Cis 462 assignment term paper example

Business, Management

AT&T Overview

AT& T corporation is a leading company in providing telecommunication services. It has been a successful company over the years with annual revenues being in excess of $74 billion. According to Tung (2001), AT& T offers services worldwide. These services include wireless services, long distance services and local telephone services, home entertainment, online services, local telephone and highly sophisticated communication networks. AT&T operations, alliances, and joint ventures offers employment to more than 100, 000 people worldwide (Tung, 2001). AT&T currently provides the largest 4G network coverage in the world. Further, the company's Wi-Fi network is the largest in the country with over 30, 000 Wi-Fi Hot Spots in hotels, bookstores, and restaurants.

Business Goals

AT&T aspires to increase its supplier base and at the same time ensure diversity of its suppliers. As of 2012, the company was trying to maintain a spending of $12 billion on women and disabled veteran owned business enterprises. AT&T tries to achieve21. 5 percent of all its products from the minorities and women, which makes them to have the best supplier diversity program in the country. Additionally, AT&T has a collaboration programs that encourages developers to partner with the company as a means of accelerating new application development.

AT&T Network Architecture

Disaster Recovery Plan Policy

A disaster recovery plan policy is essential for such a large organization such

as AT&T. This policy will have to be reviewed annually to ensure that it is relevant to the changing trends in technology. The review will be done by a number of personnel from the organization. This will include information security personnel, senior management personnel, information technology professionals, and human resources personnel. This team will be involved in developing the disasterrecovery policy. Some of the responsibilities of the team during reviewing will include risk assessment to establish the current information security vulnerabilities, conduct a business impact analysis to establish the interdependencies between the different business functions and processes, record all the information systems assets, identify critical personnel and applications and prioritize the main business functions in order of their importance.

Disaster Declaration

Upon the occurrence of a disaster, a disaster declaration policy will be used to provide the process by which the Disaster Recovery Plan will be executed. Since AT&T is primarily a technological organization, cases of IT disruptions will be quite common, thus a declaration statement will be essential in defining roles and responsibilities of the DRP team. According to Johnson (2010), the disaster declaration is important, as the cost incurred in disaster recovery for a large organization is high. Thus, the authority to declare a disaster needs to be tightly controlled.

The process of declaring a disaster will involve the following(Johnson, 2010).

- Emergency notification of all personnel and stakeholders
- Activation of the alternate site

- Activation of emergency control center
- Preparation of transport and housing arrangements
- Letting go of pre-positioned assets

Role and Responsibilities Defined in the Declaration

Personnel involved in the disaster recovery will include several teams. These will include a disaster incident management team, a recovery action team, a salvage team, and a communications team.

Disaster Management Team: this team will consist of the information security officer, head of operations, senior management personnel of the information technology services, head of disaster management services and head of customer services. The team shall be responsible for setting targets and declare when the recovery operations are complete.

Communications Team: this team will be responsible for facilitating any communications regarding the incident. They will ensure that the effects of the incident are minimized to ensure the organization maintains its reputation. They will be responsible for informing other personnel on the issues regarding the incident. Any information concerning the disaster will be communicated through the communications team.

Salvage Team: this team will be responsible for organizing and implementing relevant actions to take following the disaster. This team will prepare an outline of the activities to be carried out. Additionally, the salvage team will ensure that the remaining available resources are used effectively in aiding the recovery process.

Recovery Action Team: this team will be responsible for planning any recovery operations and select a suitable alternative site for operations. The

activities to be carried out during the recovery process shall be detailed and comprehensive. This team will not be involved in any form of external communication. The leader of this team will constantly update the Disaster Management Team of the recovery process and status as and when required.

Assessment of Security

Security assessment will be vital to ensure that occurrences of disasters in the future are reduced. One of the key tasks that will be conducted is the security assessment of all personnel involved in the information technology processes and communications. Furthermore, the physical security and operating procedures of the organization will also be accessed. Other critical areas that will need to be accessed will include personal computers, the backup and contingency plans and access control software security. Performing the security assessment will provide valuable information on possible areas where the organization can improve its security measures. The security assessment will be conducted by a Security Team comprisedof the information security officer and information technology personnel. Based on the finding they get from the security assessment, the team will be required to present their findings to the disaster management team. Further, the Security Team will be required to forward any recommendations concerning the security issues of the organization to support the recovery process.

Potential Disaster Scenarios and Methods of Dealing With the Disaster

Fire

Fire is one of the most common potential disasters that may affect the organization. According to Snedaker (2011), in the event of a fire there is expected to be damage to the building, systems, and corporate records. One of the methods of dealing with potential fire threats is to seek assistance of the fire department in identifying and eliminating or reducing potential fire risks. Developing a fire response plan can be quite an effective means of handling a fire in case it occurs. Furthermore, performance of frequent fire drills can help improve the response and safe fire evacuation procedures. To protect the information technology systems such as the servers, the organization needs to set up chemical fire suppression systems in the server rooms. Overhead water sprinkler prevention systems are not recommended in the server rooms as they may cause more damage than the fire itself.

Cybercrime

Cybercrimes that may pose a threat to the organizations include corporate identity theft, hacking of corporate network to breach confidentiality, stealing and selling confidential data such as intellectual property and hacking of the corporate website. Most of the cybercrimes threats can be handled by ensuring that only personnel with authority access the corporate networks. Additionally, any the activities of the personnel on the company’s network need to be monitored constantly to ensure that no suspicious activity is being done. Additionally, passwords for accessing the intranet need to be changed constantly.

