**CIS-481: Introduction to Information Security**

**In-Class Exercise #4 - Option B**

**IQ Team: 3**

**Names of team members: Elise Timmons, Samantha Conway, Noah Smith, Trevor Rawleigh**

**Logistics**

1. Get together with other students on your assigned team in person and virtually.
2. Review the two options available and decide on only one to pursue as a team.
3. Discuss and complete this assignment in a collaborative manner. Don’t just assign different problems to each teammate as that defeats the purpose of team-based learning.
4. Choose a scribe to prepare a final document to submit via Blackboard for grading, changing the file name provided to denote the number of your assigned **IQ Team**.

**Problem 1**

Review the *Bank Solutions Disaster Recovery and Business Continuity* teaching case linked below [Camara, S., Crossler, R., Midha, V., & Wallace, L. (2011). Teaching Case: Bank Solutions Disaster Recovery and Business Continuity: A Case Study for Business Students. Journal of Information Systems Education, 22(2), 117-122.]

<http://jise.org/Volume22/n2/JISEv22n2p117.html>

The intent of the case is to give students an opportunity to gain real world experience with a theoretical concept that can be difficult to comprehend fully. At the conclusion of this case, students should possess a greater understanding of the critical decision-making process that goes into analyzing and deciding what risks need to be dealt with as a part of a Disaster Recovery and Business Continuity (DR/BC) team. To accomplish the stated goal of this case, information from a fictional company, Bank Solutions, Inc., is provided. Bank Solutions, Inc. is a provider of item processing services to community banks, savings and loan associations, Internet banks, and small- to mid-size credit unions. As members of the engagement team performing the risk assessment, your team has been given the task of assessing Bank Solutions’ incident handling, business continuity, and disaster recovery strategy.

Each group of students will work as a member of an engagement team in charge of performing the incident handling, DR/BC risk assessment for Bank Solutions. Each group should read the case background and the facts identified in the interviews.

Together as a group, prepare a report of recommendations for correcting each of the identified conditions (thereby addressing the risks) from the assigned subset of facts given to you by your instructor. Prepare to discuss your results in class. You should be ready to explain and elaborate on why you identified each condition and each risk. Highlight the changes you recommend to their IR/DR/BC contingency plans. *(50 points)*

Bank Solutions provides a variety of services to community banks, savings and loan associations, Internet banks, and credit unions. These services include Proof of Deposit Processing, Item Capture, Return and Exception Item Processing, and Customer Statement Rendering.

Due to the sensitive nature of customer financial data, it is of utmost importance that Bank Solutions has an efficient and effective Disaster Recovery/Business Continuity (DR/BC) plan in place. As outlined in the case, the objective of Bank Solutions’ management is to sell the company. In order to be attractive to potential buyers, risks identified must be assessed and either accepted or remedied in a cost-effective manner.

The two primary risks lie in Bank Solutions’ backup process and its lack of documentation. Both pose potential detriment should the company be faced with a security incident in the form of a physical disaster, software attack, or other.

The first risk lies in the organization’s backup procedures. While Bank Solutions has both scheduled daily and incremental backups, one site reported routine failure, event logging lacks access control, and there is a lack of consistency for the storage of backup files. The cause of the backup failure at the single site should be fully investigated and remedied as soon as possible. Also, access controls should be implemented around the event logs to prevent users from potentially erasing actions detrimental to the company. In addition, backup tapes should be stored in a secure, offsite, location consistent across the company. One reported storage method was in a contracted location across the street. This method is secure in the case of a software attack on Bank Solutions but remains vulnerable in the case of a physical disaster or in the case of an attack on the other bank. Another method was storing the backups in a manager’s home. This poses risk should the manager leave the company or become disgruntled with the company and left with access to valuable resources. Instead, all backup files should be directed to the existing hot site and an additional set of backups should be kept in a secure “data center” with limited access on the premise of the central headquarters of Bank Solutions. Ideally, Bank Solutions would transition to a cloud-based backup solution but given the drive to keep IT Security costs low for potential buyers, would not be beneficial at this time.

The second greatest security risk for Bank Solutions lies in its lack of documentation and training in case of a security incident/disaster. While a documented plan is in place, it is not well practiced or distributed to all key participants, including the “hot site”. In order to lower the risk of being unprepared in the event of an incident, Bank Solutions should establish a “Break Glass Group,” of essential personnel who will gain elevated administrator privileges in the event of a disaster, and repeatedly rehearse and sufficiently document their responsibilities. There should also be backup members for the group in case a member leaves the company or is unavailable during the incident. Incidents/Disasters should be ranked by detriment to the company (P1 Incident, P2 Incident, etc.), and portions of the DR/BC Plan should be executed utilizing this direction. The most important factor to mitigating the risk of being unprepared and vulnerable is to practice the plan repeatedly with all key participants and as many different scenarios as possible (“killing” an employee, destruction of various physical sites, etc.) until it is solid and can be executed without hesitation.

In summation, an effective DR/BC Plan is necessary for Bank Solutions to remain functional in the case of a security issue and increase its attractiveness to prospective buyers. The two greatest risks presented in the assessment were issues with backup procedures and a lack of documentation/practice in the case of a security incident. Both can be easily remedied thus considerable lowering the overall detriment to Bank Solutions in the case of an attack.