Ipremier denial of service attack essay sample

What I would have done differently as CIO of iPremier Company

If I were the Chief Information Officer of iPremier, I could have coordinated those available at home to get the cause of the problem as fast as possible before it posed a threat on the computer system. This is considering I was out of town on business and therefore I could not handle anything personally. The first person I would have called would be Tim Mandel the Chief Technology officer immediately Leon Ledbetter called to inform me about the incident. This would ensure that he can co-ordinate the people on the ground. I would inform him first because he is the closest in command to me in the department. I would then proceed to talk to Joan Ripley to know how far she had gone in the investigation and give suggestions on the possible signs to look out for. The CIO in this case relied too much on Joanne and did not give considerable suggestions on what should be done about the attack.

Considering that I am a senior personnel in the Information Technology department, I would carry the contacts of Qdata with me wherever I go such that I could easily contact them in case of such an incident. This means that I would have contacted Qdata requiring them to check all traffic coming into our site so as to identify and stop the lines that were causing the problems. A series of calls would then follow after this to get the progress of the operations back at home.

Risks faced by iPremier as a result of the crisis

As a result of the crisis, iPremier faced the risk of losing customer data (Austin, 2001). If the DoS attack had turned out to be hacking, there would have been serious consequences especially if the hackers wanted to steal customer information. Theft of customer information by malicious competitors is one of the causes of computer hacking. The company would have consequently lost its customers such that major losses would have been witnessed.

Customer credit cards were at a risk of being stolen. ipremier customers paid through credit cards and if the hackers accessed the company's system there could have been a risk of credit cards being stolen from the system (Austin, 2001). Customer's money could have been stolen and recovering the credit cards could have been almost impossible or take a very long duration to implement. The direct result of this would be decrease in sales in the firm.

ipremier faces the risk of loss of customers following the attack. First of all, had the disconnection of the system taken place in trying to protect the system, it would take time to bring it back to normal hence cut communication with the customers (Austin, 2001). This in turn would result in loss of customers. As the CEO Jack Samuelson told Bob Turley in their telephone conversation, public relations issues had to be handled very carefully following the incident (Austin, 2001). Warren also points out that reporting the matter to the police would arouse the public's knowledge of the incident leading to panic among customers. The firm therefore faced a threat of losing its customers from the incident.

The crisis threatened to impact on the stock immediately the public got wind of what was happening (Austin, 2001). The stock takes were due the following day and as the VP for business development Warren Spangler noted, there was going to be an impact on the stocks. This would affect the business development department which was planning on obtaining options.

My priorities during the crisis as CIO of iPremier Company

My first priority would be to solve the hacker crisis and put the system back on track. This would mean doing everything possible even if there was a risk of the public knowing about the incident. What was most critical at the moment was for the customer information which the company relied on so much to be saved and prevent the credit cards from being stolen. The issue of public knowledge could be saved through good public relation strategies but the data and credit cards would prove harder to come by. This means that as the CIO I would put the prevention of data theft as a priority before the publicity risk.

Deficiency of the company's operating procedures

Yes. The company's operating procedures were deficient in responding to the attack. First of all, there were no specific procedures that had been set for incidence response even as iPremier officials kept saying they would address the issue. The binder that they could have used to protect the website in case the incident got serious was out of date (Austin, 2001).

There ought to be good procedure set to be used in case of occurrence of such an incident in future. The best system is where the network is installed with a self-defense mechanism to curb any attempts of DoS attacks (Embar-Seddon, 2002). However, like in this case where the cause was not well known, an incident management plan that should have been put in place before should be followed to prevent any losses from occurring. The incident management plan helps companies to deal with cases of hacking and cyber terrorism by defining the procedure to be taken in responding to the incident as well as the possible solutions in case of an attack (Embar-Seddon, 2002). It shows in a hierarchical order who is responsible for handling each duty so as to control the effects of the incident. This is the plan that iPremier need to come up with so as to be able to deal with such threats in the future.

Apart from this, better back up for possibility of any lost data should be put in place. Joanne notes that the binder is outdated and that the firewall which had been targeted by the attackers needs to be upgraded.

References.

Austin, R. D. (2001). *The iPrimier (A): Denial of Service Attack.* Harvard, MA: Harvard Business Publishing.

Embar-Seddon, A. (2002). Cyberterrorism: Are we under seige? *American Behavioral Scientist* 45(6)