Communication Network

[Author Name(s), First M. Last, Omit Titles and Degrees]

[Institutional Affiliation(s)]

Author Note

[Include any grant/funding information and a complete correspondence address.]

Communication Network

In this era of science and technology, the development of a safe and secure networking architecture is a very important issue. Multinational companies invest millions of dollars in the safe and secure implementation of our network. Complete departments are detailed with the responsibility of keeping the assets i.e. data and resources of the company safe from people with malicious intent. It is also, very well understood that companies only function when an efficient medium of communication exists between various arms of the organization to provide a streamlined workflow. This paper will discuss in detail, the various factors that play a part in the development of the network infrastructure in our company and how as a CIO, I am going to handle it.

**Network Architecture**

For the proper and efficient functioning of any organization, a completely reliable networking architecture is required. In our organization, we plan on implementing a tiered architecture in which administrative controls are granted to the administrators of the respective departments and the workers have user-level permissions.

**Three tier network model**

Cisco’s three-tier network model is the one that is implemented in the organization, the three layers being the core layer, distributive layer and the access layer. All of these layers consists of routers and switches which are configured so that reliable communication throughout the organization can be ensured.

**Core Layer.**

The core layer is the top most layer of the networking architecture and it is the one with the highest quality of routers and is thus considered as the backbone of the network. In monetary terms, the routers of the core layer are the most expensive. The main purpose of a core layer router is to merge and make reliable communication possible between geographically separated networks. This layer ensures that in terms of a distributed organizational infrastructure, important information can be shared between the computers with the maximum speed and efficiency. In technical terms, the packet switching that occurs at the routers of the core layer is between separate networks.

**Distribution layer**

The central layer of the networking infrastructure is known as the distribution layer. It is placed between the access and the core layers. The main functionality that this layer provides is a control to the administrators. The implementation of access lists and different sorts of permission filters limit the access of individuals required and grant access to another set of individuals. High-level policies are implemented at this layer and the general policy guidelines can be seen as pat of this layer. Mostly, type 3 switches are used as the main type of hardware for this layer. This layer ensures the reliability and efficiency of communication between the administrator systems of a certain network. The proper routing of packets between subnets and virtual LANS are also done in this layer at our enterprise.

**Access Layer**

The functional level of communication for example the access that a system can have on the printer is controlled at this layer. Access control lists are implemented at this layer and the main purpose of this layer of the architecture is to ensure proper exchange of packets between devices.

**Benefits of the mentioned architecture**

One of the main benefits of this architecture is its overall complete nature. It caters to a distributive organization as well as an integrated one. The level of control over the organization that can be exhibited using this architecture also makes it one of the best networking architectures out there. Some more benefits are detailed below.

1. After implementation, it has been seen that this orientation of architecture yields high performing networks.
2. In cases of network trouble, this architecture helps in isolating the problem from the rest of the infrastructure very well.
3. An easier application of access control lists and filters is seen using this architecture thus increasing the safety index of the organization.
4. Another aspect in which the architecture helps us is its scalability. Future growth can be very easily accommodated within the framework of the architecture.
5. In technical terms, the architecture provides better redundancy which means that if we need to reach a certain destination, a a number of paths can be used for this purpose.

**Security Policy**

The security policy of an organization defined the sets of rules and practices that are adopted and employed by the organization in order to keep its data and resources safe. Although, a three-tiered architecture has its fair share of benefits, it also has some security drawbacks. Since there is a difference between every two networks, the security challenges that may arise due to these issues will, obviously also differ. This portion of the document will discuss some of the generic security issues that arise in three-tiered systems and how they will be solved. A number of security options in its new network security software by the name of Oracle8i that are designed primarily for the security requirements of three-tiered architectures. We will implement the same software for the security of our networking architecture. Some of its features are given below.

**Oracle Call Interface lightweight user session**

One of the most useful security features of the software is Oracle8i is the OCI lightweight user session. In essence, OCI is Oracle’s C-language based client API which can be leveraged to access Oracle databases. This feature was initially launched in Oracle8 and this was used to allow a database client to be accessed, within a single database and a number of lightweight user, sessions could be created to access the database using several scripts (Kilday, 2016).

With the launch of the latest version of Oracle is known as Oracle8i, the database can be accessed by the middle tier server through Oracle Call Interface by the establishment of a lightweight user session for that particular user. After the authentication of the middle tier server with the database, the process of further validating the user can be skipped as a trusted certificate can be granted on the first arrival thus streamlining the process of accessing the database.

