SMALL OFFICE HOME OFFICE WLAN SECURITY FRAMEWORK

BY

Raphael Kiruthi Kariuki
P56/7271/06

SUPERVISOR
Mr. Eric Ayienga

A M.Sc. RESEARCH PROJECT IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF THE DEGREE OF MASTER OF SCIENCE IN INFORMATION SYSTEMS (IS)

OCTOBER 2012

DECLARATION

This research project is my original work, and has not been submitted for the award of a degree at any other university

Signed Date

Raphael Kiruthi

This research project has been submitted for examination with my approval as the University supervisor

Signed Date

Mr Ayienga

ABSTRACT

The adoption of wireless networks is mostly due to their ease of installation and since there is minimal cabling cost is also reduced when compared with the wired networks. However, it is not easy to confine the radio signal used in wireless networks within a particular geographical area. Due to this fact security is a big issue when it comes to wireless networks.

Having the right security controls enables proper management of people, processes and technology. The controls enable a security administrator to know which processes and technological solutions are required for the network to operate securely.

Many security administrators would like to operate a secure network but the problem is where to start. For small organizations such as a small office home office wireless network, this can be a big and costly challenge. A SOHO WLAN Security Framework can be of great help to these organizations.

From NIST Special Publication 800-30 risk management process, NIST Special Publication 800-37 risk management framework and ISO 27002 standard we were able to create the SOHO WLAN Security Framework.

From this framework an application was created using Visual Basic 2010. A field implementation of the application was done in Nairobi City center to gauge the performance of the security framework. The administrators in these organizations were satisfied with its performance but proposed that it should be thoroughly tested for it to have widespread acceptance.

AKNOWLEDGEMENTS

Firstly, I would like to thank my supervisor Mr. Ayienga who guided me throughout the years towards the completion of my project. The valuable guidance and advice he accorded is highly appreciated and will not be forgotten.

I would also like to thank my family for their continued support both financially and emotionally toward the achievement of my goals. They are a great source of inspiration.

I won't forget my class-mates who have given me encouragement and support towards my completion of the project. There are many also who have helped either directly or indirectly, I appreciate their help.

TABLE OF CONTENTS

Contents

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AP	Access Point
BSS	Basic Service Set
COBIT	Control Objective for Information Technology
CRC	Cyclic Redundancy Check
CSMF	Continuous Security Monitoring Framework
DSSS	Direct Sequence Spread Spectrum
FHSS	Frequency Hopping Spread Spectrum
IEEE	Institute of Electrical and Electronic Engineers
ISM	Information Security Management
ISO	International Organization for Standardization
IV	Initialization Vector
LAN	Local Area Network
MIC	Message Integrity Checking
RTS-CTS	Request to Send Clear to Send
SOHO	Small Office Home Office
SSID	Service Set ID
TKIP	Temporal Key Integrity Protocol
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity
WLAN	Wireless Network

Chapter 1

1.0 INTRODUCTION

1.1 Background

Kenya is investing substantially in the development of outsourcing sector. With the laying of fiber optic cables all over Kenya, it will soon be possible to work right at home or small centers in our neighborhood.

Outsourcing sector has a potential of transforming a country's economy. The massive laying of fiber optic cables all over Kenya and the amount spent on the high speed undersea fiber optic cables; South Africa, East Africa, South Asia Fiber Optic Cable(SEACOM), The East African Marine System(TEAMS), and The Eastern Africa Submarine Cable System (EASSY) is a proof that massive investment and job creation is expected. In fact outsourcing is projected to be one of the largest sources of employment in Kenya's vision 2030.

Due to the high rent in city centers and the awaited lowering of internet costs, it's expected that more people will opt to work outside city centers or at home. With internet connection, it will be possible for companies to outsource back office operations such as invoicing, data entry, order taking, and book keeping, just to mention a few.

With the low installation costs and ease in implementing, small office home office wireless network (SOHO WLAN) will be the choice of many businesses. Consequently, wireless networks are emerging everywhere and have become a popular option in the SOHO.

WLANs are appropriate in small office/home office (SOHO) due to their low cost. A SOHO includes any company with between two and fifty employees as well as the self employed who work from home (White, 2011). SOHO usually accesses the internet wirelessly.

However, the fact that WLAN use over-the-air mode of communication presents both wired and wireless specific threats and vulnerabilities. Too often people think that because

the setup of a wireless segment is literally plug and go that everything is functioning properly and securely (Prasad, 2007).

By default most vendors disable WEP, leaving it for the SOHO WLAN user to enable security. If you simply accept the default setting on the initial configuration screen you will be communicating in the clear. This is the default setting, which results in a station literally being naked, as its transmission is not encrypted.

Also, by default the network name is blank, which in actuality represents one of two settings that enables a SOHO WLAN wireless LAN client to complete the association process with an access point without having to know the name assigned to the AP. The other setting is the network name of 'any' which enables a SOHO WLAN client to connect to an access point without prior knowledge of the network name assigned to the AP. These two settings make the use of the network name as a password very insecure.

Most manufacturers of SOHO WLAN access points place their documentation on the Web. A hacker can easily make a list of default network names. The hacker then can configure his client station with those names, observing if a particular network name provides the opening he requires.

Under the IEEE 802.11 standard it is left to the implementer to determine how often to change the secret WEP key used in the SOHO WLAN. Due to this, most WEP keys have a relatively long life, which can range from weeks to months or years, depending upon the operating procedure of the SOHO WLAN organization implementing and operating the wireless LAN.

The biggest threat to Wi-Fi network security is ignorance. Management awareness and responses to wireless network weaknesses are critical to reduce the risks in Wi-Fi networks and increase the benefits of this fast-growing technology. This will in turn help to ease users' psychological fears of using these types of "invisible" networks. To the extent

that a security level is desired, the features of confidentiality, authenticity, integrity and availability should be provided in wireless networks (Hui Du et al, 2006).

From visiting Internet Service Providers in Kenya we learnt that security consideration is not a compulsory requirement but rather an option. If the customer does not request for enhancement of security in the wireless network installed the network will be unprotected. Therefore a comprehensive SOHO WLAN security framework is required as a means of aiding in setting up and operating a secure WLAN.

1.2 Problem Statement

Wi-Fi network systems are growing rapidly because they are easily deployed and provide convenient network access to users. The growth of Wi-Fi is expected to go on. The next generation of computer network is expected to be "Ethernet Everywhere" (Hui et al, 2006).

It is anybody's guess whether wireless standards such as Wi-Fi will ultimately flourish or fade, but with Intel throwing solid support behind the Institute of Electrical and Electronic Engineers'' (IEEE) 802.11 standard, their future looks promising (Bindseil, 2003). Wireless networks offer more mobility and most people have found that it is more convenient to have the mobility that wireless connections offer (Bindseil, 2003).

While the benefits of WLANs are substantial, wireless technology introduces security holes that security administrators must take into account if they are to adequately protect their organization from hackers, cyber terrorists and unauthorized intruders. Wireless networks are notoriously easy to compromise when improperly installed and operated (Ashley, 2004).

By use of a security framework, an administrator will be aware of what needs to be done to ensure that the WLAN has confidentiality, integrity and availability.

1.3 Purpose of the project

For a SOHO WLAN to operate securely the various vulnerabilities associated with this network and the threats that can exploit the vulnerabilities need to be known. With the right controls it is possible to reduce the threat level to the WLAN. A security framework which incorporates controls from internationally known standards can be used to reduce the level of risks to a level that is acceptable by the management of the SOHO organization.

1.4 Overall question

Due to its mobility and low installation cost, WLAN is an attractive technology for small office home office (SOHO). However, the mode of communication between the devices in a WLAN introduces multiple venues for attack and penetration. Will a WLAN security framework provide the necessary guidelines and practices for installing and operating a secure SOHO WLAN?

1.5 Objectives

Main Objective:

- Create a security framework that can be used to securely set up and operate a WLAN in a SOHO.

Sub Objectives:

- Determine the controls necessary for secure operation of a SOHO organization that uses WLAN.
- Determine how one can successfully implement the controls in the SOHO organization.
- Determine how one can know the level of risk of the SOHO organization if some the controls are not implemented.

1.6 Assumptions and limitation of the research

This study assumed that the SOHO organization used only wireless network. It is also assumed that the SOHO WLAN organizations consisted of no more than fifty employees.

Chapter 2

2.0 Literature Review

A wireless local area network is a LAN that does not rely on wires. In a WLAN, the signal is broadcasted and those near it can receive the signal. They make use of wireless transmission medium using radio frequency or infra red. Radio frequency is the most common transmission medium in Kenya.

The reasons why WLANs are attractive to a small business include:

a) Mobility: Users can freely move around the organization and still have internet access.
b) Deployment: Deploying a WLAN is easier than wired LANs. What is mostly required is an access point.
c) It is also easy to expand the WLAN. You just need to add additional access points if you want to increase the range.
d) Cost: Since cabling is minimal, WLAN will reduce the installation cost.
e) WLAN can also be easily integrated to the wired network.

WLAN also have some disadvantages:

a) It is slower than the wired network. IEEE 802.11n can have speeds of up to 300 Mbps.
b) Security: Due to the fact that it is not easy to confine the WLAN signal within a building, security is an issue. Also, the first standard IEEE 802.11 did not have strong security features. IEEE 802.11i is intended to enhance the security.
c) WLAN signals such as the radio signal can be interfered with by other radio signals. Cordless phones and microwaves are some common sources of interference.

In 2006 the WIFI semiconductor market shipped just under 200 million Wi-Fi Chipsets and by 2012, more than a billion Wi-Fi chipsets are to ship (Pan, 2007). This shows that the adoption of WLANs increases each year.

With the wide adoption of WLANs, it was discovered that the security features were not sufficient. The original standard IEEE 802.11 used Wired Equivalent Privacy (WEP) to provide encryption and authentication. WEP was however cracked and it is no longer considered safe.

Since it is not easy to confine radio signals inside a building, physical security is not sufficient to prevent an attacker from connecting to the WLAN. Stronger encryption and authentication mechanisms are required. This lead to the standard IEEE 802.11i being developed and it is concerned with the security of WLANs.

