Example of computer security: disaster recovery plan research paper

Business, Management

Businesses use information technology to quickly and effectively process information. Employees use electronic mail and Voice Over Internet Protocol (VOIP) telephone systems to communicate. Electronic data interchange (EDI) is used to transmit data including orders and payments from one company to another. Servers process information and store large amounts of data. Desktop computers, laptops and wireless devices are used by employees to create, process, manage and communicate information. What do you when your information technology stops working?

An information technology disaster recovery plan (IT DRP) should be developed in conjunction with the business continuity plan. Priorities and recovery time objectives for information technology should be developed during the business impact analysis. Technology recovery strategies should be developed to restore hardware, applications and data in time to meet the needs of the business recovery.

Businesses large and small create and manage large volumes of electronic information or data. Much of that data is important. Some data is vital to the survival and continued operation of the business. The impact of data loss or corruption from hardware failure, human error, hacking or malware could be significant. A plan for data backup and restoration of electronic information is essential.

For an IT disaster recovery planning project, designing of an in-depth recovery plan is highly crucial and rather the main objective of the organization. An effective disaster recovery plan is a detailed set of steps that needs to be undertaken by an organization to help recover its IT systems to an extent at which they can support the business at the

occurrence of a disaster (Kirvan, 2013).

This paper illustrates the disaster recovery plan and associated contingency requirements for TechPro, Inc. TechPro, Inc is a software company offering IT consulting services to clients worldwide, providing customized technology and consulting services with expertise in Customer relationship management (CRM), Business process management (BPM), and Enterprise resource planning (ERP). With a workforce of nearly 800 employees, TechPro has been successfully offering state-of-the-art consulting solutions for Telecommunications, Logistics, Finance, Supply Chain, and Marketing. The development team comprises of Project Managers, Senior and Top level software developers, Business Development Managers, ERP and BPM Architects, Finance executives, and several junior staff members.

This paper describes the practices and processes for mitigating disruptions to “ critical information systems” or loss of data and services from the impacts of man-made or natural calamities.

This plan is a means of responding to both major, normally ruinous, events which disallow access to the everyday facilities for a time span, and to less severe disasters that might disallow access to only segments of some system or the facility.

The DRP is a technology-specific plan to safeguard and retrieve valuable information and hence may be referred to as a Technology Recovery Plan. It has been designed to help restore operability of the assigned applications and systems in TechPro’s data centre system at an alternative site on the detection of an emergency. The current DRP was devised by and for TechPro’s IT group.

Proposed Recovery assumption: At the event of total loss of the data centre

- Firstly, the system will divert to a fully functional Hot Site with all the backup communication services and infrastructure need to resume vital operations within a comparatively short span of time.

- Once the hardware is easily acquirable and can be installed at a Cold Site, the processing will be shifted to the less costly cold site from the Hot Site.

- Processing of all applications will be eventually performed at the cold site, even those which are not seen as critical.

- The reconstruction of the original or a new permanent system work simultaneously with the backup sites, i. e. Hot and cold sites. The planning for the last transfer back to the site is also done here

With the many benefits of implementing the hot and cold site and taking its advantages as described above, IT workforce is able to successfully restore valuable production functions and data at their own system in the shortest possible time frame after a disastrous event.

It is understood from the above explanation that the cost pertaining to a Hot Site is greatly different as compared to a Cold Site. Therefore, the importance of the initial steps is importance for business value/impact. This helps in determining the appropriate investment level for protecting the business (FEMA, 2012).

Moreover, data replication can be implemented in more than one way, in a Hot Site scenario. These mechanisms include timed-copying of files or database backups, which is the cheapest of all mechanisms, performing software duplication like Double-Take Software’s Double-Take or SAN-to-SAN

hardware-based data replication which costs the most and is a complex method.

Formulating an effective disaster recovery plan aids the organization’s business to deal with IT disasters to get back up and running as quickly as possible. A DRP usually encompasses all kind eventualities, from virus to cybercrimes, to flood or fire damage.

Nonetheless, for many businesses, such as TechPro, it is their intellectual property which makes them stand out from their competitors. This intellectual property is kept in computer memory where there are possibilities of corruption, deletion, damage or theft. Hence, a DRP works as an insurance policy to preserve these intangible assets, along with the computer hardware and the servers.

