Staying Prepared for IT Disasters

ABSTRACT

IT disasters can result in severe losses if an organisation is unprepared. While many organisations have IT Disaster Recovery (DR) plans, most focus only on the recovery of IT systems after a disaster. However, recovering IT systems should only form part of the DR plan as there are other important executive actions to be carried out. Understanding and documenting the IT DR processes, and conducting regular exercises diligently as part of the IT DR plan, can help organisations to prepare for an IT disaster and resume operations quickly to minimise the impact on business.

Feng Ziheng
Yee Keen Seng
Lim Hwee Kwang

INTRODUCTION

The September 11 attack on the World Trade Centre in USA destroyed more than 12,000 data servers and caused massive critical data loss (Shore, 2002). While the world focused on the political impact and human toll of the attack, the importance of a sound IT Disaster Recovery (DR) plan was also highlighted in its aftermath. As a result, many organisations have incorporated IT DR planning as part of their business continuity plan.

An IT DR plan seeks to recover the IT systems so that they can continue to support business functions after a disaster. Apart from recovering IT systems, there are other executive actions required to manage the disaster – even in instances where only IT systems have been affected. These aspects are sometimes overlooked by organisations and excluded from their IT DR plans.

This article illustrates the key considerations of a comprehensive IT DR plan, through the scenario of a fire incident in a data centre. This scenario is cited because fire risks are higher in Singapore as compared to natural disasters like earthquakes. The article also describes measures that organisations should undertake to better prepare for IT disasters.

MINIMISING THE RISKS OF DISASTERS

While disasters often strike without warning, organisations can strive to minimise the impact on their operations through good planning. In the event of a disaster, these organisations can better manage the chaotic situation to speed up recovery of their business operations and reduce potential losses.

Besides having IT recovery procedures, a comprehensive IT DR plan should also give due consideration to the following aspects:

a) Data centre design and management

b) Alternative sites

c) Data recovery plan and infrastructure

d) Crisis management team

e) Staff training

f) Insurance policies and claims

Data Centre Design and Management

A data centre should be designed and built based on the type of IT infrastructure that it needs to house. By understanding the nature of each type of infrastructure, proper room segregation can be designed to contain the damage area and minimise losses in the event of a disaster. In addition to proper room segregation, the IT DR plan should include the following key design considerations to mitigate the effects of any fire incidents:

> Keep Uninterruptible Power Supply Batteries Away from IT Equipment

Uninterruptible Power Supply (UPS) batteries are used to provide backup power to IT equipment in a data centre. It is a common oversight to house these batteries and the IT equipment in the same room, which may arise due to space constraints or a lack of knowledge of safety requirements. The co-location of UPS batteries and IT equipment increases the probability of damage to the IT equipment as a result of a fire breakout from the highly flammable UPS batteries.

Defective UPS batteries, loose electrical cable connections, or poor maintenance can result in the overheating of batteries or cables, causing a fire to break out. If the fire is not contained immediately, the IT equipment may be damaged by fire, soot or heat, leading to disruptions in business operations. Figures 1 and 2 show the aftermath of a fire in a server room.

Figure 1. Burnt UPS batteries

Figure 2. Burnt IT equipment

To mitigate the risk of fire occurrence, UPS batteries must be housed separately in isolated rooms with proper fire-rated walls and doors. These rooms should also be equipped with the correct type of fire suppression systems which are in accordance with the fire safety code. The fire suppression systems play an important role in containing the fire – they give sufficient time for the fire fighters to put out the fire before it spreads to the neighbouring rooms housing the IT equipment. One of the recommended fire suppression systems is the dry pipe sprinkler system, where the pipes are filled with water only when the high temperature alarm is sounded. This reduces the risk of accidental water discharge or pipe leakage. The location of the IT infrastructure and fire suppression systems should be documented in the IT DR Plan.

> Implement Effective Water Drainage System

When a fire is detected, the water sprinkler will be activated to put out the fire. However, the deluge may worsen the disaster in some ways. If the water reaches the electrical circuits or battery rooms causing a short circuit, more fires may be ignited as a result. The water from the overhead sprinklers may also flow into equipment racks and damage more IT equipment. If the data centre is housed within an office building, water flowing to the office areas may result in further damage to the office and IT equipment.

An effective drainage system must be implemented to prevent flooding of the data centre or building. Regular maintenance of the drainage system is required to reduce the chance of blockage in the system. In addition, there should be an overriding system to stop the flow of water from the sprinkler after the fire has been put out.

