences of each potential threat. Each scenario should also be assessed for possibility of occurrence (probability rating) and possible impact (impact rating).

Organised and / or Deliberate Disruption

The DR Project Team will need to examine each potential disaster or emergency situation caused through activities which can be described as "organised disruption". The focus should be on the level of business disruption likely from each situation. Potential emergencies include business disruption caused by one or more of the following organised disruptive events.

*** Act of terrorism**

Acts of terrorism include explosions, bomb threats, hostage taking, sabotage and organised violence. Whether this is perpetrated through a recognised terrorist organisation or a violent protest group, the effect on individuals and business is the same. Such acts create uncertainty and fear and serve to de-stabilise the general environment.

*** Act of Sabotage**

An act of sabotage is the deliberate serious disruption of an organisation's activities with an attempt to discredit or financially damage the organisation. Business will often be immediately and seriously affected by successful acts of sabotage. This can affect the normal operations and also serve to de-stabilise the workforce. An internal attack on the IT systems through the use of malicious code can be considered to be an act of sabotage.

*** Act of war**

An act of war is the commencement of hostilities between one country and another. This could take the form of air strikes, ground strikes, invasion or blockades. Business could be immediately

affected where they are either located near the outbreak of hostilities or where they are dependent upon imports or exports for survival. Many businesses do not survive a prolonged outbreak of war.

*** Theft**

This hazard could range from the theft of goods or equipment to the theft of money or other valuables. In addition to possibly financially damaging the organisation, theft can cause suspicion and uncertainty with the workforce where it may be believed that one or more of them could have been involved.

*** Arson**

Arson is the deliberate setting of a fire to damage the organisation's premises and contents. As this can cause both loss of premises and loss of goods and other assets, this can be highly disruptive to the organisation.

*** Labour Disputes / Industrial Action**

This disruptive threat is the withdrawal of labour or working to rule usually organised by a union to which employee groups may belong. It can follow a dispute between the workers and the management of a company which has not been resolved. A withdrawal of labour is often accompanied by picketing across the entrance of the company's premises to try to discourage anyone from entering. This sort of action is highly disruptive to the business and normally results in a shutdown of the business until the dispute is resolved.

Each of the above scenarios needs to be developed and examined in detail and an analysis prepared of the consequences of each potential scenario. Each scenario should also be assessed for possibility of occurrence (probability rating) and possible impact (impact rating).

Loss of Utilities and Services

The DR Project Team will need to examine each potential disaster or emergency situation. The focus here should be on the level of business disruption likely from each loss of utilities or public services. Potential emergencies include business disruption caused by the loss of one or more of the following utilities or services.

*** Electrical power failure**

All organisations depend on electrical power to continue normal operations. Without power the organisation's computers, lights, telephones and other communication medium will not be operational and the impact on normal business operations can be devastating. All organisations should be prepared for a possible electrical power failure as the impact can be so severe. Data can be lost, customers can be lost and there can be a serious impact on revenue. Pre-planning is

essential as a regional outage can cause a shortage of back up electrical generators. Consideration should be given to installing UPS systems to avoid brownouts.

*** Loss of gas supply**

The loss of gas supply can be extremely serious where the business relies on gas to fuel either its production processes or provide heating within its premises. The impact that a loss of gas supply can have on the production process can result in the whole process shutting down. The impact on the organisation will also be particularly acute where the loss of gas-fired heating could render the premises unusable during periods of low external temperatures.

*** Loss of water supply**

The loss of the water supply is likely to close down a business premises until the supply is restored. Where the water is used in the production process this is particularly serious. The loss of water supply is also a health and safety issue as minimum sanitary needs cannot be met. This is often caused through a fault in a water supply route or as a result of a particularly severe drought.

*** Petroleum and oil shortage**

For most countries in the world, a petroleum shortage can occur at any time. This has a serious impact on businesses as rationing is likely to be imposed immediately affecting transportation and the normal operations of diesel or petrol fuelled machinery. For example, this type of shortage can be caused by a sudden reduction in production output imposed by one of the OPEC members. It could also be caused through the short-term failure of a refinery, thereby affecting output of particular grades of fuel.

*** Communications services breakdown**

Most businesses are fully dependent upon their telecommunications services to operate their normal business processes and to enable their networks to function. A disruption to the telecommunications services can result in a business losing revenue and customers. The use of cell-based telephones can help to alleviate this but the main reliance is likely to be on the land based lines.