Information Technology System Failure

Information technology systems may be sabotaged intentionally or unintentionally. The intentional acts need to be addressed as criminal activities. Theft of information technology equipment may also occur. For instance, theft of servers, firewalls, routers, cables and other information technology assets. Routine security checks of personnel leaving the organization’s building need to be done to ensure no employee carries any equipment that belongs to the organization.

Disaster Recovery Procedures

The recovery procedures will be carried out to ensure that all critical applications and information technology systems are recovered efficiently.

- The first step will involve moving the operations of the organizations to an alternative backup site. This will be done once the Disaster Recovery Plan is activated. The recovery team will ensure that this is done within 24 hours after the actual disaster occurs.
- The second step will involve the reinstatement of all critical business functions and any network activity that is necessary for the organization to operate. This will be done to ensure customer service resumes as quickly as possible.
- After the initial site has been repaired or another permanent facility has been identified, the business functions and operations of the organization can be returned to the original site or a new site.

Incident Response Team Charter

Executive Summary

The Incident Response Team Charter will cater for all the activities and actions that will be carried out by the incident response team. Recommendations from the incident response team will be forwarded to the senior management for approval and executed thereafter.

Mission Statement

The mission statement for the Incident Response Team Charter will be " Provide support to the business functions and processes by ensuring prompt mitigation of all incidents affecting the operations of the organization".

Incident Declaration

The Incident response team will be responsible for incident declaration. The incident response team will provide on-site response. This implies that the IRT will have the full authority to contain the breach or incident.

Organizational Structure

The organizational structure will include subject matter experts in different business functions of the organization and members of the information security team.

- Information technology subject matter experts: Their extensive knowledge and technical skills on IT systems will be a necessary part in the incident response team.

- Human resources personnel: human resources will be important, as they will provide ways of dealing with employees in cases of incidents. Further, the human resources will provide advice on ways to deal with incidents

caused by employees.

- Information security representative: These personnel will be important in providing risk management and analytical skills that may be useful in collecting forensic evidence.

- Legal counsel: an essential part in reviewing the incident response policy and procedures to ensure compliance.

- Business Continuity representative: aid in assisting the restoration of the system and network to functioning capacity.

- Public relations representative: provide guidance on the proper means and messages of communication after the incident occur.

Organizational Structure

Roles and Responsibilities

Management

Management will be responsible for providing support to the IRT in terms of leadership. In case of barriers or problems that may develop as the response team goes about its duties, management will ensure that these problems are resolved. Management will also be responsible for approving any recommendations, which the IRT recommend.

Information Security Personnel

Information security personnel will be responsible for detecting the incident or breach. Activation of the incident response team will be done by the information security personnel. Additionally, the information security personnel will be responsible for containing the incident, conduct forensics analysis, and conduct the recovery process.

System Administrator

System administrators will provide immediate threat response. Based on the technical skills they can be able to identify a threat and modify the system to reject the threat.

Users

Users are responsible in aiding the efforts of the incident response team. Once a user detects a threat, it is important to report the issue to the system administrator who in turn will liaise with the incident response team.

Support Services

Support services are essential in cases where the customers need any assistance during after the incident. The support services team will handle the customers who are directly affected by the incident or threat. The public relation department will be a significant part of the support services team in terms of maintaining communications with the customers.

Information Flow and methods of communication

Public relations personnel will be responsible for all forms of communication with the media and the customers. However, prior to making any public communications, the public relations personnel will inform the senior management of the content of the message and wait for their approval before informing the customers and the media. The IRT will also be required to inform the senior management of any recommendations and wait for their approval before proceeding.

Methods and Services Provided by IRT

Incident response team services and methods will include monitoring of the system and network activities, disabling access to systems that have been compromised, disabling systems services, identify the source of the threat and eradication of the threat (Whitman and Mattord, 2013).

Authority and Reporting Procedures

Johnson (2010) indicates that reporting procedures need to be clearly defined. Thus, methods of collecting data, analyzing data and reporting data need to be defined.

Collecting Data and Classification

Once the incident report is received, the first procedure involves classification of the incident. Classification will be used to establish the severity level of the incident (Johnson, 2010). If the severity level reaches a certain predefined level, the IRT is activated.

Analyzing data

Analysis will involve several steps.

- The first step in this case will involve updating the network diagram and inventory to ensure the current network is being used.
- Mapping of the traffic network will be done to ensure all information is captured.
- Understanding of the business process will be done to ensure normal behavior is clearly defined.
- All logs of the threat will be kept in in accessible area and this will then be used to develop a knowledge base of the threats.

Reporting the data to Authority

The IRT will forward their final recommendations to the senior management level for their approval. Once the senior management approves their recommendations, the IRT will have the authority to execute their recommendations.

References

AT&T Common Architecture for Real time Services. Retrieved from http://www. business. att. com/content/whitepaper/w_ATT_CARTS. pdf

Johnson, R. (2010). Security policies and implementation issues. Sudbury, Mass.: Jones & Bartlett Learning.

Snedaker, S. (2011). Business continuity & disaster recovery for IT professionals. Burlington, MA: Syngress.

Tung, R. L. (2001). Learning from world class companies. London: Thomson Learning.

Whitman, M. E., & Mattord, H. J. (2013). Principles of incident response and disaster recovery (2nd ed.). Cengage Learning.