TechPro recognizes that software is a primary tool for all the lines of business. It understands the need for specific protective steps to be for protecting the investment and ensuring maximal business and functionality continuity at the occurrence of a disaster.

Key assets are identified and the effect of loss of each asset on business is identified first, while creating DRP or Business Continuity plan of TechPro. This activity is performed regularly in the company’s security policy engagement and DRP workshop. This activity helps in determining the appropriate security needed for every identified.

Some of the examples of assets considered are:

- Accounting or ERP System and related parts (order entry, inventory, warehouse management, etc.);

- Files and Documents on your Local Area Network;

- Product Designs and Specifications (written/electronic);

- Business Strategy Documents (written/electronic);

- Facilities and Fixed Assets;

- Paper Files and Documents;

- Cash and Valuables on Premise;

- Employee Knowledge and Staff Expertise (human resources);

- Product Inventory and Raw Materials.

Secondly, it is essential to evaluate threats against the business as well as each asset. For instance, organizations that are geographically diverse have a wider range of threats based on this.

TechPro considers the following potential threats:

Natural Threats

- Fire

- Floods and Flash Floods

- Earthquake

- Hurricane/Storm

Man-Made Threats

- Terror Attacks

- Theft or Vandalism

- Bio-Hazard

- Epidemic/Pandemic

- System Crash

- Cyber Crime

- Riot

- Power/HVAC Failure

- Communications Failure

- Software and Hardware Failure

- Security Breach/ Incident

After this step, various scenarios will be defined depending on varying threats at every location. Pre-defined actions will be included in these scenarios to decide on whether or not a disaster must be declared and whether or not the Disaster Recovery site must be activated.

A key component in the DRP is an Emergency Operations Center, such a location wherein workforce and partners responsible for executing on the DRP can meet for working together and can access resources and communicate with decision-making authority. This location must be pre-established and must store resources like office supplies, telecommunications, communication lines, food and water, etc. commonly situated at the hot site used for the data centre.

Another crucial rule of DRP is “ People First.” As per this rule, the safety of workers and personnel is given higher priority than saving assets or business recovery functions. TechPro considers this fact and employees it in their DRP.

“ Keeping organizational information assets secure in today's interconnected computing environment is a true challenge that becomes more difficult with each new " e" product and each new intruder tool”. Many companies understand that there are multiple solutions or panaceas for protecting data and systems; rather, there is need for a multi-layered security strategy. An

important layer included by several organizations in their strategy nowadays is the formation of Computer Security Incident Response Team or CSIRT (Cert, 2006).

In TechPro, factors driving the creation of CSIRT include:

- A greater number of computer security incidents being reported
- An increased type and number of organizations being impacted by computer security breaches/ disruptions
- An increased awareness and focus by organizations on including strict security policies and practices in their overall risk-management schemes
- Newer regulations and laws which determine the way organizations are necessitated to secure information assets
- The need to realize that the network and systems admin team are unable to secure protect organizational assets and facilities single-handedly

While building an IRT, the following factors were also considered by TechPro:

At the initial stages of building their incident response team/ capability, organizations look to identify the most efficient strategy to implement such a structure. Organizations are not just curious about knowing what has been beneficial for their competitors, but also need some aid in the process and pre-requisites they must adopt for establishing an efficient IRT or capability.

Typical elements that need to be considered but not limited to, while developing a IRT are:

- What are the fundamental pre- requisites for creating a IRT?
- What kind of IRT will be required?

- What is the size of IRT?

- What kind of services ought to be provided?

- What is the location of IRT in the organization? At what level?

- What is the overall cost for implementing and supporting a team?

- What must be the initial measures to undertake while establishing a IRT?

Every organization has a unique IRT, so no two teams can function in the exact similar fashion. Also, organizations must be assured of the decision for building an IRT and what the objectives defined for the IRT. After this is identified, it becomes easy for IT personnel or back-up managers to formulate answers for the aforementioned questions.

Best Practices for Creating IRT:

Even though IRTs are most likely to differ in their functionality based on the available workforce, budget resources, specialization, and unique circumstances of every firm, there still exist, some basic practices applicable to all IRTs. Even though these activities are illustrated step-wise, it is likely that they may occur in parallel as the process is not sequential.

