Thomas Oshoko

Strayer University

Project Deliverable 5 Infrastructure and Security

CIS499

DR Reddy Urimindi

November 25, 2019

Project Deliverable 5 – Infrastructure and Security

**Abstract**

The infrastructure that encompasses network security and solution is a significant consideration for my firm. Given that my company would be expanding from first to the third floor shortly, as the CIO, I am responsible for the creation of the structure as well as security protocols. In this regard, I have been tasked with developing a network that is steady, redundant, as well as scalable. Equally, in this design, speed remains an essential element for consideration in this network. Assumptions are also drawn about the system use in association to network services as well as assets. All the established criteria set at the beginning are also followed in designing this plan. Consequently, the network design would support the organizational needs, operations, and hence, a pictorial view of workstations, bridges, gateways, as well as access points are used. Access paths for the internet access are also shown. Furthermore, the security of the network is also at the forefront of this design since protecting the organization’s data is a fundamental consideration.

**Introduction**

It is without a doubt that design and security go together in network creation and set up. For my organization, as already stated above, it is expanding and looks forward to offering its customers diverse ways of getting the most from its services and products. The company also wants to establish additional means of getting information from its customers for data analytics, especially in attempts to offer more personalized services and products. As such, there is a need to ensure that the network design does not only handle customers’ demand but also it is secure from any external or internal risk. As well, the relationship between network design and security and how they relate to the business’ needs is a significant consideration. Also, this paper looks at ways in which the logical and physical topology layout has to be presented in addition to how the correct placement of the network’s tools would assist in securing the company’s infrastructure.

**Infrastructure and Security**

It is supreme to note that information is a resource for any given company. Thus, such information is what makes firms like mine profitable and more meaningful to a diversity of people. My firm provide information to customers in an organized and presented manner, and therefore, making the organization the number of priorities for customers in the industry. Also, depending on how data is gotten and used, it could mean a lot to different users. Therefore, the company’s capacities to stock, present, manage, evaluate, and guard the collected information will help to draw more customers to its services. Moreover, the types of information that the company possesses also have meaningful value for different customers and what clients are particularly looking for in such data. While some information could be more substantial in value than others, the overall goal includes data reliability, security, as well as privacy.

Data has many vital applications within the business. It is, therefore, critical to remember that this form of data can be highly valuable to the enterprise’s data security experts as well. Thus, what should be done in efforts to put down the groundwork and foundation for security is to enhance the level of protection against inside as well as outside threats. In this sense, the company’s security team has to comprehend the infrastructure variations among the traditional security techniques, especially those that leverage on big data. However, in today’s business world, it is common to find a mix of different security tools that report on diverse elements of security. For instance, security monitoring, logging, provisioning, as well as risk analysis tools may be used to identify any security threats to the company’s systems. In attempts to create the kind of infrastructure that supports the company’s data environment, a secure, as well as high-speed network, is important in collecting several security system information feeds that are necessary for maintaining the required environment. Furthermore, due to the distributed and sometimes virtualized nature of the infrastructure, the organization would need to look at virtualized networks as its underlying communication infrastructure. Similarly, using tools such as VLANs between information centers as well as virtual instruments as the system is important in carrying data.

In efforts to ensure the security of data, the warehouse is also necessary and a top consideration in the security ecosystem. Hence, it has to be integrated with other existing security tools in addition to processes. Once this integration work with security data and event management systems is complete, a program has to be designed to assist in decoupling the SIEM tools to feed right into the data warehouse. Also, given that data often operates in new and different ecosystems, a tailored training program has to be designed for the organization’s security office personnel. Such a program has to focus on the newly designed analysis as well as remediation systems, which the security data warehouse undertakes to flag and report network traffics and other activities. Moreover, the real operation of a data environment must have normalized functions and recommended changes. Besides, its access must also be east to realize.

**Rational for Logical/Physical Topographical Layout**

It is important to note that the network, currently and for some time, is straightforward and is like that of a small business. Likewise, the logical and physical layouts consist of mail servers, firewalls, as well as databases, among others. All these components play an important part as they form the backbone of the company’s information-collection channel. In the planned case, the firm is moving from the first floor to the third floor. In attempts to avert any form of trouble, the layout would fundamentally remain the same. Also, on every level, the physical and logical arrangement would remain the same. It is only the hub connection that will be gathered and tied within a specific place. Furthermore, for Wi-Fi associated tools, routers that have heavy-loading abilities would be utilized. What is more, the whole server would be moved to the third floor to prevent unauthorized persons from accessing it.

**Current –Planned**

Adm. Hub

Data server

Mail server

Web server

File server

Router

Switch

Hub

Hub

Hub

**Planned-Physical**

Access

Threat detection

Secure mobility

Network protection

Internet router

Cisco ASA

Distribution

Internet

Internet distribution switch

Core

Edge protection

HDLC

Email server

Email security

Web server

Improved availability as well as resiliency

Internet access

Public services