Memorandum

To: Dr. Coyne, Assistant Professor School of Accountancy

From: James Jensen, University of Memphis Student

Date: 28 NOV 2015

Subject: Accounting Architecture Changes

Dr. Coyne,

The Accounting Architecture relies heavily on the ability to safely store data. Security breaches are a constant threat to the maintenance of data storage. The following changes were made to the Accounting Architecture to emphasize the accountant’s role in data security.

**Accounting Architecture Edit:**

“Due to the level of high importance of financial information, accountants must maintain awareness and be proactive in the area of data security. It is not enough to understand encryption and permission techniques. Accountants must work with their information technology counterparts to be proactive in combating security threats. Due to the role of big data in entity operations, the accountant’s role is elevated. Information technology can only provide the highest level of data security if they know the importance of the data, who would benefit from hacking it, and why it needs to be secured. This is where the accountant is needed in data security. Because the sheer volume of big data is so vast, not all data breeches may be detected or prevented. The accountant’s role is to prioritize the most important data and work with information technology to evolve to threats on a continuous basis.”

This is an elaboration of what was in the original Accounting Architecture. My aim here was to complement the paper by emphasizing what the accountant’s role is in data security. It is not enough to be reactive to threats, accountants and IT specialist must be proactively vigilant. The role is to bridge the gap between operators (accountants) and programmers (IT specialist). IT specialists do not have an advanced knowledge of accounting, therefore it is our responsibility to reach to IT so they know what is important to us and hackers alike. Basically, it comes down to prioritizing what is most important from what is not. Prioritization is fundamentally important to security if we are going to protect data from tomorrow’s security threats.