*** Loss of drainage / waste removal**

The loss of drainage or waste removal is likely to cause a serious sanitation and health issue for most businesses. This is likely to impact on the business through the possible loss of its workforce during the period where drainage services are not available. This, in turn, will have an immediate impact on revenue. A large number of businesses also rely on waste removal for its production processes and this will be impacted also.

Each of the above scenarios needs to be developed and examined in detail and an analysis prepared of the consequences of each potential scenario. Each scenario should also be assessed for possibility of occurrence (probability rating) and possible impact (impact rating).

Equipment or System Failure

The DR Project Team will need to examine each potential disaster or emergency situation. The focus should be on the level of business disruption potentially likely from each equipment or system failure. Potential emergencies include business disruption caused by one or more of the following equipment or system incidents:

*** Internal power failure**

An internal power failure is an interruption to the electrical power services caused through an internal equipment or cabling failure. This type of fault will need to be repaired by a qualified electrician and delays will inevitably impact on the business process. Where particularly serious faults have occurred, such as damage to main cables, the repairs could take some time and could have a severe effect on the business.

*** Air conditioning failure**

An air conditioning (AC) failure could have serious consequences where the AC unit is protecting particularly sensitive equipment such as a main computer processing unit, and the rise in temperature could cause the equipment to fail and be damaged. It can also affect the workforce as conditions in buildings can become extremely uncomfortable with a significant rise in temperatures and where the staff are adversely affected. Portable AC equipment may possibly be used as back up.

*** Production line failure**

Mechanical or electronic failure on an organisation's production line can have serious financial consequences. This is a particularly critical problem where the equipment needs to be replaced and is not easily repairable. The workforce may need to be laid off until the problem is rectified and sales and customers lost. Particularly vulnerable are the fully automated processes being used with the automotive and other industries.

*** Cooling plant failure**

Businesses that rely on cooling equipment for their production processes are particularly severely affected when the cooling plant fails. Dairy product processing and ice cream manufacturing are just two examples of a huge frozen and refrigerated food industry which is fully dependent upon cooling plants. Good back up arrangements are normally essential to avoid serious loss or damage to foodstuffs and deliveries.

*** Equipment failure (excluding IT hardware)**

All businesses rely on a whole range of different types of equipment in order to run their business processes. In many cases, it is possible to move to alternative processes to enable the business

processes to continue but this requires considerable planning and preparation. See BC 020105 below for computer systems failure.

Each of the above scenarios needs to be developed and examined in detail and an analysis prepared of the consequences of each potential scenario. Each scenario should also be assessed for possibility of occurrence (probability rating) and possible impact (impact rating).

Serious Information Security Incidents

The DR Project Team will need to examine each potential disaster or emergency situation. The focus in this section should be on the level of business disruption likely from each serious information security incident. Potential emergencies include business disruption caused by one or more of the following serious Information Security incidents:

*** Cyber crime**

Cyber crime is a major area of information security risk. It includes attacks by hackers, denial of service attacks, virus attacks, hoax virus warnings and premeditated internal attacks. All cyber crime attacks can have an immediate and devastating affect on the organisation's normal business processes. The average cost of an information security incident has been estimated at US\$30,000 and over 60% of organisations are reported to experience one or more incidents every year.

*** Loss of records or data**

The loss of records or data can be particularly disruptive where poor back up and recovery procedures result in the need to re-input and re-compile the records. This is normally a slow process and is particularly labour intensive. This can result in an increase in costs through additional working hours and a great deal of embarrassment where information is unexpectedly not available.

*** Disclosure of sensitive information**

This is a serious information security incident which can result in severe embarrassment, financial loss, and even litigation where damage has been caused to someone's reputation or financial standing. Further types of serious disclosure involve secret patent information, plans and strategic directions, secret recipes or ingredients, information disclosed to legal representatives etc. Deliberate unauthorised disclosure of sensitive information is also referred to as espionage.

*** IT system failure**

With the almost total level of dependence on IT systems within the vast majority of businesses, a failure to these systems can be particularly devastating. The types of threats to computer systems are many and varied, including hardware failure, damage to cables, water leaks and fires, air

conditioning system failures, network failures, application system failures, telecommunications equipment failures etc.