> Manage IT and Building Infrastructure

Data centres are typically built to last 20 years or more. According to Moore's Law (Downes, 2009), the computing power of IT equipment should increase by many times over this period, which in turn leads to an increase in power, cooling, and structural loading requirements. Furthermore, heavy IT equipment, such as storage area network and high-density servers, may be added to the data centre. It is crucial that the impact of these new requirements be assessed by professional engineers. The assessment

helps to ensure that the floor loading of the data centre as well as its power and cooling capacity are sufficient to house and operate the IT equipment. Exceeding these capacities may increase the risk of a disaster occurring. Thus, it is necessary to have a robust governance framework and process to manage the introduction of additional IT equipment.

Alternative Sites

While the impact of a disaster may be minimised through the appropriate design of a data centre, there remains a possibility that the data centre will become unavailable. Thus, an alternative site must be identified for the recovery of the IT systems. There are four types of alternative sites that can be set up for the IT DR:

Hot DR site refers to a fully functional site with redundant IT hardware, software and near real-time synchronised data. The production systems are commonly designed to recover IT systems within 30 minutes (Jones, 2010). The IT systems from the production site can be recovered automatically at the hot DR site, allowing business functions to resume almost immediately.

Warm DR site refers to a semi-functional site designed to achieve recovery of IT systems within 72 hours (Jones, 2010). This site has all the redundant IT hardware and software in place and ready for provisioning. Manual recovery or tape restoration has to be completed before the IT systems can be restored online.

Cold DR site refers to a site with no pre-existing IT hardware and software. This is only suitable for IT systems which can accept a recovery time of more than 72 hours (Jones, 2010). In order to convert the cold DR site into a hot DR site, there is a need to procure, deploy and configure the IT infrastructure as well as to restore the necessary data for the business functions to resume.

Mobile DR site refers to a leased or reserved stand-alone space unit placed on mobile trailers (Noakes and Diamond, 2001). This set-up is getting increasingly common as there is no need to secure a DR site in advance, avoiding the high premiums which have to be paid for building spaces. Mobile DR is also versatile enough to be deployed as a hot, warm or cold DR site, depending on the business requirements. However, it is important to note that the site planned for mobile DR deployment should have sufficient space and electrical power supply.

The type of alternative site to be implemented is determined by the required recovery time of the IT systems after a disaster. While organisations may like to achieve the near-zero downtime offered by a hot DR site, the costs to set up and keep the hot DR site running can be very significant. Table 1 presents the relative cost of each DR site set-up. Typically, it will cost 10 times more to implement a hot DR site as compared to a cold DR site.

	Hot DR Site	Warm DR Site	Cold DR Site
Expected IT Recovery Time	< 30mins	< 72hrs	> 72hrs
Relative Cost*	10X	7X	1X

* The relative cost is based on general industry assessments.

Table 1. Relative cost of alternative sites for IT DR

Data Recovery Plan and Infrastructure

Hardware and software can be replaced easily but data recovery can be extremely difficult. Organisations that fail to recover data are likely to suffer business losses which will also decrease the confidence of investors and customers. Hence, having an effective data backup plan and infrastructure is critical for IT DR.

The data backup and recovery technology can be viewed as a continuum of technological options, ranging from the basic off-site tape backup and recovery solution to complex real-time replication technologies (see Figure 3). The latter provides near-zero data loss, data compression, and bandwidth reduction for immediate system recovery and availability.

A typical off-site tape backup and recovery solution involves backing up data in tapes, transporting these tapes to the DR site and storing them securely. However, this solution relies heavily on manual effort which can result in human error, such as the misplacement or loss of tapes during transportation or failure to adhere to the right procedures during storage.

Advanced data replication technology can deliver real-time data replication (Jones, 2007) with near-zero data loss between the production and DR sites. The technology also possesses intelligent capabilities such as data encryption, data compression and de-duplication, which will reduce the demand on expensive wide-area network bandwidth. Although using this technology requires minimal human intervention, successful data replication is still dependent on network connection and bandwidth availability.

