NAME : SIRI S

SRN : PES1UG19CS485

1. According to me, the company's performance was mediocre. The people in charge were more concerned about the company's PR than about the adversaries of the attack that they were facing. There was misguided communication between the hierarchy and employees, things were all over the place. Absolutely no protocols were being followed which lost a lot of time. The emergency measures were outdated as was everything else related to the system security. The entirety of the seventy five minutes was spent on calling each other instead of taking any action or pulling the plugs.

If I was Bob Turley, I would've immediately gotten all the key personnel up to speed. Instead of enjoying my breakfast, I would've been making calls to the higher authorities and convincing them that pulling the plug is the only way out. I would've contacted the data centre quicker as that was the only clue we had which could've helped us stop the attack.

2. As already stated in the previous answer, the company had a clear lack of communication and emergency procedures. Some of the key employees had no idea of its existence or the contents, being outdated also certainly did not help. There was an absolute lack of professionalism and knowledge about the subject as they did not know whether the customers crucial information has been vandalised or not.

New, updated operating procedures would've definitely made a difference. A better and reliable data centre should've been hired, based on quality and merit and not on goodwills. They should've contacted the police when things got out of hand and no one knew how to stop the breach.

3. A new system should be formed which has all the procedures in an up to date fashion making them better handled for any future attacks. Clear communication lines must be established between employees and higher-ups and between the company and third party data centers in order to prevent future unprecedented attacks.

A new backend along with a new website that has better and safer security measures established within it would prepare the company. As the company ages, the attack will be washed away.

4. First and foremost, I would be worried about the data breach that could've affected the customers, hence track them down and know what and who has been affected. Also worry in a business point of view, try to minimise the dip in the value of company shares which would've taken a hit. Try to guarantee customers with future endeavours and gain their trust. Worry about the aftermath of the security breach, if any system was still under threat or if the hackers were still active. Appointing a specific security detail or a third party security service to monitor the firewall and the conditions extensively over a long period of time would do the company good in a long term perspective.