Term Project; Milestone One

Name

Professor

Date

 **Milestone One**

**Project Abstract**

The Cidian Bank embraced full automation early enough when several banks restricted their vital operations to the traditional filing system. The paper analyses the security architecture of the bank, beginning with its design and implementation, utilizing the most recent available security technologies. Banks transfer a lot of data over the internet. These data must be secured in all manner of ways to avoid breaches and unprecedented compromises. Data encryption is one of the trusted technologies widely used to secure data, especially in bank information systems that are directly connected to the internet but must interact with customers and protect sensitive technologies. The study issues a discussion on the bank's system security architecture solution, where the guiding principle is that the enterprise system security solution design strategies are that the entire system security is anchored on the security of every individual machine that forms part of the system.

**Introduction**

It has become an obvious experience for various corporate organizations to have their information architecture designed, developed, and eventually installed based on tactical strategies befitting the organization's line of service. A need level is usually assessed then followed by a customized specification that leads to the development of a solution believed to be up to the situation. The process of developing a security architecture of an organization occasionally suffers from the lack of an opportunity to take note of a strategic dimension. As such, the outcome revolves around the development of a mixture of technical solutions on an ad hoc basis where each solution is designed and specified independently without guaranteeing compatibility and interoperability.

**The Business Type Selected**

In this study, we depict the security architecture solution of a bank and draw various inferences that appreciate whatever efforts that have been made, the nature of threat out there, and where to put effort going forward. Banks are highly dependent on their information systems to carry out their activities. However, this dependence has come an increase in information system attacks. Any activity that may lead to the compromise of confidentiality, integrity, and availability either through the loss of information, inaccuracy of the information, or unauthorized access can have an adverse effect on the business (Han & Noah, 2017). This research depicts the information system solution architecture by way of looking at the following; gaps identified in ensuring information infrastructure protection; the frameworks developed by various experts to help in developing security architecture for the protection of the organization's information infrastructure. Information security is very important, especially with the introduction of internet banking in a banking environment, because of the increase in accessibility and exposure to malicious attacks. The main aim of this study is to develop a multi-tiered security architecture that will be used to protect against malicious attacks on a bank's network, web application platform, and database systems.

**A Brief Overview of the Business**

Banks are constantly under surveillance of attackers who, at any given moment, can carry out attacks on the information systems used to coordinate all banking operations virtually. The banking business model is largely premised on the trust that potential depositors have on the systems and modalities that given banking enterprises have put in place (Dorri et al. 2017). In the event that the enterprise suffers from challenges such as data theft, information system compromise, or any sort of issue that can potentially affect the normal operations of the bank, the resultant loss can lead to industry exit or business closure. It should be noted that the threats facing the banks can emanate from external sources as well as the internal ones. It is the constant presence of such threats that inform the decision to invest in system security solutions that do offer not only the needed protection from the potential external attacks but also the internal ones which are more difficult to deal with than anything else heavily.

In order to create a comprehensive line of reasoning while responding to the requirements of the term project, we use the Cidian Bank based in New York City to discuss the security architecture solution insightfully. The bank is headquartered in New York with slightly over two hundred employees. Additionally, the bank has a total of ten branches spread across various states in the country, meaning each branch has between 14-20 employees in each branch.

**The Goals and Approach to the Project**

The guiding principle of enterprise system security solution design strategies is that the entire system security is anchored on the security of every individual machine that forms part of the system. The idea here is that only a single machine in the system can be of certain vulnerability, thereby enabling attacks into the system as a whole. The goal of this study is to present the security architecture solution of an enterprise in the banking sector. We will hence identify various ways in which all devices in the enterprise security system can be configured using various strategies with the aim of being guaranteeing high availability as well as physical security.

References

Dorri, A., Steger, M., Kanhere, S. S., & Jurdak, R. (2017). Blockchain: A distributed solution to automotive security and privacy. IEEE Communications Magazine, 55(12), 119-125.

Han, S. R., & Noah, M. (2017). Android Mobile Guardian System Security Architecture for Handset and Data Security. Bonfring International Journal of Industrial Engineering and Management Science, 7(1), 25-28.