Management actions prior to cyber attack and business continuity plans research p...

Business, Management

Business continuity plans

Management actions prior to cyber attack

“ A cyber-attack is an attack initiated from a computer against a website, computer system or individual computer (Holland&Knight, 2013).” It compromises the integrity or confidentiality of information stored in it. The management should determine and evaluate the company’s security chain in order to identify any weak links. The management should formulate a compliance work plan to monitor the highest risks of a cyber-attack. The company should implement an enterprise wide data management program to mitigate the risk of losing company data. The management should also invest in computer security equipment and implement procedures to deter cyber-attacks.

Crisis management can be defined as the identification of threats to an organization and the methods used to manage these threats. It requires decisions to be made within a short time frame and after the threat has already taken place. Crisis management is part of disaster management as when any disaster man made or natural paralyzes normal operations the organization is faced with a crisis (Managementstudyguide. com, 2013).

Business continuity plans

A business continuity plan helps an organization prepare for disruptive events and allow the resumption of business processes. A business continuity plan is essential in preventing losses in revenue brought about by disruptions. Development of a continuity plan involves four steps: first conduct a business impact analysis to identify critical business processes. Then there is identification, documentation and implementation to recover critical business processes. Thirdly, organizing a business continuity team to formulate a business continuity plan. Finally, conducting training for the team to evaluate recovery strategies (Ready. gov, 2013). Components of a good business continuity plan include: a risk or threat assessment like financial exposures and employee issues. There is the business impact assessment that is the impact on the business upon losing business functions. The third is the business continuity plan itself containing recovery steps for the business. Then there is the IT continuity plan and the emergency response plan. IT recovery is high in priority for companies and complex in nature so the need to incorporate it in the continuity plan. The emergency response plan is invoked when an event affects facilities or people (Examiner. com, 2013).

References

Examiner. com. (2013, June 4). Components of a good Business Continuity Plan. Retrieved from www. examiner. com: http://www. examiner. com/article/components-of-a-good-business-continuity-plan

Holland&Knight. (2013, June 4). Cyber Attacks: Prevention and Proactive Responses . Retrieved from www. hklaw. com: http://www. hklaw. com/publications/Cyber-Attacks-Prevention-and-Proactive-Responses

Managementstudyguide. com. (2013, June 4). Disaster Recovery and Crisis Management:. Retrieved from www. managementstudyguide. com: http://www. managementstudyguide. com/disaster-recovery-and-crisis-management. htm

Ready. gov. (2013, June 4). Business Continuity Plan | Ready. gov:. Retrieved from www. ready. gov: http://www. ready.

gov/business/implementation/continuity