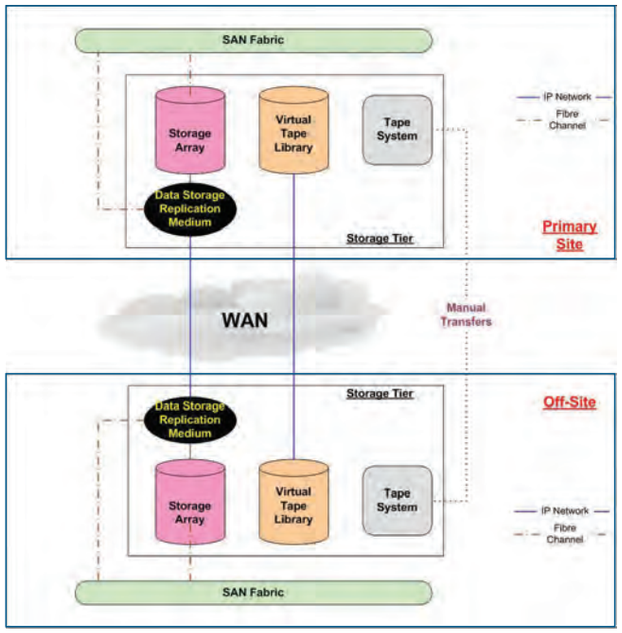

Figure 3. Data backup and recovery technologies

The data replication solution should preferably be deployed as the primary DR solution for critical IT systems as it is more reliable. The off-site tape backup solution can be used as a secondary backup for critical systems lest the data replication solution fails. It can also be employed as the backup solution for non-critical IT systems which can allow a longer recovery time.

Crisis Management Team

A formal crisis management team should be formed early and led by someone who has the authority to take charge and give immediate instructions when a disaster strikes. As part of the disaster response plan, the team should also establish a reporting structure to coordinate responses from all staff, give clear instructions to stakeholders, and mobilise the organisation in an efficient manner. Forming a centralised team minimises confusion which can arise from the various decisions made by individual teams. Thus, the organisation can react to the disaster more efficiently.

For effective containment and recovery, the crisis management team should include the following functions:

a) Corporate Communications

b) Site Management

c) Corporate Administration

d) IT Recovery

The roles and responsibilities of each function, as well as the contact details of relevant members must be defined clearly and updated in the IT DR plan. This will minimise the time required to activate all crisis management team members, creating a more efficient response to the disaster. Subject matter experts may also be co-opted into the team based on the nature of the disaster.

> Corporate Communications

The corporate communications function serves to ensure that clear and accurate messages are disseminated to stakeholders, media and staff in a timely manner.

Internal Communication. The first line of communication is with the CEO of the organisation. He or she needs to understand the extent of loss, especially if the disaster has resulted in human casualties, and if the situation has been brought under control. The CEO should issue clear instructions on the response to the disaster.

Staff involved in the IT recovery process may be uncertain of how they should react to a disaster. They also need to know the extent of damage to the IT equipment, the amount of recovery work required, and the time to start the recovery work. Those who are not involved in the IT recovery process are likely to be concerned about the impact to their work and the possibility that they may need to relocate temporarily. To minimise confusion and apprehension among staff, communication to staff must be timely and concise.

Stakeholders are concerned about the damage caused by the disaster. They should be kept up-to-date on the development of the situation and be informed about areas such as the extent of system damage, the amount of financial loss and the expected recovery time for business operations. While it is important to pay attention to stakeholders' interests, decisions made during a crisis must be based on objective considerations to remedy the situation.

External Communication. If the mass media obtains information on the disaster, the coverage in the public domain may have an adverse impact on an organisation and undermine public confidence in it. Throughout the entire disaster recovery process, the senior management and the corporate communications department must work closely together to communicate timely and accurate information to the media. This helps to assure the public that the organisation can manage the disaster well. It is also important to remind staff to direct all media queries to the corporate communications department to ensure that consistent messages and information are sent to the public.

> Site Management

The site management function serves to prevent unauthorised personnel from entering the hazardous areas and to secure the disaster zone for investigation.

For safety reasons, the site of the disaster must be secured immediately to prevent unauthorised entry. Although the data centre may remain intact after the fire has been contained, the building structure may have weakened substantially. Civil and structural engineers need to inspect the structure and certify that the disaster site is safe.

In addition, controlled access to the site ensures that the evidence is intact for fire investigations. The site and damaged IT equipment could reveal if the disaster was a deliberate criminal act. The evidence is also required for the processing of insurance claims. Any unauthorised person who has gained access to the site can destroy or tamper with the evidence unknowingly, causing a possible delay in the investigation process. This could also void the insurance coverage of the building and IT equipment. As a result, the organisation may have to bear the full costs of repairing the building infrastructure and replacing the IT equipment.

