Name: Benjamin Matthew Linam

Course Number: EGS 4032

Semester: Fall 2017

Case Study Report # 3

I certify that this assignment is the result of my own efforts.

Signature	Date: October 19, 2017
UWF Student e-mail:	bml42@students.uwf.edu
e-mail:	bmlinam1@gmail.com

Step 1: Determine the facts in the situation – obtain all of the unbiased facts possible

There is a small library that desires to store lists of book checkouts, due dates, as well as other records in a relatively more secure medium such as a computer software system. Since their current records are stored in a physical file drawer in the library, there is the possibility that someone could steal the records while they are not being monitored. The problem with electronic records; however, is that they could be accessible to someone who is knowledgeable of the system but not authorized to access it.

Step 2: Define the Stakeholders - those with a vested interest in the outcome

The stakeholders are the patrons of the library whose personal information is stored in the physical records and the librarians in charge of making the decision on whether to store the information on a computer system or retain the physical records only. If the library decides to bring in a computer specialist who is able to store the records electronically, the specialist would also be a stakeholder.

Step 3: Assess the motivations of the Stakeholders - using effective communication techniques and personality assessment

The librarians in charge of the records are concerned with the current safety of patrons' private records. If someone were to steal the records, the blame would fall on them for not properly securing them. That would also lead to bad publicity for the library leading to fewer people coming to check out books. The software specialist is concerned with making money from the library but first and foremost, should be concerned with the security of private records and helping the library to keep that information secure.

Step 4: Formulate alternative solutions - based on most complete information available, using basic ethical core values as guide

There are not alternatives for this situation, but degrees of how concerned the specialist is with keeping the records secure. The specialist should focus on the safety of the patrons' private records as well as understand that the system should be kept from access by anyone who should not have access. The specialist could also care very little for the security of the records and do the job while leaving security at a minimum and charging the library the most possible for the job.

Step 5: Evaluate proposed alternatives - short-list ethical solutions only; may be a potential choice between/among two or more totally ethical solutions

The most ethical decision would be for the specialist to put as much effort possible towards securing the patrons' records by both training an employee as operator of the system and securing access as tightly as possible. As the specialist would most likely not always be available for the editing of records, he or she and the library would need to choose an employee for the specialist to teach how to operate the system. The employee would need to undergo security training and have a well-known history of trustworthiness to make sure the records would be as secure as possible. In current day, information breaches of online systems are becoming more common, so it is much more important to do everything to secure system access to safeguard records. If the specialist were not to care very much about the security of the library by putting the least amount of work in on the project and charging the library as much as possible, then he would be going against the first fundamental canon of the NSPE Code of Ethics by putting the security of the public at risk by not securing their personal information.

Step 6: Seek additional assistance, as appropriate - engineering codes of ethics, previous cases, peers, and reliance on personal experience, prayer

Since the first fundamental canon of the NSPE Code of Ethics is to "[h]old paramount the safety, health, and welfare of the public," the least ethical solution would be for the specialist to put the least amount of care into designing and implementing security for the software system.

Step 7: Select the best course of action - that which satisfies the highest core ethical values

The best solution for the specialist would be for he or she and the library to choose an employee for the specialist to teach how to operate the system and for the specialist to put as much care initially in the setting up of the security for the system.

Step 8: Implement the selected solution - take action as warranted

The specialist has decided to design his own system that would be more secure than using another more widely-known program that could be easily infiltrated. The specialist made sure to implement security features that would allow only people who have proper clearance to change the records. Since the specialist is not physically able to constantly monitor the system, a trustworthy representative from the library was chosen to monitor it. Access to change important records lies solely with the representative, but access to editable records such as due dates and checked out books is available to all the librarians.

Step 9: Monitor and assess the outcome - note how to improve the next time

A week after implementing the new system, a librarian accidently spilled ink into the drawer containing the records, effectively ruining the old records. Thankfully, having the records stored on the system has saved the library from a disaster. There have been no security leaks and at this point, the library has chosen another representative who will also learn use of the system and who will have dual control over the records with the first representative. Due to the system being such a success, the library paid the specialist much more than originally agreed upon. Also, the library recommended the specialist to another library which was having the same problem. The only aspect of the situation that could have been changed was having dual control over the system from the start to maintain a higher level of security.

Appendix

Case 3 (Case 38-5e) Software for a Library

A small library seeks a software system to catalogue its collection and keep records of materials checked out of the library. Currently, the records of who has checked out what, when materials are due, and the like are kept in a file drawer behind the check-out desk. These records are confidential. Patrons are assured that these records are not accessible to anyone other than library personnel. But, of course, drawers can be opened when no one is looking. What assurance is there that the software systems under consideration will provide as much, if not greater, security? Assuming that no one in the library is a software specialist, the library has no alternative but to place its trust in someone who presumably has the requisite expertise. How concerned should that expert be (again, bearing in mind that even the best system is not completely sleuth proof)? Furthermore, what assurance has the library that it is not being oversold or undersold in general? To what extent should software specialists be concerned with determining precisely what the various needs of the library are—and to try to meet those needs rather than offer more than is necessary in order to secure greater profit or less than is needed in order to come in with a lower bid?