STP Limited

Networking Project

2017

9/16/2017

Table of Contents

[Introduction 3](#_Toc493528866)

[Project Background 3](#_Toc493528867)

[Project Scope 3](#_Toc493528868)

[Project Goals 4](#_Toc493528869)

[Strategic Alignment of the Project 4](#_Toc493528870)

[Network Security 5](#_Toc493528871)

[Ideal Branch-Office Security Solution 6](#_Toc493528872)

[Securing data 7](#_Toc493528873)

[Mobile device security 8](#_Toc493528874)

[Plan for Hardware Purchases 8](#_Toc493528875)

[Business continuity 9](#_Toc493528876)

[Risk management 9](#_Toc493528877)

[Risk Management Strategy 9](#_Toc493528878)

[Risk Identification 9](#_Toc493528879)

[Risk Responsibilities 10](#_Toc493528880)

[Risk Assessment 10](#_Toc493528881)

[Risk Response 10](#_Toc493528882)

[Risk Mitigation 10](#_Toc493528883)

[Tracking and Reporting 10](#_Toc493528884)

[Conclusions 10](#_Toc493528885)

[Recommendations 11](#_Toc493528886)

[References 13](#_Toc493528887)

# Introduction

STP Limited is an organization that is based out of Wollongong and has its head office in the same city. The organization manufactures cabinets and is expanding to the other regions as well. The sales and revenue are going good for the organization and as a result, it recently bought office premises in Bathurst and Lithgow. They have also set up a new office in Sydney. The company is currently located in four locations and has warehouse machines and other equipment installed in these locations. Networking has become a major area of concern for the company because of the need to come up as an integrated unit to provide good quality services to the customers.

# Project Background

There are new networking and communication technologies that are being used by STP Limited to enhance its connectivity and integration capabilities. Every office of the company is equipped with a modem and a switch and the Internet connection is made active with the aid of ADSL. The members of the staff are allowed to Bring their Own Devices at work which is also known as the BYOD scheme. The wireless connections are also made enable by the organization.

With the use and application of new networking channels and mediums in the organization, there can be a lot of growth and development that the organization may witness. It is because of the reason that the enhanced network connections will allow the employees to be connected with each other at any hour of the day. It will aid in the resolution of the problems and conflicts in a timely manner and will make it possible to experience enhanced efficiency and productivity of the employees. The customers will also be able to contact the organization in case of any query or complaint. There will be enhanced help and assistance services provided which will make it easy to increase the levels of customer trust and engagement (Cisco, 2008).

## Project Scope

The scope of the project is to develop the measures that may enhance the integration and security of the new networks and communication channels.

It will include the design, development and deployment of these measures so that the enhanced networking mediums are implemented. Privacy is one of the essential properties that are required to be maintained in association with the information and networks. The efforts will also be implemented to make sure that the privacy of the information and the communication networks is not disturbed or violated.

## Project Goals

* Ability to make sure that all the office locations and units of STP Limited are integrated with each other as a single unit.
* Ability to ensure that the security of the networks and the information channels is maintained along with the assurance of privacy (Pareek, 2011).
* Ability to make sure that enhanced revenues and customer engagement is earned with the improved networking and communication medium.

## Strategic Alignment of the Project

|  |  |
| --- | --- |
| Alignment Perspective | Description |
| Strategic Execution | * The strategies to implement the networking mediums and communication channels are in line with the organizational goals of achieving enhanced revenues and customer engagement. * The design, development and deployment of the networking integration measures will be done to achieve the goals. * The design, development and deployment of the security and privacy measures will be done to achieve the goals. |
| Technological Potential | * The wireless connections and networking equipment that have been set up are compatible with the organizational systems and applications. * The integration and security solutions that are proposed are feasible on the basis of technical feasibility study. |
| Competitive Potential | * Network security and privacy is a much in demand trend in the market. * The quality of the services is enhanced with the use of the advanced networking and communication mediums. |
| Service Level | * A networking strategy has been designed and determined by the Project Manager so that the organization goals are met. * Resources have been allocated to the project tasks and activities at the operational and managerial levels. |

# Network Security

There are various issues that must be addressed from the point of view of network security. It must be made sure that there are enough human resources in the department of local IT as the support staff. It would be necessary to understand the significance of remote management of the security controls and mechanisms which will involve roles such as network administrator, security analyst etc.