> Corporate Administration

With the disaster site out of bounds to staff, alternative arrangements have to be made for business operations to continue. The function of corporate administration is to provide resources for the relocation of work spaces and procure the necessary equipment for business operations to resume.

For work that needs to be performed at the data centre and offices, arrangements could be made for staff to share workspaces. For some organisations, additional network points may have to be implemented at the shared workspace for staff to connect to the organisation's network and IT systems. Other arrangements could be made for staff to work from home or other offsite locations. To facilitate their work, secure remote access to the IT systems has to be implemented.

During the IT DR planning, provision for shared workspaces or off-site locations must be made. The IT DR Plan should also include the activation procedures to facilitate staff access to the IT systems.

The corporate administration team has to be involved in assessing the office equipment to explore the redeployment of items which are still in working condition. Thereafter, they will replace the damaged office equipment and refurnish the office area for staff to resume work at their workstations.

> IT Recovery

The IT Recovery function serves to execute the IT DR plan and resume business operations as soon as possible. As each disaster scenario may differ, the IT DR plan needs to be flexible enough to adapt to various situations in a disaster.

Executing IT Recovery. The IT DR plan guides the IT recovery process. At the hot DR sites, the IT systems will be activated automatically to continue supporting the organisation's operations. For warm DR sites, the IT recovery team needs to bring the IT systems online before the organisation can continue with its operations. As for the cold DR sites, emergency procurement processes have to be activated to purchase and implement the hardware and software at the DR site.

Proper allocation of the organisation's emergency funds has to be done during the IT DR planning stage and be reflected in the IT DR plan. However, unforeseen circumstances, such as the price increase of equipment due to a global supply shortage, can affect the budget allocation. As such, it is important to prioritise the recovery of the most critical IT systems, while funds can be diverted from other areas to recover the rest of the IT systems.

Prioritising IT Recovery. The IT DR plan which was drawn up prior to the disaster should include a priority list of IT systems to be recovered. However, this priority list may change, depending on the organisation's needs at the time of the disaster. To illustrate how a change may be required in the priority list, a scenario where a fire has destroyed system A and system B can be used.

Out of these two systems which are used for testing and development, system A's recovery is accorded priority in the IT DR plan. At the time of the disaster, however, system B is on a tight project timeline and needs to complete its testing urgently for implementation. A delay in the implementation of system B may affect the organisation's capabilities and result in financial loss. On the other hand, system A is supporting a non-critical patch test. This situation may not have been foreseen during the IT DR planning phase. Thus, the IT DR plan needs to be adapted according to the situation to sustain the organisation's capabilities and minimise losses.

Staff Training

Having an IT DR plan in place can accelerate the recovery of IT systems, but the chances of resuming business operations within the stipulated recovery time are much higher if the plan is carried out by well-trained staff. Conversely, staff who are not familiar with the recovery process may be more prone to errors, leading to greater losses and a longer recovery time.

For instance, if the gas-based fire suppression system is activated, well-trained staff are likely to keep the room sealed, as the fire suppression system will reduce the amount of oxygen in the room so that a fire can no longer be sustained. However, an untrained staff may open the door to assess the situation, which allows fresh oxygen into the room to reignite the fire. If the fire is reignited, the water-based fire suppression system will be activated to put out the fire. In this case, the water may cause damage to the rest of the IT equipment in the data centre.

There are several other ways for untrained staff to increase the risk of a fire or worsen the damage caused by the fire unintentionally. This human element can be addressed by conducting formal training, periodic exercises and refresher courses. The training should include aspects like data centre configuration, use of various fire safety systems in the data centre, and the disaster response plan.

Insurance Policies and Claims

With appropriate insurance coverage for the data centre and its equipment, an organisation can minimise its financial losses in the event of a disaster. However, organisations do not usually receive full compensation for their losses. This could be due to unclear requirements and definitions, misinterpretation of clauses and coverage, or breaches in the insurance policy. It is thus important for organisations to review their insurance coverage on a regular basis. At the same time, the advice of subject matter experts should be sought to ensure that the insurance protection coverage is adequate and commensurate with the business value of IT assets in the organisation.

Processing insurance claims can be a lengthy process. Depending on the amount and quality of evidence available from the investigation, the insurance claim process can range from a few months to several years. This process may take longer if the investigation is delayed or extended, which will affect the organisation's cash flow or even force it to cease operations.