The fact that WLANs are easy to install and configure is due among other things that the security features are usually not enabled when shipped. If the network is used without the features being enabled, the system will be vulnerable. With the growth of the wireless system and its adoption in SOHO WLANs a comprehensive security framework is important.

System vulnerabilities continue to be a pressing risk for organizations and new threats emerge constantly (Lin et al, 2011). Controls therefore need to be put in place that can aid at mitigating or reducing the risks to a level that is acceptable to the management of the WLAN. Controls are needed to enhance trust in the information systems and are put in place to protect the network from attacks (Srinivasan, 2006).

In the past few years, senior management's interest in good internal controls has increased (Garber, 2010). This has mostly been due to the highly published attacks on WLANs especially when WEP was used for encryption and authentication.

Surveys in recent financial magazines show that many chief financial officers (CFOs) would like to have internal control monitoring programs in their enterprises, but do not know where to start to develop a program (Garber, 2010).

For small businesses, maintaining an effective IT control system can be a significant and costly challenge. Yet this is a vital task for them. Unlike larger corporations, smaller companies simply do not have the staff to deal with their exposure to escalating IT risks. Without adequate security solutions, a small business's entire computer operations could be shut down, severely impacting the business and causing devastative financial consequences (Busta et al, 2006).

The study attempts to find out whether security controls can be used to guide the management on where to use their resources effectively in reducing the risks to a SOHO WLAN to an acceptable level.

2.1 Technological Security in WLAN

There is a wide spread use of SOHO WLANs in Kenya today. Accompanying the growth in the use of SOHO WLANs is recognition that as initially designed they are not secure. The 802.11 was developed as an 'open' standard.

When security is not engineered into a solution during the initial stages, the security solutions have historically been less than optimal (Tung et al, 2006).

There are many vulnerabilities associated with the use of wireless LANs due to the over the air transmission. Users of these WLANS need to know how to overcome the security limitations. Too often people think that because the setup of a wireless segment is literally plug and go that everything is functioning properly and securely.

There are four functions necessary to provide a high level of security to a SOHO WLAN organization. These are authentication, authorization, encryption and accounting.

Authentication in SOHO WLAN refers to the verification of the identity of a user. Under WEP authentication occurs through the use of a common key configured on clients and an access point. The key performs encryption. Each SOHO WLAN client and access point are configured with the same key, resulting in the term shared key cryptography used to refer to the encryption method. An access point can issue a challenge to any station attempting to associate with it. The station then uses its shared key to encrypt a response to authenticate itself and gain access to the SOHO WLAN. However WEP key is weak and shared key can be recovered via passive monitoring of the SOHO WLAN traffic. This means that IEEE 802.11 SOHO WLANs do not have a secure method of authentication, but one that can be compromised.

Some proprietary techniques employed by SOHO WLAN vendors use the MAC address of the wireless PC Card for authentication. WEP which provides encryption services does not hide source MAC addresses and this means an unauthorized third party could learn and spoof a MAC address and become an uninvited participant on the SOHO WLAN.

To provide a higher level of authentication in the SOHO WLAN one should consider a solution that authenticates the user and not the user's hardware. Examples of potential authentication solutions include the use of a RADIUS server, a secure ID card and other user/password authentication schemes that require a wireless client to be verified by a server prior to gaining access to the SOHO WLAN.

Authorization represents the permission or denial of access to various SOHO WLAN network and computer functions based upon the identity of the user. It ensures that no user who successfully connects to the network has access to data that he/she should not see. 802.11 standards and its extension do not address authorization.

One can effect network and computer authorization in a SOHO WLAN through a variety of hardware and software products. For SOHO WLAN network authorization you can

consider router access lists and firewall configurations as mechanism to enable or disable the flow of wireless traffic. In computer environment you can use operating system functionality as well as third part products to enable or disable the ability of SOHO WLAN users to access directories and file, run different programs and perform other types of computer activities.

Accounting represents a function of many SOHO WLAN security performing devices that can be valuable for setting rules and obtaining historical data which can be used by law enforcement agencies to prosecute an individual. Many servers in the SOHO WLAN can be configured to log access requests as they occur to form a database of different events such as successful or unsuccessful logon attempts. Using this database the server can be configured to enable or disable future logons based upon the prior history of unsuccessful logons during different predefined periods of time, a situation referred as a lockout. The history of activity in the SOHO WLAN based upon MAC and layer 3 addresses attempting to access different facilities can be used by prosecutors if you need to alert law enforcement agencies about actual or attempted break-ins.

Encryption in SOHO WLAN is performed by use of Wired Equivalent Protocol (WEP). This results in the data flowing through the wireless LAN having the same security as that in a wired network that does not have encryption. WEP is however weak and there is upgrade to 802.11i.

Each access point and served clients in the SOHO WLAN are identified by a network name. However, many manufacturers configure their access points with default network names and it is easy to guess a valid name. Changing the default name will make it hard for an unauthorized third party to gain access to the SOHO WLAN. Disabling the broadcast of network names in our SOHO WLAN will make it more difficult for unauthorized people to recognize the SOHO WLAN. This is because AP periodically transmits beacon frames that

enable clients to note the presence of the AP. By default AP transmit their network name in beacons. Also in default settings, WEP is disabled.

The human factor and the way they deal with device settings, placements and overall managements have significant value in wireless security (Naamany et al, 2006).

There are several steps that are employed to enhance the level of SOHO WLAN security. If you don't have software that automatically changes WEP keys in the SOHO WLAN, then changes should be done periodically. Changing the SOHO WLAN keys forces an unauthorized third party that recovered a prior key literally back to square one.

Also, the AP should be configured to restrict access based upon client Media Access Control (MAC) addresses. Although MAC addresses can be learned via passive monitoring, its use as an access mechanism makes it more difficult for an unauthorized third party to gain access to the SOHO WLAN.

Positioning and shielding of the antennae should be considered in the SOHO WLAN to reduce or eliminate radio frequency waves flowing to parking lots and other floors in the building.

Since most AP used in the SOHO WLAN support Dynamic Host Configuration Protocol (DHCP) to dynamically assign IP addresses to clients, limiting the number of addresses that can be issued to the number of clients in the SOHO WLAN will limit the ability of unauthorized third party to gain access to the network.

The use of stronger authentication and encryption protocols in the SOHO WLAN will also improve security. The use of Challenge Handshake Authentication Protocol (CHAP) can be used to authenticate the user or with a MAC hardware address to authenticate both the hardware and SOHO WLAN user.

Folder sharing should be disabled in the SOHO WLAN. Instead, file and folders to be shared should be moved to servers that are offered protection by a firewall. This is because in a mixture of operating systems, folder sharing can represent a weak link.

The SOHO WLAN AP should also be protected by a firewall when connecting to the wired network. This will enable one to take advantage of the security features of the firewall. These features include filtering based upon source and destination IP addresses, port numbers and other parameters as well as the use of IPSec to create a VPN over the wireless infrastructure.

2.2 The SOHO WLAN Network architecture

In 1997 the Institute of Electrical and Electronics Engineers (IEEE) adopted the 802.11 standard. This standard defined transmission rate of 1 and 2 Mbps for three Media Access Control (MAC) methods: Frequency Hopping Spread Spectrum (FHSS), Direct Sequence Spread Spectrum (DSSS) and infrared.

It wasn't until the 802.11b extension to the 802.11 standard was adopted that wireless LANs achieved significant growth. That extension raised the maximum data transmission rate to 11 Mbps, which enabled the technology to become well suited for both home and office applications that included Web browsing and file transfers.

Basic networking devices

There are four general types of wireless LAN devices that can be used to form different types of wireless network structure. These devices are the wireless LAN station, an access point, wireless routers and wireless bridges.

The WLAN station is the device that incorporates the functionality of the 802.11 standard in the MAC and physical layers to support wireless communications. A station can represent a notebook or desktop computer or devices referred to as access points, bridges and broadband routers.

Most notebook and desktop PCs obtain their wireless LAN functionality via the use of a Wireless Network Interface Card (NIC) and a software driver. In addition to PC Cards, other popular form factors used for the fabrication of wireless LAN network interface cards include a PCI bus based adapter and a USB compatible self-contained NIC.

An access point represents a second type of wireless station. The access point functions as a two-port bridge, linking a wired infrastructure to the wireless infrastructure. As a layer 2 bridge it operates using learned MAC addresses to perform filtering, forwarding and flooding.

The dual antennas mounted on the access point enable the device to select the best possible signal since signals are typically reflected off stationary and moving objects on their path from source to destination, resulting in each transmitted signal having multiple received components. The use of dual antennas is referred to as space diversity.

The wireless bridge represents a special type of access point. This type of access point typically consists of a separate base unit and antenna that are connected to one another by a low loss cable. Typically the wireless bridge antenna is designed for mounting on the edge or roof of a building. Its high level of receiver sensitivity provides a line of sight communications capability that permits communication between two geographically separated locations that can be between 4 and 7 km apart.

Building upon the functionality of the access point, several vendors introduced wireless routers that add a routing capability to an access point. In addition to providing support for basic routing, wireless routers typically include support for the Dynamic Host configuration Protocol (DHCP) and Network Address Translation (NAT).

DHCP provides a router with the ability to dynamically issue IP addresses to each station. In addition to assigning stations with an IP address, the router supporting DHCP will also dynamically issue the gateway and DNS server addresses to each station.

While it is possible for DHCP to be configured to use any block of IP addresses, in a wireless environment one of three blocks of special addresses reserved for private networks are commonly used. Under RFC 1918 the Internet Assigned Numbers Authority (IANA) reserved three blocks of IP addresses for use on private networks. Those address blocks represent Class A, B and C address as indicated below:

- 10.0.0.0 – 10.255.255.255
- 172.16.0.0 – 172.31.255.255
- 192.168.0.0 – 192.168.255.255

Although RFC 1918 addresses cannot be directly used on the Internet they facilitate the assignment of IP addresses on internal networks. Then through the process of network address translation RFC 1918 addresses can be translated into a public IP address that can be used on the Internet.