The device configuration that is set up shall be allowed to be accessed with the means of HTTP, HTTPS, Telnet, SSL and likewise. Remote management must provide the capability of remote configuration and management with minimal errors.

In a nutshell, the security solutions that are set up at the branch office must target the needs and requirements of the office sizes and these shall also be easy to deploy and economical in nature. Apart from the security services and solutions, the set of appliances at the branch office must also include the enhanced network capabilities such as secure routing, WAN connections etc. This will eliminate the requirement of installing separate networking devices and equipment.

Another condition that must be considered is the changing landscape of the security threats and attacks. There is a change of technology that is being witnessed with each passing day which leads to the emergence of new forms of threats and risks. There may be some extremely severe implications of these attacks and threats. For instance, in the year 2003, Slammer worm infected 90% of the susceptible hosts in 10 minutes with the doubling rate of 8.5 seconds. There are signature based countermeasures that are being implemented in the organizations which cannot be updated at such a short period of time (Canavan, 2001).

The effectiveness of the security solutions at the branch office would therefore need supplementing of the reactive countermeasures that may have the ability to prevent the uncertainties and security attacks that are not predicted earlier. The use of network focussed defence mechanisms shall also be used for preventing the security attacks associated with application layer and services.

## Ideal Branch-Office Security Solution

At a broader level, the following set of features and mechanisms shall be present in the ideal security solution at the branch office.

* It shall provide a fast and safe VPN connection based on the site-to-site connectivity. This would provide secure access to the centrally operated applications and services along with the support for remote access and management for the employees.
* A direct and secure access to the internet shall be provided. This would be significant in the avoidance of unknown Internet traffic re-directed through any of the regional headquarters location.
* Improved security services and solutions shall be provided for the internal services and network connections. It will be beneficial for the branch office and will also provide indirect benefits to the other connected sites and locations (Alabady, 2009).
* It shall be easy to use and shall also be cost-effective in nature. There shall be system qualities such as performance, reliability and usability maintained.

## Securing data

* Virtual Private Networks: The establishment of IPSec VPNs will be a prime necessity for the branch security solutions and services. There shall be maintenance of more than 100 simultaneous tunnels along with encrypted throughput, such as, greater than 100 Mbps. The use of secure encryption algorithms, such as tripe DES and AES shall be used with key exchange and user authentication protocols (Joshi and Karkade, 2015). NAT traversal and Microsoft VPN clients shall also be made available for the maintenance of security.
* Firewall: Firewall is one of the most significant measures for the security of the data. It should just not stick to the basic networking controls and access control at the transport layer. The access to only the traffic that is secure and as per the policies and regulations eliminates the possibility of many of the security threats and attacks. The effectiveness of firewalls can be realized only by the mode of application of the same, for instance, the implementation of firewall at the network layer only will not be able to prevent the security risks associated with the application layer.
* Attack Protection: There is certain amount of traffic that passes through even with the set up of the firewalls. It also does not identify certain types of security risks and attacks. Intrusion detection and prevention is a technology that comes in the picture to identify and prevent the entry of the bad elements. There are anomaly based, signature based, network based and behaviour based intrusion detection and prevention systems that have been developed for preventing many of the denial of service, flooding and integrity attacks (Strebe, 2004).
* Advanced Content Filtering: There are many of the anti-malware packages that are present such as, anti-viruses, anti-spyware etc. these are completely reactive in nature but have the capability to control the file based attacks and many of the known threats and attacks. There are also some of the serious malware such as Keylogger Trojans that can be prevented and controlled with the aid of this mechanism. There is Web/URL filtering measure that may focus on the outbound traffic and prevent the access to the web sites that are not safe (Soriano, 2011).
* Segmentation & Security Domains: Internal security at the branch office may be improved with the aid of this measure. It makes sure that the associated appliances have the capabilities such as multiple LAN interfaces along with VLAN connections. A unique security policy is enforced on the basis of the users and the computing resources.

## Mobile device security

Mobile devices are being increasingly used by the users and business organizations. A security strategy shall be developed and implemented to ensure the safety and security of the mobile devices. There are also unknown devices that may be connected to the office network with the use of BYOD technology.