Each of the above scenarios needs to be developed and examined in detail and an analysis prepared of the consequences of each potential scenario. Each scenario should also be assessed for possibility of occurrence (probability rating) and possible impact (impact rating).

Other Emergency Situations

The DR Project Team will need to examine each potential disaster or emergency situation. The focus should be on the level of business disruption likely from other emergency situations not already covered above. Potential emergencies include business disruption caused by one or more of the following incidents:

*** Workplace violence**

Acts of violence in the workplace can affect morale, absenteeism, create fear and uncertainty and increase the rate of turnover of employees. This can have a significant affect on productivity and could also result in claims for workers compensation, harassment claims and a need for increased security measures. Statistically, this type of incident is especially prevalent at organisations which have recently merged or are being re-sized or restructured, where there are regular threats of industrial action, or where permanent employees have been replaced with temporary employees.

*** Public transportation disruption**

Disruption to public transport has a major effect on businesses through the inability of employees to get to their normal place of work. This disruption can be caused through major accidents, industrial action, equipment failure, bad weather conditions and major preventative repairs. Difficult travelling conditions increase absenteeism as well as lower morale and productivity.

*** Neighbourhood hazard**

A neighbourhood hazard is defined as a disruptive event in the close vicinity which directly or indirectly affects your own premises and employees. An example would be a seepage of hazardous waste from a neighbouring factory or the escape of toxic gases from a local chemical plant. Health and safety regulations require that the organisation take suitable action to protect its employees. This may have severe disruptive implications for the business particularly where it can take some time to clear the hazard.

*** Health and Safety Regulations**

For organisations that do not properly and fully observe all the necessary Health and Safety Regulations, a complaint or an inspection can result in the operation being completely closed down until the situation is corrected. This could result in substantial delays on major projects with

significant financial implications. Organisations should ensure that they meet the necessary regulations and requirements at all times.

*** Employee morale**

A large number of internal or external factors can have a direct impact on the level of employee morale. This can often arise where there is a combination of poor management, uncertainty and difficult working conditions. Productivity will be affected and employee turnover is likely to rise.

*** Mergers and acquisitions**

Mergers and acquisitions can be extremely de-stabilising on the employees of both businesses involved. Employees may be uncertain about how they will be affected or even whether they are about to lose their jobs. Unless well managed, the effect on the staff could be considerable with a dramatic lowering of morale and productivity.

*** Negative publicity**

Unfavourable press comments can result in a lowering of employee morale or a loss of customers. Any company can suffer from negative publicity and an internal crisis is best resolved from within, prior to the media feeding of the uncertainties and disputes. Reports may also be inaccurate, particularly where reliable information is not available, and therefore, well-worded press statements may be issued to quieten down adverse reports. Information can be leaked to the press from disgruntled employees and industry competitors.

*** Legal problems**

Legal problems are both time consuming and expensive. Organisations can experience a wide range of legal issues including sexual harassment, contract disputes, copyright disputes, health and safety regulations and discrimination. It is important that organisations are fully aware of their legal duties and the rights of their employees.

Each of the above scenarios needs to be developed and examined in detail and an analysis prepared of the consequences of each potential scenario. Each scenario should also be assessed for possibility of occurrence (probability rating) and possible impact (impact rating).

Reference: Business Continuity Planning / Disaster Recovery Planning -- An Online Guide. Sections BC 020101 thru BC 020106

<http://www.yourwindow.to/business-continuity/>

Appendix B

SECTION 1-11-435. Protection of critical information technology infrastructure and data systems.

To protect the state's critical information technology infrastructure and associated data systems in the event of a major disaster, whether natural or otherwise, and to allow the services to the citizens of this State to continue in such an event, the Office of the State Chief Information Officer (CIO) should develop a Critical Information Technology Infrastructure Protection Plan devising policies and procedures to provide for the confidentiality, integrity, and availability of, and to allow for alternative and immediate on-line access to critical data and information systems including, but not limited to, health and human services, law enforcement, and related agency data necessary to provide critical information to citizens and ensure the protection of state employees as they carry out their disaster-related duties. All state agencies and political subdivisions of this State are directed to assist the Office of the State CIO in the collection of data required for this plan.

Full and associated text can be located at the South Carolina Legislature Online website:
<http://www.scstatehouse.net/code/t01c011.htm>