**SSL**

The SSL protocol has been implemented for the safe and secure transfer of data between database clients and the database. The process of encryption and exchange is monitored by the SSL protocol. In the security process of three-tiered networking architecture, the SSL configuration for a database means that the exchange of data between the distribution layer and the database can be made secure by encryption using SSL. The protocol has become very popular and has become very widely used in modern networking nowadays. The implementation of Oracle8i has been developed to support the three modes of authentication which are usually seen as standard include server-only authentication, anonymity (Diffie-Hellman), and mutual client-server authentication. One of the major problems that arise in a three-tier system is that of protected data exchange. This problem is addressed head-on with SSL. SSL provides strong and standard-based encryption procedures such that breaking it would take computational capacity which is not commonly found. One of the main differences between this and any other encryption system is that unlike any password-based authentication, which only has the client to server authentication, SSL can be used to authenticate the authenticate server to the client as well. This can be easily summarized that usually when you access any website that website authenticates you but you do not always have the necessary tools to authenticate the website. SSL provides the functionality for you to authenticate the website as well. The color of the lock at the beginning of the URL indicates the level of SSL authenticity that is available with any website.

**Public Key Infrastructure**

Nowadays, the main authentication technology that is used for the authentication of communication is known as the Public Key Infrastructure. It is generally used for the internet and e-commerce authentication as they require the highest level of security. There are a number of reasons why this might be the case. One of which is the high scalability that is found in the implementation of the public key infrastructure. In public key infrastructure, authentication is based on a user-owned certificate (Austein, 2017) . Before gaining access to any service provided by any particular service, the client authenticates itself and is granted a certificate from that service. After getting the certificate from that particular server, the client is granted access to that service. As mentioned earlier, SSL also provides a feature of certificate-based authentication, thus these two features can work hand in hand.

**Virtual Private Database**

A new standard of security that is introduced in Oracle8i is known as the virtual private database. It has a number of qualities that set it apart from the rest of the bunch. It is an access-controlled, server-enforced with secure application context which is used in enabling multiple customers to have relatively direct access to the data. Within the boundaries of the enterprise, the database results in lower use of resources and lower cost of ownership while deploying applications. This technology enables security to be built at once which means that rather than developing infrastructure, it can be sued to make the application secure with deploying server-based security.

**Critical elements for successful implementation**

With the widespread of information and advancement in Information Management Systems, threats of data theft and cybercrimes have increased. It is believed that there are two kinds of websites, the first kind are those which are hacked/breached and second type of websites are going to be hacked. Management Information systems are very important in this regard as they are used to collect, store, process and share the important data of an organization. As a matter of fact, data is considered as the most important asset of this century so it is very important to implement effective communication network systems with the underlying mechanisms of security to prevent data loss and data theft. There are a number of critical elements for the successful implementation of the communication system for an organization. Some of them are discussed below.

**Security Accountability**

It is the responsibility of the Chief Information Officer (CIO) of a company to identify the responsibilities and roles of the management, key staff, and general users. Enforcement of all the ancillary procedures and policies can be made efficient and effective by making an accountability system for all the three types of categories of users. The task becomes easy if data is divided into different classes including general, internal, confidential and external (Limba et al., 2019). By dividing data into different types, it becomes easy to determine what kind of data should be accessible to what type of users. For sending data out of the organization for any purpose must be endorsed and allowed by the management.

**Network Policies**

To determine safe and secure access management, it is important to make separate dedicated policies for IP address management, Access list, switch and router security procedures, and remote access. Before the implementation of changes, security team and management must check and review all the changes in ACL. This section also includes the requirement of defining and managing intrusion detection system and network access policies of the communication system.

**System Policies:**

System policies are also very critical in determining the compatibility of the infrastructure with respect to different services and processes. So a CIO must ensure that the security configuration of the servers and operating systems are well-defined. The services include firewall policies, anti-virus, messaging, database, intrusion detection system, password management, and account management policies.

**Incident handling and Response.**

In case of any incident or security breach, it should be specified what procedures must be followed in a flow to secure the system and information. Further, in such cases, how the incident must be reported and so that the threat is removed and what personal and department must be consulted immediately under such circumstances.

**Physical security**

Physical security of the infrastructure and other related material resources is also very important. It is the duty of Information Officer to define and determine card-key readers and buildings security. It might sound that this is irrelevant to the IT security but it should be kept in mind that physical security is equally important to avoid attacks.

**Behaviors**

It is believed that security is not a process or infrastructure rather it is a behavior that should be reflected from all the aspects of the organization. It is necessary to indicate what kind of behavior is required and expected from the management team and employees. A company must ensure that employees and staff must read and acknowledge the security policy and sign the documents. In case of any violation related to cybercrime, data breach or any such activity, the company reserves all the rights to exercise legal penalties take disciplinary actions.