A second features that goes hand-in-hand with DHCP implemented on wireless routers is Network Address Translation (NAT). NAT was originally developed as a mechanism to economize upon the use of IP addresses, since it permits multiple hosts to share the use of a common IP address. A second function associated with NAT which is mostly applicable to wired stations' is that you obtain a degree of security as its use hides host IP addresses from view, preventing a direct attack on a station.

The Basic Service Set

The basic building block of an IEEE 802.11 wireless LAN is referred to as a Basic Service Set (BSS). A BSS can be viewed as an area of communications coverage that permits member stations to exchange information. There are two types of BSS that correspond to the two transmission methods supported by wireless LANs – peer-to-peer and infrastructure.

A group of two or more wireless stations that communicate with one another without the use of an access point form an Independent Basic Service Set (IBSS). Each station can

communicate directly with another station without having to use the facilities of an access point. This type of networking that permits peers to communicate directly with one another is referred to as peer-to peer networking.

The second type of network structure supported by IEEE 802.11 wireless LANs requires stations to communicate through the use of an access point. This type of network structure results in the use of an access point functioning as a relay device between wireless stations or wireless stations and a wired infrastructure. The use of an access point results in the network structure referred to as an infrastructure and the Basic Service Set being referred to as an Infrastructure Basic Service Set.

Because signals attenuate as they flow through the air the range of coverage of an Infrastructure Basic Service Set has a finite limit. To extend the area of coverage requires the installation of one or more additional access points, with each access point creating another Infrastructure Basic Service Set. This results in The Extended Service Set (ESS). The connection of two or more access points occurs through the use of a Distribution System (DS).

Station Services

Under the IEEE 802.11 standard several types of services are defined that provide both security and data delivery functionality. One of those services is authentication, which provides a mechanism to control access to a wireless LAN. Authentication represents both a security and an access control feature.

Under the IEEE 802.11 standard any station that requires the use of the wireless LAN to transport data must be authenticated prior to being able to transfer data. The 802.11 standard defines two types of authentication:

1) Open system and
2) Shared key

Open system authentication represents the default authentication method supported by the IEEE 802.11 standard. Under this authentication method a station transmits an authentication request to an access point. The access point processes the request and determines whether or not to allow the station to proceed. Based upon the response received from the access point (success or failure), the station will either continue or terminate its access.

Under open system authentication, a station can authenticate with any other station or access point as long as the receiving station is configured to support this method of authentication and has resources available to communicate. Thus, open system authentication represents a null authentication method and requires the development of an application layer program to enhance its operation.

The second type of authentication supported by the IEEE 802.11 standard is shared key authentication. Under shared key authentication either a 40 bit or 104 bit key in the form of 10 or 26 hex characters is distributed to each station out-of-band. Here the term ‘out-of-band’ references the fact that the key is distributed to stations by a method other than wireless communications.

The key is used both to enable security in the form of the WEP algorithm and to provide authentication. Once the applicable key is distributed to stations the access point generates a ‘random’ 128 bit text challenge. Each station encrypts a challenge using the previously configured shared key and responds to the access point. The access point will decrypt the challenged text using the same shared key and compare it to the challenged text it previously transmitted to the station. If a match occurs, the AP will respond indicating authentication was successful. If not, the access point will respond with a negative authentication.

Deauthentication represents a station service used to terminate an existing authentication. This service can be invoked by either authenticated party and represents a notification that cannot be refused.

A third station service is privacy. Under the IEEE 802.11 standard and its extensions privacy represents an optional station service in the form of the WEP algorithm. WEP is designed to provide a level of security equivalent to a wired LAN where data flows non-encrypted.

WEP was never designed for providing secure communications similar to what we would expect when transmitting data via a VPN overlaid over the Internet. Also WEP by default is normally disabled. This means that unless you configure your stations to support WEP and configure an applicable key for each station, all messages will be transmitted in the clear.
IEEE wireless LANs operate using a modified form of Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA), referred to as the Distributed Coordination Function (DCF).

2.3 IEEE wireless LAN standards

The basic IEEE 802.11 is the first standard. The IEEE 802.11 standard defined three physical layers methods that could transport the frames defined for MAC operations.

Physical layer operations included two Radio Frequency (RF) methods that were originally developed for military operations to overcome enemy jamming of RF communications. Those two physical layer methods are Frequency Hopping Spread Spectrum (FHSS) and Direct Frequency Spread Spectrum (DSSS). The third physical layer supported by the IEEE 802.11 standard is diffused infrared (IR).

The 802.11b extension was one of two extensions to the 802.11 standard that was published shortly after the basic standard, the other being the 802.11a extension. The 802.11b extension operates in the same frequency band as the basic standard. The 802.11b extension specifies the use of DSSS at 1, 2, 5.5 and 11 Mbps. The frequency used is 2.4 GHz.

The 802.11a extension to the 802.11 standard uses a frequency division multiplexing scheme referred to as Orthogonal Frequency Division Multiplexing (OFDM). A second

difference is the fact that this extension defines a physical layer standard for wireless LANs operating at data rates up to 54 Mbps. The frequency used is 5 GHz.

The 802.11g extension to the 802.11 standard can be considered as a high speed extension to 802.11b. Equipment that supports the 802.11g extension operate in the 2.4 GHz frequency band using OFDM to obtain data rates up to 54 Mbps as well as being backward compatible with 802.11b equipment.

Recognizing the limitations of WEP resulted in the development of the 802.11i extension to the 802.11 standard. This supplement to the MAC layer enhance wireless LAN security and apply to 802.11 physical standards defined by the a, b and g extensions. The 802.11i supplement defines two new encryption methods as well as an authentication method. This authentication method uses port-based authentication defined by a prior IEEE standard (802.1x) which was in turn based upon an Internet RFC. The two encryption methods designed to replace WEP include the Temporal Key Integrity Protocol (TKIP) and the Advanced Encryption System (AES).

Frame Formats and Basic Security Operation

Wireless LANs transport information in protocol data units referred to as frames. IEEE 802.11 wireless LANs operate at the second layer in the OSI Reference Model, the data link layer, with each frame containing a header, a variable length body, and a trailer in the form of a 32 bit cyclic redundancy code contained in a Frame Check Sequence (FCS) field.

The initial communication between two stations in an independent BSS, or between a station and an access point within an infrastructure BSS, is referred to as an association.

The association process is accomplished through one of two types of scanning. The first type of scanning, which is referred to as passive scanning, results in a station listening to each IEEE 802.11 channel for a predefined period of time. The station listens for a special

type of management frame referred to as a beacon. Access points periodically broadcast beacon frames that identify the AP and define its capabilities.

Included within the beacon is an identifier referred to as a Service Set Identifier (SSID) which functions as an elementary password. Because it is possible to have multiple access points within a geographic area, stations require the ability to associate themselves with a predefined AP. To do so you configure your station with the SSID of the access point you wish to communicate with.

A second scanning method results in a station transmitting a probe frame on each channel, waiting for all access points within hearing of the probe to respond with a probe response frame. This type of scanning is referred to as active scanning. Like a beacon frame, the probe frame contains an SSID.

Regardless of the type of scanning used once a station recognizes an access point it will transmit an associate request frame. This frame will denote the capabilities of the station and the data rates it supports. The access point will respond with an associate response frame. The associate response frame includes a status code and station ID for the station. Upon receipt of the associate response frame the station becomes part of the network and can begin transmitting.

Through the use of the network name ‘any’ you can usually connect to most access points even if you do not know the SSID. An access point periodically transmits beacon frames as a mechanism to inform stations of its presence.

Once a station notes the presence of an access point it can negotiate access to the AP. This negotiation process results in the transmission of an associate request frame from the station to the AP. The access point will respond with an association response frame.

Once a station is associated with another station or access point either party can break the association. To do so the station or access point will transmit a disassociation frame that must be honored.

The goal behind WEP was to provide wireless LANs with a level of privacy equivalent to a wired infrastructure. It was not intended to represent a totally secure method of communication, nor was it intended to provide a cryptographic method of transporting data that is unbreakable. WEP was designed to provide a wireless LAN with a level of privacy equivalent to data that flows in plaintext over a wired Infrastructure.

Security Risks and Countermeasures

IEEE 802.11 wireless LAN requires each client station to be configured to use the network name associated with the access point they wish to communicate with. The network name is more formally referred to as the Service Set Identification (SSID). The SSID represents a unique identifier that is included in the header of wireless LAN packets when a client station attempts to join a Basic Service Set (BSS) via communicating with an access point that forms the service set. The actual role of the SSID is to provide wireless LAN commonality.

While the SSID or network name is obviously an easy to defeat 'password,' you can make it more difficult for an unauthorized third party to access your network. To do so you can remove the SSID from beacon frames if your equipment supports its removal. In addition, where possible you should change the SSID from its default setting. While this is possible for most equipment, some access points appear to have been configured to always use the MAC address of the device as the network name. When this occurs, software will not allow the SSID to be changed.

The establishment of a wireless LAN within an office building or home results in walls providing a false sense of security. The risk associated with this is eavesdropping. Although

the transmission distance of wireless LANs is normally limited to hundreds of meters, this limitation is based upon the use of small antennas built into PC Cards and other form factors used to create wireless network interface cards. When more sensitive antennas are used, it becomes possible to pick up the radio frequency transmission of wireless LANs at a considerable distance from their source. There are several programs that can be obtained from the Internet which can reconstruct the WEP key in use if a sufficient number of frames are captured.

One cannot decrypt a signal one cannot hear. A valuable countermeasure to eavesdropping that one can utilize is to obscure or hide RF signals from unauthorized third parties. To do so you can consider antenna positioning and the use of shielding. While antenna positioning is important, it may also be possible to control the use of a particular antenna when your wireless LAN device supports antenna diversity.

If a third party can eavesdrop on your wireless LAN communications it becomes possible for that party to pretend to be a legitimate user of the network. Masquerade can be very dangerous as it provides a literal open door to your network resources.

