CIS-481: Introduction to Information Security

InfoSec Chapter Exercise #4 - Option B

Team: Project Team 11
Participants: Sohal Patel, Erika Maglasang, Nathan Moran, Gabriel Rolink, and Tyler Samuelson

Logistics

A. Get together with other students on your assigned team in person and virtually.
B. Review the two options available and decide on only one to pursue as a team.
C. 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.
D. 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 **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 midsize 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)*

Answer:
First Presidential Bank is a major bank and offers a wide range of services. It was the primary provider of item processing services to community banks, savings and loan associations, Internet banks, and small- to midsize credit unions. These services included in clearing and Proof of Deposit (POD) processing, item capture, return and exception item processing, image archive storage and retrieval, and customer statement rendering. Bank Solutions Inc. was established by First Presidential Bank when they realized the potential in item processing systems. By offering this service they can serve financial institutions that want to reduce operating expenses and focus more on growth strategies and other core business functions. Bank Solutions Inc. continued like this for 15 years and served 41 small- to midsize financial institutions in 1988. They hoped to expand their customer base to outside of the Northwestern region, but failed to do so because they could not compete with the item processing services with 'top of the line' software systems. First Presidential Bank saw this as a liability and sold off Bank Solutions Inc. to new management. (Camara S.)

Bank solutions Inc thrived because they made these changes. They now use financial institution core processing system outsourcers. This helps expand the capability of their processing system that can take on more customers and keep the customers data secure. They also introduced a new company culture. The company now works more as a unit than a single entity. "The development of a proprietary, state of the art item processing system that uses state-of-the-art Optical Character Recognition (OCR) technology to achieve character recognition accuracies that were previously unheard of.", (Camara S.) the addition of this will make Bank Solutions favorable for interested buyers.

To combat external threats, the company should get compliance of CMMC, ISO 27001 and GDPR, to ensure better data security standards. Bank Solutions Inc. should focus on how to implement the CIA Triad, to secure the organization's sensitive data from phishing and cyber hacking. To protect the company internally, employees will be required to complete training and incentives should be provided to employees to keep them safe from social engineering' attacks. Moreover, backup files should be ensured so that in case of data phishing an organization wouldn't lose its data. Secondly, the organization shouldn't store all of its data in a single software, but it should be divided in different software's so that in case of an attack, all the data available will not be compromised. As per the given articles, Bank Solutions Inc has defined the type of solution it needs for risk management, incident handling, business continuity and disaster recovery.

The identified risks can be stated as follows:

- Procedures - The procedures in the DRBCP are emergency/crisis response procedures, business recovery procedures, "return to normal" procedures , and various appendices. The DRBCP does not have a Recovery Time Objectives and Recovery Point Objectives identified for each procedure.
    - solution: Create Specific recovery procedures and add them procedures in DRBCP. Each procedure needs to have a recovery time objective and recovery

point objective, so that each procedure has an estimated complete time and an estimated pass-fail criteria.

- Review Mechanisms- The mechanism being used by Bank Solutions have not been properly reviewed before implementation.
    - solution: Review mechanisms should be implemented into the DRBCP. Before implementation, procedural planning must be completed. The DRBCP Template should not only be discussed but other methods from other companies should be applied by conducting research on what the market is using today.
- Processing Facilities - Item processing facilities of a smaller caliber have been neglected
    - solution: Stop the negligence of small caliber item processing facilities by creating customized DRBCP templates for small item processing centers. There should be a new template created for large item processing facilities as well, this template will cater to the need of the large facilities as they have a larger inventory and therefore possess more risk. Small facilities can be checked first because their DRBCP will take less time, and they have less risk if the plan goes wrong.
- Backups - DRBCP is stored on the network. Neither the DRBCPs nor any other documentation outline specific processing responsibilities for backup facilities.
    - solution: DRBCP needs to be stored in a backup file and not on the network to reduce the risk of it being lost or damaged. The plan is available to everyone when it is stored on the network, but many of the employees that need to see it are unaware of its location. The DRBCP will be moved to a place where everyone can see it. The plan will be changed to include specific processing responsibilities for backup facilities
- Storage - At the item processing facilities, the management has been tasked with contracting the off-site storage of backup tapes. At one of the item processing facilities, management has contracted the bank across the street to store its backup tapes in a safety deposit box. At another item processing facility, the night Operations Manager stores the backup tapes in a safe at his home. At a third item processing center, tapes are stored in a shed at the back of the building.
    - solution: It is good that all of the backups are stored in different places but some of the places that they are stored in are less than ideal. Backups being stored in another bank across the street presents the risk of company trade secrets being stored by the bank's competitors. The backup should be stored in a company owned facility. backup tapes should not be stored in managers houses, if that manager quits then the backup will be lost forever. The backup should be stored in the manager’s office instead. Finally, a backup shouldn’t be stored in a shed because it is prone to being lost or broken, the backup should be stored in a filing cabinet or on a secure computer.

- Security Controls - Neither the DRBCP nor any other policy, standard, guideline, or procedure addresses security incident handling steps, including escalation points of contact and procedures for preserving the forensic qualities of logical evidence.
    - solution: Security controls need to be implemented; these controls will state policies, standards and guidelines that will be used in the case of a security breach. A detailed plan that is capable of addressing all possible security issues needs to be created. If a plan exists then when a security issue happens then individuals will know how to act at a moment's notice.
- Planning- Full backups of critical data files, software programs, and configurations are performed once a week and incremental backups are performed on a daily basis Monday through Friday.
    - solution: If plans are missing, the task should be divided amongst all the team, human efficiency matters more than that of machine learning. All the organizational vulnerabilities, threats/ attacks and problems should be discussed and troubleshooted by mutual meetings; all the suggestions should be overlooked, and the best should be implemented across the organization.
- Testing - Testing of Bank Solutions Inc. data centers have not been conducted since 2007.
    - solution: Bank solutions data centers need to be regularly tested preferably on three-month intervals to keep up to date.
- Documentation - A review of the network diagram and conversations with the Network Architect reveal that redundancies have been implemented at the network perimeter (e.g., routers, firewalls, IDS, load balancers, etc.).
    - solution: Rather than just providing strategies Bank Solutions should also focus on how it can cope with organization in order to reach sustainable advantage and operational excellence. Redundancies should be reduced once these organizational strategies have been implemented.
- Training - Critical plan participants have not been trained to use the plan.
    - solution: Train critical plan participants. Teach them how to handle the DRBCP. They should be taught using the mentoring system that has already been implemented in Bank Solutions Inc.

Work Cited

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.