**Training**

To maintain an effective and secure communication system, one-time investment or management is not enough rather it is a continuous process. Norms and practices in Information technology are changing every date and to keep pace with it is necessary to keep systems and security up to date. To involve maximum individuals of the company in ensuring the security of the security, time to time training is highly recommended in order to sustain the company’ security policy.

Once these seven criteria are determined and a secure system is established, one must draft frameworks and procedures as how to retain and comply with these policies. Before implementing any new technology or infrastructure, a company must review the authorization process prior to proper installment.

**Alignment with the Organization’s objective:**

 Generally, it is perceived that security in the communication system of an organization is the responsibility of IS (Information security) department. This mindset is perpetuated because of the fact that usually security related concerns, funding, and projects are normally limited to the IS department alone and rest of the department and employees have kept unaware of them. Some companies regard this as a cultural change and need a long-term commitment that means it is slow to understand and realize. There are many solutions to this problem and one of them is the alignment of the company’s security strategy with risk management and also to develop and implement the governance requirements. Each aspect or line of business that needs a certain level of security must designate a liaison to cooperate with the IS manager to make sure that all the necessary requirements are properly prioritized and reflected in the strategy of information security(Barrett, 2018). The evaluation mechanism should report to the board on a quarterly or annual basis regarding alignment of communication system and its security with the laws and regulations of the company.

In communication system, the company’s business and the information security are interlinked with each other and it is very important to understand and implement the required mechanisms for reliable services. There are some aspects of information security that follow a services model and many initiatives of the IS should be closely aligned with the relative business initiatives. One thing must be kept in mind that the cost of managing security and intellectual assets must not exceed than the actual value of the assets. An effective and secure communication requires the fulfillment of CIA framework. CIA is the acronym of confidentiality, integrity and accessibility. The whole concept of security management for the communication system revolves around these three aspects of communication reliability. It is necessary to have an effective and cooperative dialogue between experts in Information security for the communication system and experts from business areas.

With the advancement in technology, offices are not only restricted to workplaces and corporate environments. With the widespread internet and advances devices, one can work from anywhere and complete assigned tasks while sitting at home. As a CIO of a company, it is important to investigate and determine the requirements of Information system and security for the remote workers because safety systems installed in the office and implemented frameworks do not comply with the remote workers. It is required to implement different policies for remote workers as compared to the office workers. To avoid problems in the future, it is the responsibility of the CIO to formulate a security plan or policy for remote workers too. Absence of an effective and comprehensive policy may result in data theft or other potential harms. For remote workers following steps must be taken by CIO.

• A majority of malware and viruses that steal data by infecting PC come through email and web. To avoid this, good computer hygiene must be practiced by using security software.

• To avoid potential damage to the system, install whole-disk encryption software in your PCs, which will keep un authentic or un authorized persons from getting access to your system whether they are remote users or normal users.

• For a small company, web-based applications are sufficient to allow remote users work and share internet data with the company’s system but on large scale taking services of cloud service providers is an easy and comparatively secure approach (Richmond, 2012).

In the above sections, we have discussed the security requirements of a communication system underlying policy requirements from the management and technical point of view. The question arises that whether an effective communication management system is a managerial issue or purely technical? It is important to understand that both aspects are important and essential to determine effective communication and information handling.

 From a managerial perspective, back in the days, it was assumed that security management is only the responsibility of the concerned department of a company which is the Information security department. But today, companies are considering it the responsibility of all the departments and in fact all the employees of a company. Security is not a process or mechanism; it is rather a mindset and behavior which suggests that management plays an important role in this regard. Without proper management, technical framework and infrastructure is of no use. For managing the security of remote workers, a lot of technical accesses are required to make sure that the employees do not inflict any kind of threat to the sensitive data and MIS framework of the organization

References

Austein, R. (2017). An Out-of-Band Setup Protocol for Resource Public Key Infrastructure (RPKI) Production Services.

Barrett, M. P. (2018). Framework for improving critical infrastructure cybersecurity. National Institute of Standards and Technology, Gaithersburg, MD, USA, Tech. Rep.

 Kilday, R. W., Kaushik, S. S., Bali, S. S., Ma, X., & Wei, S. S. S. (2016). U.S. Patent No. 9,258,793. Washington, DC: U.S. Patent and Trademark Office.

Limba, T., Plėta, T., Agafonov, K., & Damkus, M. (2019). Cyber security management model for critical infrastructure.

Richmond, R. (2012, 8 22). How to Maintain Security When Employees Work Remotely. Retrieved from Entrepreneur: https://www.entrepreneur.com/article/224241