Case 1 – Equifax

From Rithu Anand Krishnan and Johann Thomas

**Question 1:** In the year before the breach, Equifax did not adhere to almost every single principle of the NACD framework. At first, it seemed like Equifax wanted to emphasize cybersecurity as they “invested millions in cybersecurity measures” (pg 2) but in reality, Equifax ignored most of their key issues. Equifax’s Global Threat and Vulnerability Management team (GVMT) was responsible for tracking down threats and notifying “relevant personnel across the company about such threats through emails and monthly meetings” (pg 3). However, when GVMT notified several people across the company about the Apache Struts vulnerability that led to the breach, they were ignored. Managers and executives did not attend these meetings as they were not considered required, which suggests that cybersecurity was not taken seriously enterprise-wide as outlined in the NACD Framework. Equifax did not adhere to the first principle as they did not treat this issue as an enterprise-wide risk. They seem to adhere to principle two as they split up security responsibilities in two different chains of command, one of them relating to legal issues and the Chief Legal Officer was at the head of this team. For principle three, Equifax did seem to bring in outside help such as hiring Deloitte to perform a cybersecurity audit although Equifax seemed to ignore their recommendations. Furthermore, several other companies warned of a security breach at Equifax, but nothing was done. For principle four, Equifax did seem to adequately staff and budget for cybersecurity as they spent “ around one percent of its operating revenue on cybersecurity each year between 2014 and 2017” (pg 2), and according to their website, their operating revenue was 2.4 billion in 2014 and increased every year after meaning they spent tens of millions on cybersecurity. For principle five, it seems clear that the board was not discussing specific IT issues and left it up to the security department as evidenced by Smith and Payne’s contrasting congressional testimonies.

**Question 2:** Now coming to the year after the breach, the board members seem to be more proactive regarding cybersecurity. They have better understanding of the company's state in cybersecurity, thereby satisfying the control environment component of the COSO framework. They opened up a dedicated website, www.equifaxsecurity2017.com, to help consumers get more details regarding the breach. To follow the monitoring activities component of the COSO framework, they formed a special committee of members responsible for various operations. This committee was responsible for monitoring company-wide risks and not just one particular team, and they were expected to meet with the board members frequently. However, the exact frequency of the meeting was not mentioned in the case study. The responsibilities included revising the company's cybersecurity policy, keeping it up to date, and ensuring that any future breach information is shot up to senior board members. One major step towards Information and Communication was included, where the committee would actively identify risks associated with new product development. This involved diving into deeper details, such as placing the potential issues and threats occasioned by new technologies, especially disruptive technologies. Thereby planning for the future to avoid any discrepancies. Disaster recovery and business continuity were newly added to the list of things monitored by the special committee. Significant steps towards enhancing risk assessment involving appointing an advisory council with various stakeholders and data security experts were created. This council would advise the company on how to adhere to current public policies. To conclude, the CEO, Smith, mentions that the goal was not to fix the problem and move on but to confront cybersecurity risks and treat it as a daily fight. They plan to keep investing in data security moving forward. It is unfortunate that it took a major breach for the company to take such an active part in data security. Still, it is good to see that they are making constant efforts to enhance their cybersecurity.