There are network tools that may be used for enhancing the mobile device security.

* **Fingerprinting:** It is a mechanism that enhances and inspects the characteristics that are associated with the mobile devices to understand the type of the device, operating system installed in the device, browser version and so on. It may highlight the unsafe devices and their presence in the networks (Souppaya, 2013).
* **Network Access Controls:** It is commonly abbreviated as NAC and is a measure that may be used for advanced device management by the organizations. An in-depth analysis of the device is done under NAC to highlight the presence of any intruders associated with the device, anti-virus and anti-span packages and so on. If the necessary security solutions are not present in the device, then access of the same is limited in the corporate environment.
* **Authentication:** This is the security solution that comes after the fingerprinting and NAC. It authenticates the users on the basis of the WLAN standards such as 802.1x standard. The combination of the three controls will provide the organizations with the required set of security controls and network management (Sujithra and Padmavathi, 2012).

# Plan for Hardware Purchases

There may be a lot many equipment necessary for installation and testing purposes. Some of the necessary hardware may include the following:

* Computer Systems: These may be required for accessing the tools and applications for the purpose of installation and testing.
* Servers: There are web and file servers that may be required for accessing various information sets along with the database servers as well.
* Peripheral Equipment: Networking equipment such as switches, bridges, routers, hubs, gateways would be required for establishing and maintaining network connections.
* Simulators and Emulators: It would not be possible to carry out testing activities on all the devices and these tools will come into the picture for gaining a virtual experience and testing purposes.
* Diagnostic Equipment: The troubleshooting and diagnostic processes will be carried out for network management and security using this equipment.
* Communication Devices: These will be necessary for the sharing of information and data.

# Business continuity

* A disaster recovery plan shall be prepared by the administrators so that the backup and recovery of the data is made possible. The plan shall target upon the critical IT resources along with the resources required for the recovery of the data and system. The plan shall focus the critical information assets.
* Administrators that are responsible for the management of central/departmental servers must create multi-generational system backups.
* Administrators that are responsible for server management must secure that the current systems is secure and protected. A hard-copy listing of the backup shall also be created.

# Risk management

Risk is defined as any event that may have a probability of occurrence associated with it and it may have a positive or a negative impact. Risk management is defined as a process that may include the measures for the identification, assessment and treatment of the risks.

## Risk Management Strategy

### Risk Identification

A risk register will be prepared by the Project Manager covering all of the possible risks and attacks.

### Risk Responsibilities

The responsibility of dealing with the risks shall be distributed to all of the stakeholders. The risk responsibility shall be allocated for each of the risk that is identified. The mapping of the stakeholder must be done on the basis of the type and category of the risk (Berg, 2010).

### Risk Assessment

The assessment of the risk shall be done on the basis of its impact and likelihood along with the various factors that may be associated with the risks. The risk ranking shall be applied and assigned to every risk.

### Risk Response

A response strategy shall be defined for every risk that is identified and assessed. The response may include different treatment strategies and measures. There are various methods that may be applied for the risks, such as, avoidance, acceptance, transfer and mitigation (Crane, 2013).

### Risk Mitigation

It shall include the activities for the control of the risk along with the contingency plan associated with the same. The risk mitigation strategies as identified in the risk response process shall be applied and implemented for every risk (Dcu, 2015).

### Tracking and Reporting

The risk mitigation strategy shall be applied and the same shall be tracked and reported by the Project Manager. There shall also be a weekly report that must be prepared to keep a track of the same and the senior management must carry out monitoring and control activities (Debono, 2016).

# Conclusions

Brach offices along with the personnel working in the offices are critical assets for the organization at the strategic level. It is essential to make sure that the security of these branch offices is ensured by developing and implementing the measures for security the data and mobile devices. There is an enhanced network management that must be carried out for securing the information and for maintaining the business continuity. The threat landscape is changing at a rapid pace and the corresponding countermeasures that are developed shall be in accordance with the same. There must be system qualities that must be maintained which shall include reliability, availability, performance and usability.