Hence, organisations should facilitate the investigation process by providing the relevant evidence to investigators and by submitting an insurance claim that is written clearly. It is important to ensure that the claim statement should coincide with what is written in the policy. For example, if the insurance policy states that the organisation can only claim for the "restoration" of IT equipment, claims for the "replacement" of IT equipment may be rejected by the insurance company.

CONCLUSION

It is essential for organisations to plan ahead and prepare for IT disasters, to prevent severe disruption to their operations. Implementing an IT DR plan that only focuses on recovering the IT systems is insufficient. The IT DR plan should also consider other factors which can minimise the impact of the disaster, manage the situation and recover the IT systems swiftly. Sufficient preparation for an IT disaster will minimise losses and allow organisations to resume business operations in the shortest possible time.

REFERENCES

Downes, L. 2009. The Laws of Disruption: Harnessing the New Forces that Govern Life and Business in the Digital Age. New York: Basic Books.

Jones, R. 2010. Data Center Availability Gartner, Inc. http://www.gartner.com/DisplayDocument?doc_cd=203965 (accessed 16 July 2011)

Jones, R. 2007. Survival of the Fittest: Disaster Recovery Design for the Data Center. Burton Group. http://crescententerprise.net/paper/filename/13/Burton_Group_-_Survival_of_the_Fittest_-_Diaster_Recovery_Design_for_the_Data_Center.pdf (accessed 16 July 2011)

Noakes-Fry, K. and Diamond, T. 2001. Business Continuity and Disaster Recovery Planning and Management: Perspective. Gartner, Inc. http://www.availability.com/resource/pdfs/DPRO-100862.pdf (accessed 23 July 2011)

Shore, D. 2002. Sept. 11 Teaches Real Lessons in Disaster Recovery and Business Continuity Planning. TechRepublic, 17 May. http://www.techrepublic.com/article/sept-11-teaches-real-lessons-in-disaster-recovery-and-business-continuity-planning/1048799 (accessed 24 July 2011)

BIOGRAPHY

Feng Ziheng is a Senior Engineer (Infocomm Infrastructure). She drives the set-up of the Integrated Workforce for data centre operations in the Ministry of Defence (MINDEF). She is also involved in the design and development of the next-generation data centre for MINDEF and the Singapore Armed Forces (SAF). Ziheng has designed and implemented messaging systems for MINDEF and the SAF, including the disaster recovery set up which won the MINDEF Corporate IT Award in 2010. Ziheng obtained a Bachelor of Engineering (Electrical and Electronics) degree with Honours and a Master of Science (Knowledge Management) degree from Nanyang Technological University in 2005 and 2009 respectively. She received further certification as a Data Centre Specialist from Enterprise Product Integration (EPI), and as a Business Continuity Planner from Business Continuity Management Institute.

Yee Keen Seng is a Senior Engineer (Infocomm Infrastructure). He oversees the development and design of the next-generation data centre for MINDEF and the SAF. Previously, Keen Seng established the MINDEF Data Centre master plan for Corporate IT systems and managed the operations of an existing MINDEF data centre. He served in the SAF Chief Information Officer Office, where he managed the development and governance of the SAF Enterprise Architecture Framework and pioneered the Ops-Admin Systems Integration initiatives. He also managed several best-sourcing projects including the provision of shared services and end-user IT support to MINDEF and the SAF. Keen Seng is certified by EPI as a Data Centre Specialist, and by Institute of System Science (ISS) as a Certified Enterprise Architecture Practitioner. He holds a Bachelor of Science (Information Systems and Computer Science) degree from the National University of Singapore (NUS).

Lim Hwee Kwang is Head Capability Development (Information Assurance). He is responsible for ensuring information assurance in MINDEF, the SAF and DSTA. He builds and maintains the required information assurance engineering competencies in DSTA. He plays a key role in establishing IT Security architectures and plans, as well as developing and providing cost effective IT Security solutions. He also oversees the enforcement of information assurance standards through audits, vulnerability assessments and security reviews. Hwee Kwang managed a portfolio of Infocomm Infrastructure projects when he was the Assistant Director (IT Infrastructure) in MINDEF and the SAF. He built disaster recovery capabilities for critical IT infrastructures and led the development of the master plan which charted the development of data centres in the SAF. Hwee Kwang holds a Master of Science (Information Security) degree from Royal Holloway, UK and a Master of Science (Management of Technology) degree from NUS. He further attained the Chief Information Officer Certificate as a Top Distinguished Graduate in the National Defense University, USA in 2007.