Step 1: Obtain management support and buy-in: to build an efficient IRT, management approval and support is important. This support includes supply of resources, time and capital to the group of personnel employed as the project team for executing IRT. Apart from this, the management must show commitment to sustain IRT functions and authority for the long-term business (Cert, 2006).

Step 2: Determine the CSIRT strategic plan: in this step questions like “ how the development of the IRT will be managed?, what are the administrative

issues and how they will be dealt with?, what project management problems must be resolved?” need to be addressed. Here the realistic time frames or deadlines must be set, a project group must be assigned, and development of the IR capability must be updated to the organization personnel, and so on. This step demands the project team to record and communication the collected data, particularly if it is geographically dispersed.

Step 3: Gather relevant information: information collection is important to determine the incident response and service requirements of the company. Data can be best gathered via general discussions, interviews, online discussions, surveys, etc. with concerned members of the organizational staff. A meeting with prime stakeholders will be conducted to discuss the organization’s incident response requirements as well as to obtain an initial agreement on definitions, strategic focus, expectations, IRT responsibilities, and so on. Typically, come of the stakeholders include business managers, representatives from IT, representatives from the legal department, HR representatives, representatives from public relations, any existing security groups like physical protection, risk and audit management experts, constituency representatives.

TechPro, Inc makes sure agreements are made regarding the IRT’s authority over business systems and who will make decisions if vital business systems need to be shutdown or disconnected from the base network.

Furthermore, information can be gathered by reviewing some resources like:

- organization charts for the enterprise and specific business functions

- topologies for organizational or constituency systems and networks

- critical system and asset inventories

- existing disaster-recovery or business-continuity plans

- existing guidelines for notifying the organization of a physical security breach

- any existing incident-response plans

- any parental or institutional regulations

- any existing security policies and procedures (Cert, 2006)”

Step 4: Design the CSIRT vision

Step 5: Communicate the CSIRT vision and operational plan:

TechPro communicates the IRT vision and functional plan to management, with its constituency. The plan is adjustable according to the feedback.

Step 6: Begin CSIRT implementation: here, the IRT staff is appointed and trained, equipment is purchases and the necessary network infrastructure is built for the team. Once specifications are defined, the incident tracking system is set up along with the initial set of IRT policies, regulations procedures. After this, the incident-reporting guidelines are developed.

Step 7: Announce the operational IRT: the IRT is declared across the constituency of the organization as soon as it is operational. TechPro uses a sponsoring management to make this announcement. This activity may also include distribution of brochure or flyers to publicize the IRT missions and services.

Step 8: Evaluate IRT effectiveness: TechPro evaluates the effectiveness of its IRT and their services by gathering a broad array of feedback mechanisms such as:

- benchmarking against other IRTs

- evaluation questionnaires sent across company personnel and constituency members regularly

- conducting general discussions with representatives

- Establishing a defined set of quality criteria to be employed by an audit or 3rd party for evaluating and assessing the working of the IRT.

After discussing the importance of a robust and practical DRP, it must be noted that in-depth planning and organization is highly essential for defending an organization’s IT assets. “ Documenting procedures for different incident types should be detailed, but at a level to allow flexibility for variations to different scenarios of similar types of incidents” (Quality Technology Solutions).

TechPro has created a practicl DRP to be used by an efficient and highly reliable IRT. It uses the incident response plan as a living document and all incident processes take advantage of the above processes and update its documentation on regular basis. With proper implementation, an incident response plan is capable of reducing the damage caused by an incident, to a great extent, and can reduce the time period needed by the IT environment to restore and resume to normal operation.

References:

Cert, (2006). “ Creating a Computer Security Incident Response Team: A Process for Getting Started”. Retrieved http://www. cert. org/csirts/Creating-A-CSIRT. html.

FEMA, (2012). “ IT Disaster Recovery Plan”. Retrieved http://www. ready.

gov/business/implementation/IT.

Kirvan, P. (2013). “ How to write a disaster recovery plan and define disaster recovery strategies”. Retrieved http://www. computerweekly. com/feature/How-to-write-a-disaster-recovery-plan-and-define-disaster-recovery-strategies#structure.

Quality Technology Solutions, “ 10 steps to implement a disaster recovery plan”. Retrieved http://www. qtsnet. com/StayInformed/White%20Papers/10%20Steps%20to%20Implement%20a%20Disaster%20Recovery%20Plan%20-%20QTS%20White%20Paper. pdf