One often overlooked security vulnerability that can occur is if Windows file sharing is enabled on one or more wireless LAN stations. This security vulnerability can happen even when your network is hardened through the use of authentication, encryption, and accounting because under most versions of Windows it is difficult to authenticate file-sharing users.

In a wireless LAN environment jamming can occur without the use of specialized equipment because the manner in which FHSS and DSSS communications occurs is well-known. In addition, the design of the wireless LAN protocol makes it very susceptible to jamming by simply modifying software to transmit certain types of frames.

Countermeasures you can consider using to reduce or minimize the potential for your wireless LAN to be jammed are:

1) Periodic monitoring of your network when throughput appears to decrease can be used to determine if someone is jamming your organization's network. By using a protocol analyzer you can note if an exceedingly high level of a particular type of frame is literally clogging the air. If so, you can use the signal strength indicator, available with most utility programs that are bundled with different wireless LAN adapter cards, to locate the direction from which the frames are being broadcast. By moving a laptop or notebook computer around you may be able to locate the source of the apparent jamming and then take appropriate action.
2) Another technique that can be considered to minimize the effect of jamming is to turn off the ability of clients and access points to use the RTS-CTS frame sequence.

Based upon the manner in which access points operate it is possible to monitor wireless broadcast traffic and learn information about wired network traffic.

Another threat is theft of hardware. One of the key countermeasures to equipment theft is employee education. Employees should be aware that it is imperative to report the loss of equipment which includes network enabled devices. In addition, it is equally important to change the settings on the security mechanism used by your organization on a periodic basis. Doing so can minimize the adverse potential resulting from the unreported loss of network enabled equipment.

Because the cost of access points has reduced many organizations now face the threat of rogue APs. There are several types of monitoring tools that network managers and LAN administrators can consider using to locate rogue access points.

Standards Based Security

When connecting to a wireless network, one must perform some type of authentication. There are two main types of authentication per the current IEEE standards: share key

authentication and open key authentication. Open key authentication involves supplying the correct SSID.

Shared key authentication is not considered secure because a hacker who detects both the clear text challenge and the same challenge encrypted with a WEP key can decipher the WEP key. With open key authentication, even if a client can complete authentication and associate with an AP, the use of WEP prevents the client from sending data to and receiving data from the AP unless the client has the correct WEP key.

Open authentication sends an authentication request but does not receive a challenge; instead, it is allowed to talk by default. When WEP is enabled, the process is slightly different. When the wireless client starts to talk, it automatically encrypts all the data with WEP encryption. When the access point hears data being sent, it decrypts the frames and forwards them. If the frames are encrypted with a different key than the access point, the decryption portion fails and the packet is dropped.

Wired Equivalent Privacy Standard (WEP)

The Wired Equivalent Privacy (WEP) standard was created to give wireless networks safety and security features similar to that of wired networks. WEP is defined as the optional cryptographic confidentiality mechanism used to provide data confidentiality that is subjectively equivalent to the confidentiality of a wired local area network (LAN) medium that does not employ cryptographic techniques to enhance privacy.

To meet its goals, wireless had to address the three tenets of information security: (1) confidentiality, (2) availability, and (3) integrity.

1) The fundamental goal of WEP is to prevent eavesdropping, which is confidentiality.
2) The second goal is to allow authorized access to a wireless network, which is availability.

3) The third goal is to prevent the tampering of any wireless communication, which is integrity.

The WEP protocol is used to encrypt data from a wireless client to an access point. This means the data will travel unencrypted inside the wired network.

The WEP protocol is based on RSA Securities' RC4 stream cipher. This cipher is applied to the body of each frame and the CRC.

There are two levels of WEP commonly available: (1) one based on a 40-bit encryption key and 24-bit initialization vector, which equals 64 bits; and (2) one based on a 104-bit encryption key and 24-bit initialization vector, which equals 128 bits.

In performing the WEP encryption process, a number of steps are performed. The first step is to generate a seed value. This seed value is used to start the keying process. This value can be referred to as a key schedule or as the seed value. It is considered the WEP key. After this value is defined, it must then be entered into the access point. To ensure that the client can receive and decrypt the transmission, the seed value or WEP key must be entered on to each client. This will allow a WEP encrypted conversation to occur. This value consists of a 26-digit hexadecimal number.

This value is not used alone to create a WEP encrypted data stream; a technique to randomize the key is applied as well. This technique uses a 24-bit initialization vector (IV) that is created on a frame-by-frame basis. The technique on which the IV is created differs between vendors. The WEP standard that is outlined inside 802.11b states the IV size and requires that the IV change on a frame-by-frame basis. Outside of this, there are no requirements in the standard defining how to increment or randomize the IV sequence.

Once the IV and WEP key are together, they can be used to encrypt the frame. When the data is ready for transmission, the WEP key and the IV are combined; then, using the RC4 cipher, the key and IV are XORed with the data to create the encrypted frame. Next, a

copy of the same IV is put into the frame header as clear text. The last step is to send the packet.

Once the other end receives the frame, the IV is picked out of the frame header and applied to the predefined seed value to produce the same session-based WEP key that was used to encrypt the packet. The same RC4 encryption process is performed in reverse, allowing the encrypted text to turn from cipher text to plaintext. Once this operation is complete, the CRC is removed and applied to the data to make sure that it was not corrupted in transit.

WEP weaknesses were recognized soon after its release as part of the 802.11 standard. Because of a weakness in the RC4 key scheduling algorithm, the output key stream was significantly non-random. This allows the encryption key to be determined by analyzing a sufficiently large number of data packets encrypted using the key.

In essence, WEP transmits information about the encryption key as part of the encrypted message so that a determined hacker, equipped with the necessary tools, could collect and analyze transmitted data to extract the encryption key. WEP also uses a static shared key, as there is no mechanism for changing the key other than manual re-entry of a new key or passphrase into every device that operates on the WLAN. New and more powerful encryption methods were the required.

Wi-Fi Protected Access (WPA)

To overcome the known vulnerabilities in the original 802.11 security implementation, the Wi-Fi Alliance developed Wi-Fi Protected Access (WPA) as a means to provide enhanced protection from targeted attacks. WPA was an interim measure that was based on a subset of the enhanced security mechanisms that were then still under development by 802.11 TGi as part of the 802.11i standard.

The Wi-Fi Alliance created WPA by leveraging what the 802.11i task group had already done and formalized it into WPA.

WPA uses the temporal key integrity protocol (TKIP) for key management, and offers a choice of either the 802.1x authentication framework together with extensible authentication protocol (EAP) for enterprise WLAN security (Enterprise mode), or simpler pre-shared key (PSK) authentication for the home or small office network which does not have an authentication server (Personal mode).To combat someone using this key to eavesdrop on others' conversations, WPA uses a method that creates a unique session key for each device. This is done by having a pre-shared key called the group master key (GMK) that drives a pair transient key (PTK).

Temporal Key Integrity Protocol (TKIP)

The Temporal key Integrity Protocol (TKIP) was an interim solution developed to fix the key reuse problem of WEP. It later became part of the 802.11i. The WEP encryption vulnerability was addressed in WPA by two new MAC layer features: a key creation and management protocol called TKIP (temporal key integrity protocol) and a message integrity check function (MIC).

After a station has been authenticated, a 128-bit temporal key is created for that session, either by an authentication server or derived from a manual input. TKIP is used to distribute the key to the station and access point and to set up key management for the session. TKIP combines the temporal key with each station's MAC address, plus the TKIP sequence counter, and adds a 48-bit initialization vector to produce the initial keys for data encryption.

With this approach each station will use different keys to encrypt transmitted data. TKIP then manages the update and distribution of these encryption keys across all stations after a configurable key lifetime that might be from once every packet to once every 10,000

packets, depending on security requirements. Although the same RC4 cipher is used to generate an encryption key stream, TKIP's key mixing and distribution method significantly improves WLAN security, replacing the single static key used in WEP with a dynamically changing choice from 280 trillion possible keys.

WPA supplements TKIP with a message integrity checking (MIC) that determines whether an attacker has captured, altered and resent data packets. Integrity is checked by the transmitting and receiving stations computing a mathematical function on each data packet. While the simple CRC-32, when used to compute the ICV in WEP, is adequate for error detection during transmission, it is not sufficiently strong to assure message integrity and prevent attacks based on packet forgery. This is because it is relatively easy to modify a message and re-compute the ICV to conceal the changes. In contrast, MIC is a strong cryptographic hash function, which is calculated using source and destination MAC addresses, input data stream, the MIC key and the TKIP sequence counter (TSC).

If the MIC value computed by the receiving station does not match the MIC value received in the decrypted data packet, the packet is discarded and countermeasures are invoked. These countermeasures consist of resetting keys, increasing the rate at which keys are updated, and sending an alert to the network manager. MIC also includes an optional countermeasure, which will deauthenticate all stations and shutdown the BSS for any new association for one minute, if an access point receives a series of altered packets in quick succession.

802.1x

The 802.1x standard was designed for port base authentication for all IEEE 802 networks. This means it will work across Ethernet, FDDI, token ring, wireless, and many other 802 networking standards.

802.1x is in no way any type of encryption or cipher. All the encryption takes place outside the 802.1x standard. It was intended for, port-based authentication. The standard takes the authentication request, decides if it is or is not allowed onto the network, and then grants, or revokes, access. The authentication server, authenticator, and supplicant are three main roles of any 802.1x exchange.

The authentication server provides the access granting and access rejecting features. It does this by receiving an access request from the authenticator. When the authentication server hears a request, it will validate it and return a message granting or rejecting access back to the authenticator.

The authenticator is the first piece of network electronics that an 802.1x device will attempt connection. It can be a wireless access point, although it can be anything providing access to the network. The device's role is to let only EAP packets pass through and then wait for an answer from the authentication server. Once the authentication server responds with accept or reject message, the authenticator acts appropriately. If the message is returned, it is a reject message and it will continue to block traffic until the result is access accept. When the accept response comes from the authentication server, the authenticator then allows the supplicant the ability to access the network.