# Recommendations

Evaluation of the network security:

* Third party testing process shall be used and implemented
* WLAN access logs shall be compared so that risks and attacks associated with the unknown devices are uncovered
* Determination of the usage of the app usage associated with the network tools
* Use and implementation of an identify-centric security model for the purpose of mobility

Evaluation of the level of infrastructure integration:

* The set of applications, cloud services and devices that is available and visible in an unified manner.
* The identification of the set of appliances that are old and make use of obsolete technology.
* Estimation of the people hours that may be saved from the IT staff for using a wired or a wireless network.

Evaluate the mobile population of the company:

* The number of employees that tele-commute an d the mediums that they use
* The number of employees that are present in this field
* VPN capabilities that are associated with the same

Evaluation of the present WLAN usage and the population of the devices:

* The number of the inventory device types that are used
* The number of form factors along with the operating systems that are used
* Site survey for the determination of the current usage of geographies and hotspots
* WLAN capacity that will be required along with the factors that contribute in the growth of tablet and the usage of Smartphones
* Evaluation of the VoIP and related latency sensitive applications that may assist in the development or building of the WLAN requirements and applications.
* Evaluation of the 802.11ac. If the use of 802.11ac the costs and architecture associated with it will be required to be developed.

# References

Alabady, S. (2009). *Design and Implementation of a Network Security Model for Cooperative Network*. [online] Available at: http://www.iajet.org/iajet\_files/vol.1/no.2/Design%20and%20Implementation%20of%20a%20Network%20Security%20Model%20for%20Cooperative%20Network.pdf [Accessed 18 Sep. 2017].

Berg, H. (2010). *Risk Management: Procedures, Methods and Experiences*. [online] Available at: http://ww.gnedenko-forum.org/Journal/2010/022010/RTA\_2\_2010-09.pdf [Accessed 18 Sep. 2017].

Canavan, J. (2001). *Fundamentals of Network Security*. [online] Available at: https://whc.es/Network/Fundamentals%20of%20Network%20Security.pdf.1.pdf [Accessed 18 Sep. 2017].

Cisco (2008). *Wireless and Network Security Integration Solution Overview*. [online] Available at: https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Mobility/secwlandg20/sec\_wireless\_overview.pdf [Accessed 16 Sep. 2017].

Crane, L. (2013). *Introduction to Risk Management*. [online] Available at: http://extensionrme.org/pubs/IntroductionToRiskManagement.pdf [Accessed 18 Sep. 2017].

Dcu (2015). *Introduction to Risk Management*. [online] Available at: https://www.dcu.ie/sites/default/files/ocoo/pdfs/Risk%20Mgt%20Training%20Slides.pdf [Accessed 18 Sep. 2017].

Debono, R. (2016). *Project Risk Management*. [online] Available at: http://www.isaca.org/chapters11/Malta/Documents/Events/210416%20-%20Mark\_Debono%20-%20Understanding\_Risk\_in\_the\_Field\_of\_Project\_Management.pdf [Accessed 18 Sep. 2017].

Joshi, M. and Karkade, R. (2015). *Network Security with Cryptography*. [online] Available at: http://www.ijcsmc.com/docs/papers/January2015/V4I1201544.pdf [Accessed 18 Sep. 2017].

Pareek, R. (2011). *Network Security: An Approach towards Secure Computing*. [online] Available at: https://www.rroij.com/open-access/network-security-an-approach-towards-secure-computing-160-163.pdf [Accessed 16 Sep. 2017].

Soriano, M. (2011). *Information and Network Security*. [online] Available at: http://improvet.cvut.cz/project/download/C2EN/Information\_and\_network\_security.pdf [Accessed 18 Sep. 2017].

Souppaya, M. (2013). *Guidelines for Managing the Security of Mobile Devices in the Enterprise*. [online] Available at: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf [Accessed 18 Sep. 2017].

Strebe, M. (2004). *Network Security Foundations*. [online] Available at: https://imcs.dvfu.ru/lib.int/docs/Networks/Security/Network%20Security%20Foundations.pdf [Accessed 18 Sep. 2017].

Sujithra, M. and Padmavathi, G. (2012). *Mobile Device Security: A Survey on Mobile Device Threats, Vulnerabilities and their Defensive Mechanism*. [online] Available at: http://dl.icdst.org/pdfs/files/35dc646a4630971fd27c6b2d32661555.pdf [Accessed 18 Sep. 2017].