Example of essay on business security issues and essentials of disaster recovery ...

Business, Management

Introduction: The existence of fierce competition as a consequence of globalization had made it inevitable for any business today to get equipped with the latest information technology available relevant to the management to facilitate its lucrative survival. This is where information systems come to the rescue of businesses to help them gather, store, organize and distribute large volumes of relevant data in an accurate, concise and timely manner to assist easy usage and retrieval of such information. Consequently, the businesses could efficiently perform their functions pertaining to decision-making, problem solving and control.

As a result an immense amount of dependence on the information technology has become inherited in almost all the businesses in the present era. It is essential to ensure timely availability, strict confidentiality and proper integrity of the data pertaining to the business. The variants of security issues faced by any business due to its enormous dependency of the information technology are as follows. The errors that occur on the part of the users, such errors most of the time are malevolent in nature. Attacks devised by hackers to steal information or make considerable changes to the information about the business in question. Attacks devised by unauthorized users to misuse the information for personal benefits while causing substantial losses to the business. Unethical hacking can be done by either internal or external sources to disrupt the services and damage the brand image of the business. Therefore the potential security threats to any business can be broadly recognized as

Disaster Recovery: A disaster can be defined as an unexpected catastrophic occurrence that can hinder the normal functioning of a business and disrupt

its critical processes. Disaster recovery can well be understood as a procedure employed to recover as much significant data as possible that was otherwise lost in the event of a disaster to enable business continuity. A disaster recovery plan forms an integral part of a Business Continuity Plan which aims to address the function oriented problems of a business from a broader perspective. The components of an effective disaster recovery plan are:

1. Development of a relevant contingent planning group
2. Performing risk assessment and relevant audits
3. Deciding on the priorities of involved applications and processes
4. Preparing for the backup resources while carefully documenting the plan
5. Provision for the efficient training of the required back up resources
6. Deciding on an offsite emergency meeting place
7. Observe immediate responding in emergency situations through realistic exercises
8. Deciding on an efficient communication system during the crisis period
9. Establishing verification criteria and procedures.
10. Working with emergency responses (PD/FD/EMT)
11. Implement the plan and evaluate the performance and suggest for further improvements if required.
12. Conduct testing on a regular basis

An effective disaster recovery plan is one that directs its endeavors towards facilitating a feasible, efficient and cost-effective recovery of data concerning the technology department of the organization.

The ethical and information technology issues pertaining to business

decision making that are encountered by the contemporary managers and its restoration are discussed below:

Privacy of any information relating to either employees or consumers is of considerable significance to the managers. Improper handling of such information can lead to stress among employees and conflicts from consumers. Hence ensuring the security of such information becomes of utmost importance to the managers. The volume of efforts and expenses involved on the part of the managers to gather the required data needs a proper justification so that the resources involved are efficiently used and the privacy of the parties involved is not breached after a certain undesirable limit. Other issues of significance are freedom of speech while not popularizing unethical practices, maintaining professionalism by conforming to the required practices and eliminating social inequality by not promoting it.

Conclusion: Business intelligence is a system that facilitates efficient decision making in a business by making vigilant combination of the operational data and the analytical tools available to the managers. Such system makes the most out of the unstructured data to present a clear picture that in turn helps efficient decision making. In order to keep alive the ethical values in the business it becomes the responsibility of the managers to ensure conforming to practices such as compliance, fulfilling responsibility and preserving the privacy and rights of concerned parties.

References

1. James A. O'Brien, George M. Marakas. (2006). Management Information Systems. Irwin: McGraw hill.

2. Jackson, I. (1996). Corporate Information Management. New Jersey: Prentice-Hall International

Appendix

Diagram Illustrating the Potential Security Threats