Managerial finance issues

Finance

On August 15, 2012, Saudi Aramco (“ Aramco”) experienced what has come to be described as the most destructive act of computer sabotage on a corporate entity to date (Kennedy, 2012; Arthur, 2012). The impact of this cyber attack becomes clearer when you analyze the role of the company in global energy security given that Aramco is arguably the largest oil company in the world.

The magnitude of the destruction wrecked by the computer virus unleashed on the company on that fateful morning on August 15 has kept the corporation in the international limelight for four months now and become a reference point for governments and corporate entities around the world. This attack has no doubt reignited debate about the threat of cyber attacks at the highest corporate and government level worldwide (Fisher, 2012).

Following the attack on Aramco, the international news media largely angled on the political intrigues surrounding the probable cause of the attack, the probable reasons as to why it was orchestrated and who may have been responsible for this heinous act. Security experts on the other hand zeroed in on analyzing the type of virus that was unleashed on Aramco in a bid to crack its code and hopefully find out where it originated from.

Multiple hacker groups claimedresponsibilityfor the attack amid claims that it could have been an inside job (Leyden, 2012). Consequently, little attention has been given to the managerialfinanceimplications of this sabotage primarily because the issue has broadly been approached from a security perspective. However, the attacks had a greater corporation-wide effect over

and above the security aspect that has dominated the headlines (Roberts, 2012). On August 26, 2012, Aramco’s president and CEO Khalid A.

Al-Falih announced that the threat had been contained and went on to point out that the real intention of the hackers was to shut down the company’s production but they did not succeed because Aramco’s production facilities were running as smoothly as ever (Roberts, 2012). Roberts (2012) p 1 however suggests that the company’s management left out some important information regarding the attacks. To begin with, the al-Shamoon virus that infected Aramco’s corporate personal computers (PCs) wiped out enormous amounts of drilling and production data.

The virus affected about 30, 000 PCs and altered their hard disks in such a way that data contained in the hard disks could not be recovered. Secondly, since the hackers chose to attack during a holiday, it is likely that enormous amounts of drilling and production data may not have been backed up and was therefore lost completely (Leyden, 2012). The major objective of thiscase studywill be to ascertain the effects of cyber attacks on a company with Saudi Aramco as the primary case reference due to the increase of cyber attacks on energy infrastructure in recent years.

The study will mainly focus on managerial finance-related issues arising from computer sabotage as opposed to the security angle that has been the dominant perspective with which cyber attacks are viewed. The reason for this approach is because the damages caused to corporate networks by hackers ultimately result in financial losses and therefore they are not just about security. In addition to this, cyber attacks is an ever-present threat

and a company can never consider its securityenvironmentto be so secure that it eliminates all likelihood of a successful hacker-instigated computer sabotage.