The supplicant is the device that wants to connect to the 802.1x network. This can be a computer, laptop, PDA, or any other device with a network interface card. When the supplicant connects to the network, it must go through the authenticator. This authenticator only allows the supplicant to pass EAP request traffic destined for the authentication server. This EAP traffic is the user's or device's authentication credentials. Once the authentication server determines that the user or device is allowed on the network, it will send an access-granting message.

Extensible Authentication Protocol (EAP)

Extensible Authentication Protocol (EAP) is a standard method of performing authentication to gain access to a network.

When Password Authentication Protocol (PAP) first came out, security issues quickly made it a less desirable authentication method. After that, the Challenge Handshake Authentication Protocol (CHAP) came out and this also quickly became plagued with security issues. The industry decided it was easier to make an authentication protocol act the same way no matter how or what type of authentication validation took place.

This meant that for the first time a protocol could be inserted into products and software that allowed for passwords, tokens, or biometrics without having to write any extra code to support the different methods.

This is how and why EAP was created. To use EAP, one must specify inside the type field what kind of authentication one is going to use. This allows one to use EAP for password, tokens, and other authentication types. EAP can adapt to security issues and changes by leveraging different methods of authentication. EAP also is able to address new and always-improving authentication techniques without having to make any changes to EAP supporting equipment.

One of the main points in using EAP is the ability to leverage multiple types of authentication mechanisms.

Wi-Fi Protected Access (WPA2)

WPA2 is the Wi-Fi Alliance's implementation of the final IEEE 802.11i standard and replaced WPA following the ratification of 802.11i in June 2004.

WPA2 implements the advanced encryption standard (AES) encryption algorithm using counter mode with cipher block chaining message authentication code protocol (CCMP).

802.11i

The IEEE 802.11i standard defines security enhancements for 802.11 WLANs, providing stronger encryption, authentication and key management strategies with the objective of creating a robust security network (RSN).

The key features of the RSN are;

- A negotiation process that enables the appropriate confidentiality protocol for each traffic type to be selected during device association
- A key system that generates and manages two hierarchies of keys. Pairwise keys for unicast and group keys for multicast messages are established and authenticated through EAP handshakes during device association and authentication
- Two protocols to improve data confidentiality (TKIP and AES-CCMP).

Key caching and pre-authentication are also included in 802.11i to reduce the time taken for roaming wireless stations to associate or re-associate with access points.

The client would first need to make a connection to the access point. This would happen through the normal open key authentication process. Contrary to most 802.11 standards, 802.11i only allows for open system authentication. This is due to the discovery of a security flaw in shared key authentication. After the initial connection request, the client would need to hear an RSN IE broadcast or send a probe request with an RSN IE. Whichever way this RSN IE frame is sent, both clients and access points need to negotiate on a cipher suite for use. After sending the RSN IE frames and reaching a negotiation, the EAP process starts. This can start with the access point sending an EAP identity request or a client sending an

EAPOL Start frame. Once the EAP process has started, it will go through the EAP authentication process associated with each particular EAP type. It ends with the client receiving an EAP success message from the access point. During this process, an AAA key is sent from the authentication server to the wireless end device. This key is used as a seed key to create the keys outlined below.

The key exchange process takes the original 802.1x EAPOL-Key frame and makes some modifications, allowing for the use of WEP-40, WEP-104, TKIP, and CCMP cipher suites. From the 802.1x section, the EAPOLKey frame only supports WEP-40 and WEP-104 keys. The 802.11i standard modified this and added the ability for the frame to carry TKIP and CCMP keys as well. A process known as the four-way handshake accomplishes this key exchange. This process takes two main keys and creates unique group and session keys for each client. These session and group keys are created from the two main keys: (1) the pairwise key or the pairwise master key (PMK) and (2) the group key or the group master key (GMK).

In an 802.1x 802.11i setup, the PMK comes from the authentication server. If the 802.11i setup is using preshared keys, then the PMK is mapped to a password. The PMK is divided into three keys. The first key is the EAPOL-key confirmation key (KCK), which is used to provide data origin authenticity. The second key created from the PMK is the EAPOLkey encryption key (KEK), which is used to provide confidentiality. The last key is called the pairwise temporal key (PTK) and this key is also used for data confidentiality. To create the PTK, a pseudorandom function takes place with the access point's MAC address, client MAC address, and a nonce sent from each side as well. This allows a single master key to create multiple session keys without having to re-exchange a new master key each time.

The next key with regard to 802.11i main keys is the group key or group master key (GMK). This key is similar to the PMK except that it is used for beacon and management

traffic encryption. The same process of hashing senders' and receivers' MAC addresses and nonces is used to create a group temporal key (GTK) from a group master key.

Robust Secure Network (RSN)

Robust Secure Network (RSN) was created as part of the 802.11i security standard. RSN specifies user authentication through IEEE 802.1x and data encryption through the Temporal Key Integrity Protocol (TKIP) or Counter Mode with CBC-MAC Protocol (CCMP).

RSN also has the option to use TSN to allow for the use of older security methods such as WEP. RSN uses TKIP and AES as encryption methods to protect the confidentiality of data. The TKIP solution is used for backwards compatibility for legacy devices, and the AES is what RSN is using as a long-term encryption method. AES is set up in Counter Mode with the CCMP. AES can be set up and used in multiple ways, so 802.11i stated that AES must be used in a method called CCMP.

The RSN protocol also uses EAPOL-Key messages for key management. The description below reveals how RSN works with 802.11i in aiding to choose an available authentication method and encryption cipher scheme.

Advertising the cipher suites supported on an access point and client is done through Robust Secure Network Association (RNSA) messages. These messages spell out the supported ciphers of each party and negotiate what method will be used to connect securely. These messages are located inside what is called an RSN IE or an RSN information element.

A RSN IE is used to tell the other devices about what cipher suites the sending device supports. The RSN IE can be sent in a beacon from an access point or in an association request from a client. After an association request, a response will be returned with an RSN IE listing what requesting method matched the method supported by the other party.

The standard allows RSN IE optionally to be inside each of the following management frame types:

- Beacon
- Association Request
- Reassociation Request
- Probe Response

The RSN standard is a method to negotiate what types of security methods each client and each access point supports. These security methods are identified as cipher suites inside the RSN IE frame. These cipher suites allow for the use or non-use of any combination of security methods. This means that a policy could be put into place that negates the use of weaker security methods such as WEP and allows for a choice of TKIP or AES. This gives the architects or designers the ability to create a policy allowing or denying whatever cipher suites they might feel are weak or not needed.

The Transition Secure Network (TSN) is part of the RSN portion of 802.11i. It is used to achieve backwards compatibility with older wireless systems. It was carved out of RSN to provide this backwards compatibility. With RSN, as stated above, it is possible to have a number of authentication and encryption types running on an access point. To make sure that some of the weaker authentication and encryption types were not set up in RSN, they were taken out and considered TSN. This makes RSN more secure and allows an easy way to turn off all the older weak methods. With RSN, if one chooses not to support TSN, WEP will not be included as an option to negotiate between the access point and the wireless client.

Advanced Encryption Standard (AES)

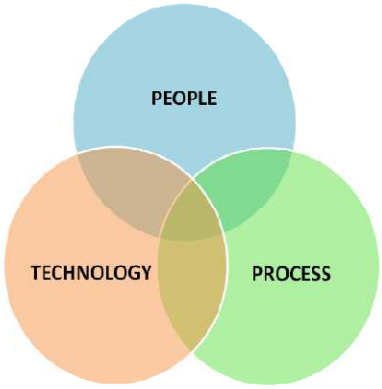
One can apply AES in many different ways. The way that the 802.11i standard has chosen to apply AES is with CCMP, which is based on CBCMAC. CCMP was chosen for data integrity and authentication, with the Message Authentication Code (MAC) providing

the same functionality as the Message Integrity Check (MIC) used for TKIP. AES has several modes. The first term is CTR; this is AES in Counter mode. This mode is used for confidentiality. The next mode is called CBC-MAC, which stands for Cipher Block Chaining Message Authentication mode. This mode is used for integrity. AES also has combined CTR and CBC-MAC to create CCM. CCM is the acronym for CTR/CBC-MAC mode of AES that incorporates both the confidentially of CTR and the integrity of CBC-MAC.

2.4 People, Process and Technology

For SOHO WLAN to be secured People, Process and Technology must be combined. The way these components interact will directly impact the level of security in a SOHO WLAN.

Figure 1: People, Process and Technology



Technology: Technology is the first component necessary for effective SOHO WLAN security management. Most organizations have already deployed an extensive security architecture consisting of Firewalls, Anti-Virus and Intrusion Detection Systems. Unfortunately because of the evolving nature of attacks and the fact that humans are at the root of the attacks, these systems will never provide the absolute prevention desired.

Process: A SOHO WLAN security framework can be used to determine which controls are required for the WLAN to be considered to be operating securely. The

framework can be used to determine which controls that should have been implemented are missing and the risk level of the organization hence the organization can be in a position to make an informed decision as to which controls should be implemented.

People – People are the most important component of an effective security management program. People in the SOHO WLAN must be committed towards the improvement of the security in the WLAN. They should be prepared to work together towards the creation of a secure WLAN. Their roles should be clearly defined. Behind every attack, even ones that are automated are people. The only way to counter these attacks is by deploying an organizations' human talent against it. The SOHO WLAN administrator must have the relevant training in WLAN security for the security management to be effective. Also as time goes on the administrator will have had enough experience to be able know the level of security that an organization should have.

2.5 Securing SOHO WLAN through monitoring of Controls

In today's inter-networked environment, organizations depend heavily on information technology (IT) (Sekar et al, 2009). We use Information Technology to process or store information that is used by organizations to make decisions. As discussed, wireless technologies may empower users with easier and greater access to data at reduced costs and with low access barriers, but these conveniences also leave them vulnerable to data compromise and security breaches. This technology introduces a magnitude of critical security risks and challenges, and it is critical to implement strong security measures to mitigate significant risks (Susan, 2004).

