Business fraud: educational credit management corp flashcard

Educational Credit Management Corp – ECMC, a student loan guarantee agency based off of Minnesota, announced on March 2010 that there was a security breach in their establishment. Student loan borrowers had their personal information (names, social security numbers, addresses, and dates of birth at a minimum) stolen off of the premises via ??? portable media???. In the article, Data Theft Hits 3. 3 Million Borrowers, Pilon noted that this is believed to be the largest data breach of its kind and ??? could affect as many as 5% of all federal student-loan borrowers??? (Para. 1).

As a precaution, ECMC made arrangements with Experian, the credit protection agency, to provide credit monitoring services to borrowers affected by the data breach. In addition to the free credit monitoring services, borrowers will also be given identity theft insurance coverage (Karnowski, 2010, para. 5). There are several types of security controls to prevent systems and/or information breach. The three controls that were apparently absent from ECMC headquarters were: Authentication controls, physical access controls and training controls.

According to the text, Accounting Information Systems, Romney (2009) distinguishes these as Preventative Controls (pp. 259)ECMC was very careful in giving details about the data breach, including if the perpetrator was known, so assumptions are necessary in identifying the control issues that were compromised in this case. According to Romney, authentication controls are those that focus on verifying the identity of the person attempting to access the system (pp. 259). It is possible that ECMC failed to require authentication controls from their employees. If employees were

required to have ID badges or passwords to gain access to content sensitive areas perhaps the breach wouldn??? t have happened.

Although it is unknown who the perpetrator was, it is possible that the portable media device containing the borrower??? s personal information was stolen by an outsider who was able to gain access because of the lack of authentication controls. Training is also a preventative measure for data breaches. Employees should be properly trained to understand and follow the company??? s security policies. According to Romney, training ??? is especially needed to educate employees about social engineering attacks, which use deception to obtain unauthorized access to information resources??? (pp.

261). Proper training of employees could have prevented the breach as well. Assuming that an outsider was the thief, I believe it would have been obvious that he/she was not wearing an ID badge or would have been aware of piggybacking, for example (pp. 261). Lastly, physical access controls are those that refrain entry into an area that may contain sensitive information.

According to the text, this control ??? is essential to achieve any degree of information security???. There are a wide range of potential threats that an intruder that is left unsupervised can cause an organization such as copying files with a portable device or as daring as stealing the computer itself (Romney, 2009, pp. 262). Physical access controls had to have been lacking at ECMC. As Romney states, ??? physical access control begins with entry points to the building itself??? so assuming the data was taken by an

outsider, if physical access controls would have been placed the breach would have been prevented (pp. 262).

After researching the situation at ECMC, I failed to locate details about the perpetrator. It was revealed that they notified law enforcement immediately and made the news public shortly after that. However it is unknown whether the breach was caused by an employee. Now let us ask ourselves: If the crime would have been caused by a member of management or a professional would they have made the news public? It is a possibility that companies hesitate to prosecute white-collar criminals because of the negative publicity that it may give the company. The idea of ending up in the news in a bad light could possibly scare away possible investors and/or clients. The problem with not prosecuting white-collar criminals is the possible message given to other employees and the public in general.

This might lead others to believe that it is ok or that there will be no consequences if caught. Employee morale might also suffer. Law enforcement officials can encourage the prosecution of white-collar criminals by taking every case, no matter how small, seriously. There should be lectures on the possibility and commonality of fraud and how to prevent and recognize the signs of it.

They should push for companies to comply with their internal control systems and to train employees correctly (Romney, 2009, pp. 188-189)Referenceshttp://www. nbcnews. com/id/36060713/ns/technology_and_science-security