

Research Statement

Ahmed Al Zaidy

Academic Institutions, private schools, or public both share the same importance of delivering knowledge to students, as it is required schools need to hold student information, like social security numbers, legal names, real physical address, etc. Due to this data collection, academic institution becomes a good target for hackers to get access to this information, that can be used in criminal activity such as Identify theft. Academic Institutions employees need to understand the risk of being employed by academic institution; they can become the next target in line.

Per John Hitt the president of University of Central Florida about the security breach that accrued the begging of January, 2016 to the system of the university where the breach affected per Hitt 63,000 student where the social security numbers has been accessed by the hacker, but not credit card information, and other information (Hitt, 2016).

Academic Institutions need to be in compliance with federal act like the Family Educational Rights and Privacy Act (FERPA) which require that student information need to be confidential, ensuring systems and data security one of the essential of FERPA.

Information confidentiality one of the tenets of information systems security, which indicate who had access to the information, like employee and staff, anyone who do not have authorization to access the information will consider a violation to the tenets of information system security, and a violation to the FERPA. Per David Kim and Michael Solomon (2014) Cyberspace add new threats to individuals and organization (Kim & Solomon, 2014, p. 460), information systems face threats from both sources human made and natural threats (Kim & Solomon, 2014). The importance of understanding threats so huge for the organization to prepare for a plan that held to respond to these threats or to overcome on it and secure the system. My research addressing the topic of information confidentiality and cyber security in the academic intuitions, the study targeting the training that the employee gets when being hired in the current position, as well as, the trainings they get around the year, the notification about attacks attempts and warning from the IT security administrator about a potential attempts or attack. The type of information that the user conduct in terms of the information sensitivities.

References

- Hitt, J. C. (2016, February 4). *Intrusion into UCF Network Involves Personal Data*. Retrieved from University of Central Florida: <https://www.ucf.edu/datasecurity/>
- Kim, D., & Solomon, M. G. (2014). *Fundamentals of Information Systems Security*. Burlington, MA: Jones & Bartlett Learning .