Information fuels business. In every industry—from financial services to manufacturing to healthcare—information reigns supreme (Egan, 2005). Just like any assets, information in a SOHO WLAN needs to be protected from both passive and active attacks. IEEE 802.11 provides for confidentiality, integrity and authentication. However according to

International Telecommunication Union Telecommunication Standardization Sector (ITU-T) standard, X.800, five security services need to be achieved for the system to be considered secure. They are data confidentiality, data integrity, authentication, access control and non-repudiation.

Use of WLANs in an organization can introduce risks. Lack of sufficient policies to govern wireless networks and their use leave unaddressed a number of configuration features and settings (Susan, 2004). Information must remain accessible yet secure. Protecting information, in turn, must become a top business priority rather than just another technology issue (Egan, 2005). One of the activities that will continually be done for the information in the SOHO organization to be secure will be security monitoring.

2.6 Monitoring Technical Computer Security

Information Security Management (ISM) generally addresses two areas, the technical computer security and non-technical security management.

The SOHO organization requires a mechanism to be able to know which security measures are required for the organization to be secure. In his work: A Framework Based on Continuous Security Monitoring (Erturk, 2008) states that as we become more and more interconnected, new threats such as malicious hackers and industrial spies emerge. As business embrace the business opportunities brought about by the internet, IT security is becoming a growing priority for organizations and IT security investment is expected to grow. With other security products, organizations are also employing security standards to enhance their level of security.

As addressed by the IT security standards and regulations, security monitoring is an essential part of the organizational security and security management is not possible when monitoring is absent. Security monitoring is critical to be able to identify control failures before a security incident occurs to detect an intrusion or other security incident in due time

to give an effective and timely response and to support post event forensic activities (Erturk, 2008).

With monitoring, an organization can be able to determine vulnerabilities and threats that can exploit the vulnerabilities. Incidents can be detected early hence preventing or minimizing their impact. Measuring the program compliance level of the system on the basis of employed standards can also be used to enhance security due to the adoption of best practices laid down by these standards. The management will be enabled to make informed decisions. Through monitoring they would be availed with a report on the status of security in the organization.

(Erturk, 2008) intention is to give managers and administrators information regarding the situation and security trends in the organization by proposing a continuous security monitoring framework. He states that security monitoring is required so as to understand how the system is acting.

To enable one to know how well or bad the security situation is, security metrics are necessary. They facilitate decision making since if expressed as cardinal number or as a percentage, they can be used to measure the effectiveness of a specific technology deployed. Security metrics can be used to identify security controls that are implemented incorrectly, not implemented or ineffective.

The Continuous Security Monitoring Framework (CSMF) proposed by (Erturk, 2008) is a security measurement, collection and reporting framework. It is supposed to give an insight to the managers and administrators about the current situation and security trends in the organization. It identifies the security measurements that can be used to gauge the security controls. It involves the collection of information from logs and alerts from a variety of systems such as firewalls, routers and servers and then it collects, organizes and makes sense of what they means. From this measurement it can be possible to know how a control is doing

by defining a metric goal, setting a baseline and target value. If a particular metric when the analysis is done is below the baseline, then a remedial action is needed.

The advantage of this framework is that it makes it easy to capture native log data into easily understood language. The report can be presented using a graph or chart hence the management can easily know the status of the system. Also since it is a continuous monitoring system, there will be improved incident response and policy compliance by allowing security personnel to investigate exception and take immediate action. Lastly the security personnel don't have to stare at a console or logs for length periods of time.

The disadvantage of this framework is that it can be cost prohibitive for small organizations. It may require dedicated servers to be installed. Users of this system will require more training. If the organizations don't have a lot of bandwidth, it can contribute towards network congestion. It can also be difficult to decide of the many events that are there, which are the best.

Although technology and processes represent foundational pieces of a corporate information security framework, a third component is needed to complete the picture: people. It is not just that people make security technology run or that people create and follow critical security policies, procedures and processes. It is that people—that is, having the right people in the right places—can compensate for deficiencies in processes and technology (Egan, 2005). For security monitoring to be therefore effective in keeping risks at bay, the people factor come into play and the key question is: is the SOHO WLAN being operated by people who are aware of the security issues associated with wireless networks?

2.7 The People Factor

(Patil, 2008) Information Security Framework: Case Study of a Manufacturing Organization states that Information Security Management(ISM) encompass people, process

and Information Technology (IT) systems that safeguards critical systems and information protecting them from internal and external threats.

If technology alone were enough to keep an organization secure, Internet threats would be little more than an afterthought for many enterprises. It is not just that people make security technology run or that people create and follow critical security policies, procedures and processes. It is that people—that is, having the right people in the right places—can compensate for deficiencies in processes and technology (Egan, 2005).

As stated earlier Information Security Management (ISM) addresses two areas; (Patil, 2008) framework addresses non-technical security aspect of the information security framework.

The scope of his work focuses on four areas:

- IT Governance and Compliance
- Policies and Procedures
- Impact of Laws and Regulations on the Organization
- Risk Analysis and Assessment

IT Governance is usually the responsibility of executives and board of directors and provides leadership, organizational structures and processes that would ensure that the organization meets its objectives. Since there are many legislative or industry mandates, compliance with the standards laid down is an indicator that an organization will meet its objectives. Policies and procedures ensure that as the organization strive to meet its mandate; it addresses its security related issues. As scandals of organizations misappropriating customer funds continuing to increase, organizations worldwide are impacted by an increasing number of laws and regulations that they must meet. They are also required to identify the risks that might prevent them from attaining their goals and they therefore perform risk analysis and assessment that helps them identify potential threats.

To eliminate business risks, an Information security framework is necessary (Patil, 2008). A comprehensive security framework boils down to three familiar basic components: people, technology, and process (Patil, 2008). When correctly assembled, the people, technology, and process elements of your information security program work together to secure the environment and remain consistent with your firm's business objectives. Only a successful integration of these three elements, people, technology, and process can provide a strong, effective security infrastructure (Reveche, 2005).

Keeping information secure is not only the responsibility of information technology (IT) security professionals, but also the responsibility of all people within the organization. Therefore, all users should be aware not only of what their roles and responsibilities are in protecting information resources, but also of how they can protect information and respond to any potential security threat or issue (Rotvold et al, 2008).

(Patil, 2008) proposes an information security governance framework for action that outlines specific roles for business unit heads, senior managers, CIOs, and the CEOs. The information security framework defines roles and responsibilities for CEO, business unit heads, and senior managers. This is because Information security should not be treated solely as a technology issue, but it should also be treated as a governance issue. Different technology can be used to address the security problem but apart from technology, there should be proper policies, procedures in place which will handle information security issue more appropriately.

(Patil, 2008) framework has the advantage of the fact that if the senior management support the organization’s information security policies, objectives and controls, then meeting security objectives will be easier. If the top management of a SOHO organization appreciate the importance of operating in a secure WLAN environment, then it will be easier for a security administrator to request and to be given the required resource that can be used to

secure the WLAN network. People can be either the weakest or the strongest link in the security chain (Egan, 2005). Making them the latter is possible with executive involvement, the assistance of security professionals, cross-functional corporate input and scheduled independent reviews.

The biggest inhabitant to this framework is the competent level of the information security management team. If they are technically qualified and experienced at managing information security then the framework can work. They do however need to know the risks that face them and how to eliminate or minimize the effects of these risks. This requires risk management.

2.8 Risk Management

Due to the various vulnerabilities in a SOHO WLAN, we need to combine both the technical computer security and non-technical security for the management of the threat sources that might attempt to exploit these vulnerabilities.

To determine the controls required, a SOHO organization requires a risk management plan that is not cost prohibitive; the security administrator should be able to use it easily while providing the right results and should not require a lot of resources such as bandwidth or dedicated servers. The adopted methodology should require minimal training while at the same time providing the management with enough information on the level of security within the SOHO WLAN and where resource are required to mitigate against risks that face the organization.

Information security is not a destination, it is a journey. It is a continuous practice. To achieve a continued success in information security, an organization needs to focus continuously on improving its information security practices as the technology environment keeps changing and new threats arise (Sethuraman et al, 2009).

Since WLANs were not been designed to be secure, the security that can be achieved through technical means is limited, and should be supported by an appropriate risk management plan and procedures. Identifying which controls should be in place for the SOHO WLAN to be secure requires careful planning and attention to detail.

A SOHO organization should identify its security requirements. There are three main sources of security requirements:

1) One source is derived from assessing risks to the SOHO organization, taking into account the organization's overall business strategy and objectives. Through a risk assessment, threats to assets are identified, vulnerability to and likelihood of occurrence is evaluated and potential impact is estimated. The various vulnerabilities and threats to a WLAN have already been discussed. The question that remains is how attacks to the WLAN can be prevented or their impact reduced.
2) Another source is the legal, statutory, regulatory, and contractual requirements that an SOHO organization, its trading partners, contractors, and service providers have to satisfy, and their socio-cultural environment.
3) A further source is the particular set of principles, objectives and business requirements for information processing that an SOHO organization has developed to support its operations.

This study is based on identifying a SOHO WLAN's security requirements from assessing risks to the SOHO organization. To be able to identify the vulnerabilities in a SOHO WLAN, the risks that might exploit these vulnerabilities and controls necessary to eliminate or minimize the impact if an attack is successful, risk management need to be performed.

The principal goal of an organization's risk management process should be to protect the SOHO organization and its ability to perform their mission. A well-structured risk management methodology, when used effectively, can help the management in SOHO organization to identify appropriate controls for providing the mission-essential security capabilities.

