**How well did the iPremier Company perform during the 75-minute attack?**

In my opinion, the iPremier Company preformed quite poorly during the 75-minute attack. The recounting of the events shows negligence towards securing their customers personable identifiable information. They not only didn’t have an emergency plan, but their business continuity plan that may address situations like this was not kept up to date with relevant contact information. So, immediately at the start of the attack the company is starting on a poor foundation to respond adequately. Another point of emphasis is that they relied upon QData for the entire protection of their website’s servers. When the time came and they required physical access to begin a forensic analysis of the situation, they were stalled by being unable to reach someone in power. Any time spent wasted during an attack like this could be critical, which is why iPremier should have migrated to server providers who allowed access to server consoles through the internet instead of only on physical location.

Since iPremier is a publicly traded company, time had to be spent thinking about the public relations of the attack and the damage it could do to its stock price, which is understandable. Ripley was able to analyze where the traffic was coming from that was causing their website to fail, but she relied upon permission from the Qdata staff before shutting the traffic down. In situations like these, there should be full autonomy those in charge to make the decisions needed to control the situation. Shortly after attempting to shut down traffic, which caused more zombies, the attack suddenly stopped. If not for the mysterious end to the attack, who knows how much longer the situation could have lasted given the conditions. This entire attack highlights the importance of crisis planning, and something that every company should routinely cover to ensure effective management when the time comes. This company was left quite unprepared for being publicly traded and put the shareholders at risk with their negligence.

Week 7: iPremier Company, post hoc actions

No unread replies.No replies.

***Note that there will be no new postings on Wednesday this week in recognition that you have exam preparation to complete.***

Based on the iPremier Company case in your readings for this week and your understanding of Information Security Management to this point in the course, respond to the following questions:

In the aftermath of the iPremier attack, what actions would you recommend should be taken

* immediately?
* soon, but not immediately?

Explain what basis you used to distinguish between the immediacy needed for these actions

In the aftermath of the iPremier DDOS attack, the actions that should have been taken immediately are:

* Instruct Joanne to acquire all digital logs of traffic from Qdata for authorities to conduct a thorough forensic analysis.
* Instruct Stewart to notify the senior board members of an emergency meeting regarding the attack, and the plan going forward
* Keep the website running, and continue conducting business as usual
* Implement the proper firewall protections
* Reset any passwords for those who have access to critical network infrastructure

My thinking here is that since the company is publicly traded, the amount of damage done from a complete shut down is a non-starter. However, it’s not to say there won’t be precautions taken in the future but the respect for the shareholders must be considered here. Customer data is at the top of the list as well, but what was known from the attack immediately was that it was DDOS in nature and the intrusion was only through the means of SYN flooding. Which is why instructing Joanne to collect all traffic logs and important data for the authorities to provide digital forensics later should be done immediately as well. To keep the website running but give some assurance that there is no malicious elevated user access, I recommend resetting the passwords of anyone who can control the networks infrastructure.

The actions that should be taken soon, but not immediately are:

* Write and release a press statement to the public about the attack incident
* Send a company wide email, and to customers to change all passwords
* Rework their business continuity plan, and disaster recovery plans
* Perform digital forensics to confirm if Personable identifiable information was stolen

My thought process for these actions taken place soon is that they fall further down the line of importance. The public deserves a right to know what happened, but only when the correct information has been acquired about the situation. It makes no sense to drive the stock into a panic with false information. Resetting passwords is a way to ensure there is no malicious actors with no possible continued access. The business continuity plan was out of date and needs to be brought to modern standards to address situations like the attack that occurred. Leaving management without a written, well though emergency plan is not acceptable for a publicly traded company.