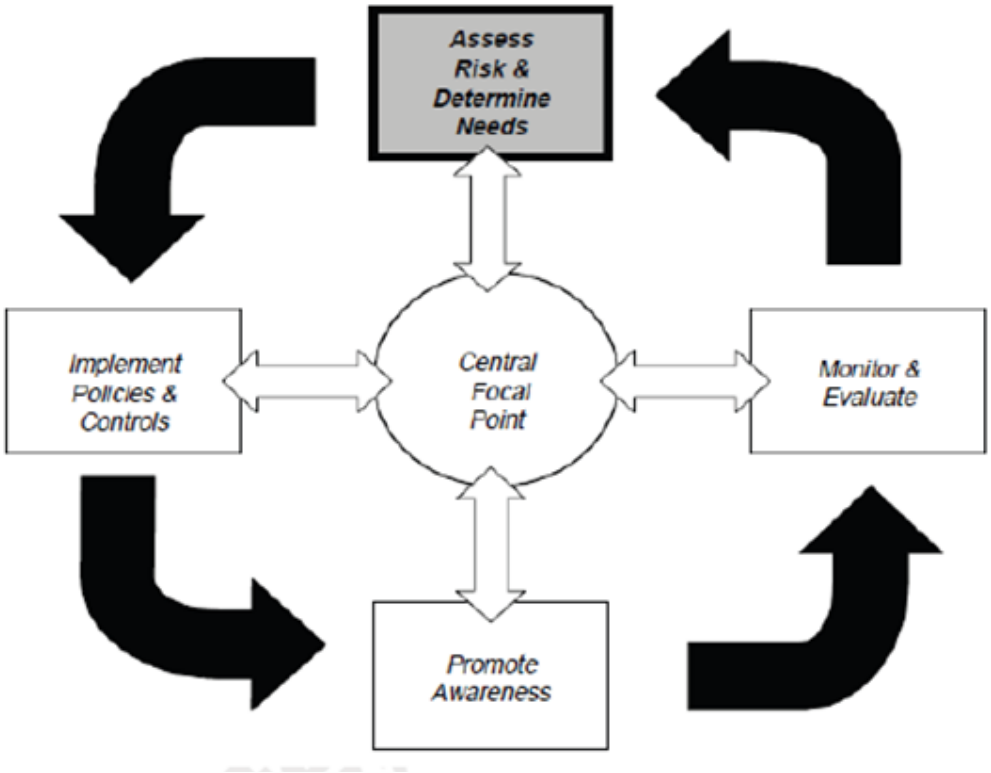
The objective of performing risk management is to enable the SOHO organization to accomplish its mission by better securing the IT systems. The results of this can enable the management in the SOHO organization to make well-informed risk management decisions that can justify the security expenditures that are part of an IT budget.

Risk management encompasses three processes: risk assessment, risk mitigation, and evaluation and assessment.

Risk Assessment

Risk assessment is the first process in the risk management methodology. A SOHO organization can use risk assessment to determine the extent of the potential threat and the risk associated with an IT system. Risk assessment process provides for a risk management cycle with the following items (Peláez, 2010):

Figure 2: Risk Management Cycle



1) In the first stage, the risks to a SOHO WLAN are determined and controls that can reduce these risks determined. The purpose of this stage is to provide a mechanism that can provide the management in a SOHO organization with the information they need to understand the risk factors that may adversely affect the operations and affect the outputs of the company's processes.
2) In the second stage, controls that can mitigate or minimize the risks to a SOHO WLAN are implemented.
3) The third state recognizes the fact that risk to a SOHO WLAN can be properly managed through training. Users of the WLAN should be regularly trained to maintain awareness of risk management policies in the organization.
4) The last stage is monitor and evaluate. This stage is used to determine whether the level of risk exposure to the SOHO WLAN has increased or decreased.

The National Institute of Standards and Technology (NIST) Risk Management Guide for Information Technology Systems, NIST Special Publication 800-30 provides a guide on how to perform risk management. It subdivides risk management into risk assessment, risk mitigation, and evaluation and assessment.

The NIST risk assessment methodology encompasses nine primary steps:

- Step 1: System Characterization
- Step 2: Threat Identification
- Step 3: Vulnerability Identification
- Step 4: Control Analysis
- Step 5: Likelihood Determination
- Step 6: Impact Analysis
- Step 7: Risk Determination
- Step 8: Control Recommendations
- Step 9: Results Documentation

Step 1: System Characterization:

This step consists of describing the SOHO WLAN system; its purpose and mission is to identifying the assets in the SOHO WLAN. The assets can be physical such as buildings and computers and logical such as intellectual property and reputation.

Step 2: Threat Identification:

This step comprise of identifying all the threats a SOHO WLAN can be faced with.

Step 3: Vulnerability Identification:

This step involves identifying all the weaknesses that the SOHO WLAN has that can be exploited by a threat source.

Step 4: Control Analysis:

This step involves identifying all the controls a SOHO WLAN has and all the planned controls analyzing their effectiveness and changing, removing replacing or retaining them.

Step 5: Likelihood Determination:

This involves determining the likelihood of a threat vulnerability pair being realized.

Step 6: Impact Analysis:

This step involves determining the impact of a threat being realized to the SOHO WLAN.

Step 7: Risk Determination:

This step determines the level of risk the SOHO WLAN is exposed to.

Step 8: Control Recommendations:

The controls necessary for the SOHO organization to operate at an acceptable level of security are determined.

Step 9: Result Documentation:

The output of risk assessment can help the security administrator in the SOHO organization to identify appropriate controls for reducing or eliminating risk.

Controls needed to be implemented in the organization needs to be balanced against the business harm likely to result from security failures. The results of the risk assessment will help to guide and determine the appropriate management action and priorities for managing information security risks, and for implementing controls selected to protect against these risks.

Once security requirements and risks have been identified and decisions for the treatment of risks have been made, appropriate controls should be selected and implemented to ensure risks are reduced to an acceptable level.

Information security controls are an important component of an organization's internal control structure. Safeguarding and monitoring a company's data and information assets are essential parts of information security controls (Lin et al, 2011).

Becoming more knowledgeable about and familiar with the information security controls that are currently being implemented within organizations, one can make a more informed attempt to establish organizational guidelines for companies striving to effectively manage information security.

Controls can play an important role in managing risks in a SOHO organization. The adoption and application of a security framework based on controls by the organization can play a significant role in information security management. ISO 27002 Information technology—Security techniques—Code of practice for information security management is an international standard from the International Organization for Standardization (ISO) that establishes guiding principles and benchmarks for creating, implementing and sustaining information security management in an organization.

ISO 27002 contains a list of control objectives and specific controls that organizations around the world are using as practical guidelines to manage information security (Lin et al, 2011). It basically outlines hundreds of potential controls and control mechanisms, which may be implemented in an organization. It has a list of best practice controls that can be implemented by an organization.

The advantages of using ISO 27002 is that it is a globally recognized Information security standard hence the management in the SOHO organization can be more assured of the quality of a system. It is a well defined security standard from International Organization for Standardization (ISO) hence the compliance methodology helps building the SOHO organization's client confidence which is key business driver. Compliance with it can provide a bench mark for both the current position and future progress. Lastly it provides best practices recommendation on information security management.

The controls in this standard can be used in a SOHO organization to mitigate risk for the better protection of mission-critical information and the IT systems that process, store,

and carry this information. However before implementing the controls, a risk assessment process which is one of the three processes in risk management needs to be performed.

Risk Mitigation

In risk mitigation, the management in the SOHO organization makes decisions on how they can reduce the risks to the WLAN. There several options:

- Risk Assumption. The SOHO organization can accept the potential risk and continue operating the WLAN or to they can implement controls to lower the risk to an acceptable level
- Risk Avoidance. The SOHO organization can avoid the risk by eliminating the risk cause and/or consequence. They can forgo certain functions of the system or shut down the system when risks are identified.
- Risk Limitation. The SOHO organization can limit the risk by implementing controls in the WLAN that minimize the adverse impact of a threat's exercising a vulnerability. They can implement supporting, preventive, detective controls.
- Risk Planning. The SOHO organization can manage risk by developing a risk mitigation plan that prioritizes, implements, and maintains WLAN security controls.
- Research and Acknowledgment. The SOHO organization can decide to lower the risk of loss by acknowledging the vulnerability or flaw to the WLAN and researching for controls that can correct the vulnerability
- Risk Transference. The SOHO organization can transfer the risk by using other options to compensate for the loss, such as purchasing insurance.

Evaluation and Assessment

The risk management process is ongoing and evolving process. With continued operation of the SOHO WLAN new risks will surface and risks previously mitigated may again become a concern. The risk management process will therefore have to done all over again after some time.

The weaknesses of the WLAN are well documented. The vulnerabilities in this system are well known and the technical controls that can be used to prevent or minimize the probability of a threat source exploiting a vulnerability have been found to be not efficient. Information security covers the three major components: people, process and technology (Tsang, 2005). IEEE 802.11 only addresses the technology aspect. This framework intends to bring together people and processes in the management of SOHO WLAN security. It intends simplify the management of security in a SOHO WLAN by providing a tool that the security administrator can use to determine which controls in the SOHO WLAN are missing and which ones require attention hence enabling the management to know where to spend their IT resources in providing cost-effective safeguards that meet the security needs of the organization.

Chapter 3

3.0 SOHO WLAN Security Framework

A security administrator requires a framework that can enable him to determine which controls in the SOHO WLAN organization to implement and the impact to the organization if a threat agent is to exploit a vulnerability if the controls are not implemented.

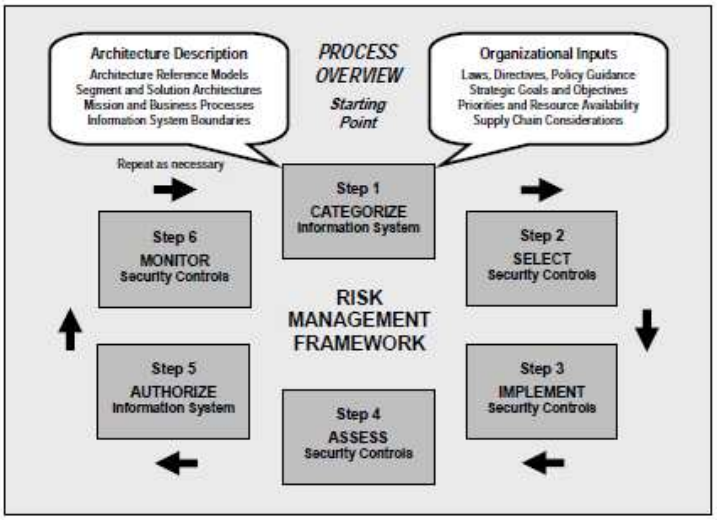
The National Institute of Standards and Technology (NIST) Special Publication 800-37 has a risk management framework that can be used as a guide for applying the risk management framework to Federal Information Systems (RMF).

The purpose of this publication is to provide guidelines for the security certification and accreditation of information systems supporting the executive agencies of the United States federal government.

Security certification and accreditation are important activities that support a risk management process and are an integral part of an agency's information security program. Security accreditation is the official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations, agency assets, or individuals based on the implementation of an agreed-upon set of security controls.

The figure 3 below shows the six steps in that framework.

Figure 3: NIST Special Publication 800-37 Risk Management Framework



1. **Categorize** the information system and the information processed, stored, and transmitted by that system. One should define criticality /sensitivity of information system according to potential impact of loss.
2. **Select** an initial set of baseline security controls for the information system based on the security categorization; tailoring and supplementing the security control baseline as needed.
3. **Implement** the security controls and describe how the controls are employed within the information system and its environment of operation.
4. **Assess** the security controls using appropriate assessment procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
5. **Authorize** information system operation based on a determination of the risk to organizational operations and assets, individuals, other organizations, and the Nation resulting from the operation of the information system and the decision that this risk is acceptable.

6. **Monitor** the security controls in the information system on an ongoing basis including assessing control effectiveness, documenting changes to the system or its environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to designated organizational officials.

From this framework we were able to create the SOHO WLAN Security Framework. It also consists of six steps.

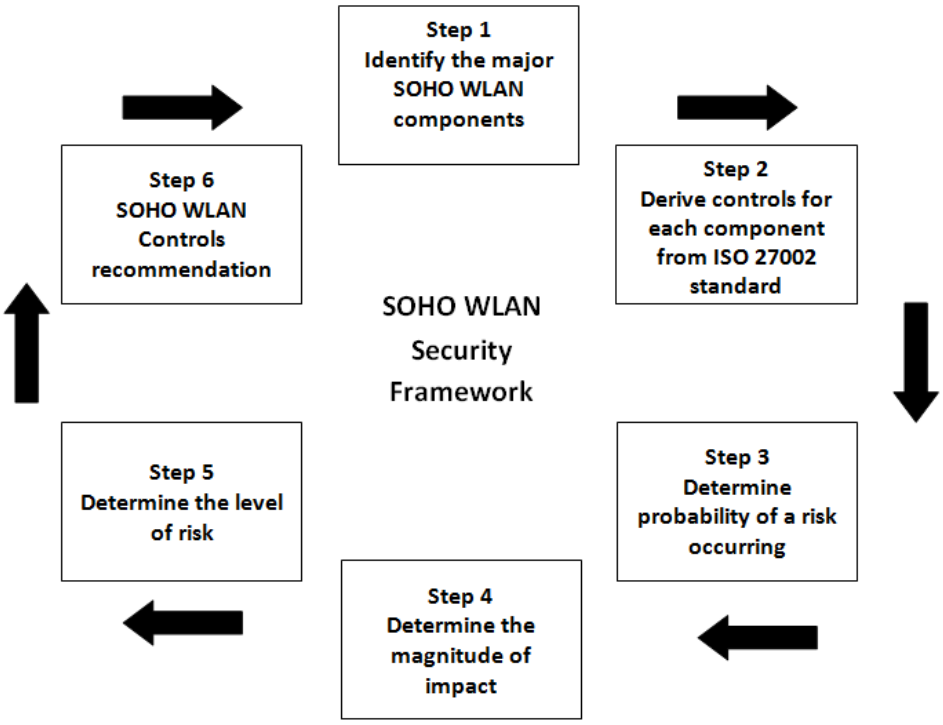
1. **Step 1:** Identify the major SOHO WLAN components. This is to simplify risk management. One can focus on one component, make sure that the risks have been managed to a level acceptable to the management, and then proceed to the next component.
2. **Step 2:** Derive controls for each component from ISO 27002 standard. For each component, we were able to determine the controls that are necessary. When the SOHO WLAN is implemented and some controls are omitted may be due to lack of resources, a vulnerability will have been created.
3. **Step 3:** Determine probability of a risk occurring. If some controls are omitted in a particular component, the chances of a threat source exploiting this vulnerability will have to be determined.
4. **Step 4:** Determine the magnitude of impact. The impact to confidentiality, integrity and availability due to lack of controls in a particular component will have to be determined. If high, then the management will have to be advised on the need of using the organization's resources in implementing the necessary controls.
5. **Step 5:** Determine the level of risk. For all the components, the level of risk that the organization is exposed to due to the fact that controls are missing will have to be determined. If the level of risk to the organization is low, an attack is unlikely to

occur, medium, an attack may or may not occur and high, an attack is expected to occur.

6. **Step 6:** SOHO WLAN controls recommendation. The findings from step five are presented to the management, and by this the level of risk exposure to the SOHO WLAN organization is know by the decision makers. If the level is high, they can choose to employs resources to reduce the risk or they can accept the risk and continue operating.

Figure 3 below shows the SOHO WLAN security framework:

Figure 4: SOHO WLAN Security Framework



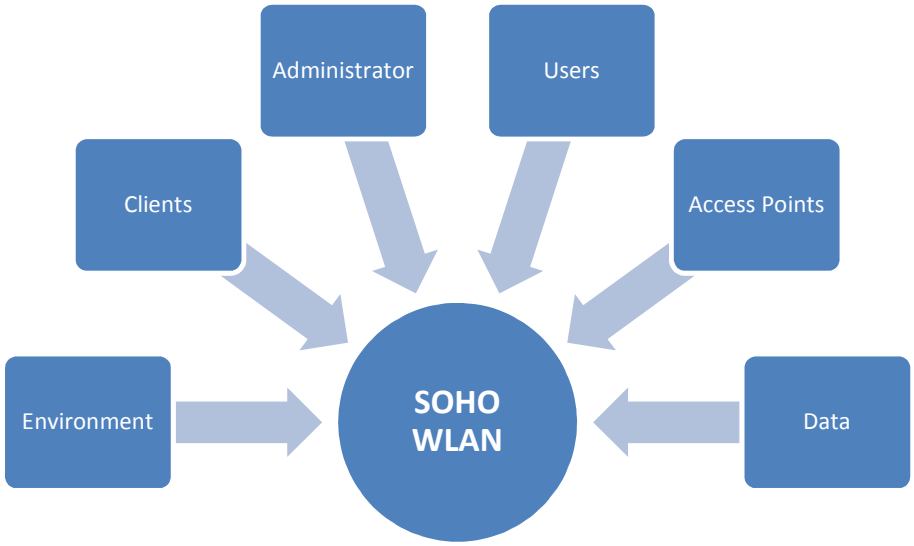
Step One: Identify the major SOHO WLAN components

We were able to identify that a SOHO organization consist of:

1. Data
2. Access Points (AP)
3. Client Machines (Clients)

4. Administrators
5. Normal Users (Users)
6. The WLAN Environment (Environment)

Figure 5: Components of a SOHO WLAN Organization



As figure 4 shows the SOHO organization requires *Data* to make its decisions. This data is generated by *Users* in the various departments of the SOHO organization and they use wireless *Client* devices such as servers, PC, and Laptops to process and store the information. An *Access Point* enables communication to be possible wirelessly among the various wireless client machines in the organization. The *Administrator* ensures that the WLAN operates smoothly and securely. Therefore the *Environment* in which these components operate on should be secure and through the SOHO WLAN security framework, it is hoped that this can be achieved.

Step two: Derive controls for each component from ISO 27002 standard

After the SOHO WLAN environment was subdivided into six logical components, the necessary controls for each of these components were then derived from ISO/IEC 27002 standard.

For each component controls were chosen as shown in appendix B. The subdivision of the WLAN into six logical components and the laying down of the controls that were deemed necessary for each component of the SOHO WLAN to be considered to be operating securely are supposed to provide guidance to a SOHO WLAN administrator on how the WLAN can be secured.

By implementing these controls the SOHO organization will be in a position to minimize or eliminate the likelihood of a threat agent exploiting a weakness in the WLAN system. When the SOHO WLAN is being configured, the administrator can use the SOHO WLAN security framework as a guide regarding which controls are required for each component. The administrator will also need to know what the impact would be if he left out some of the controls. Through risk likelihood and impact analysis, the administrator can be able to know the level of risk his organization is exposed to due to lack of these controls.

Step three: Determine probability of a risk occurring

The SOHO WLAN administrator uses this stage to determine the probability of a risk occurring in the SOHO WLAN due to lack of some controls. As the administrator undertakes to install the SOHO WLAN he wants guarantees that this will be done successfully. He wants assurances that it will be run securely. He would want to know what the impact would be if some controls are not implemented. However before he can know the impact, he needs to know the likelihood of a threat source exploiting a vulnerability due to lack of the controls. For each control in the SOHO WLAN framework, the risk likelihood can be described as:

a) Very High: An attack will certainly occur if the required control is not there. An attack is expected to occur in most circumstances as there is a history of regular occurrence.
b) High: An attack is expected to occur in most circumstances. There is a strong possibility the attack will occur as there is a history of frequent occurrence.

c) Moderate: The attack might occur at some time as there is a history of casual occurrence.

d) Low: Not likely to occur. There's a slight possibility of an attack occurring at some time.

e) Very low: an attack is highly unlikely to occur, but it may occur in exceptional circumstances. It could happen, but probably never will.

After determining the likelihood of an attack occurring, the SOHO WLAN administrator would like to know what the impact will be.

Step four: Determine the magnitude of impact

In this stage the administrator is able to determine how much the SOHO WLAN organization would be affected in case an attack occurred.

The impact can be impact to SOHO organization's customer service, internal operations, financial loss and legal requirements. The impact can be a temporary loss of revenue to SOHO organization or going out of business.

Impact can be in terms of:

a) Impact upon confidentiality: unauthorized, unanticipated or unintentional disclosure could result in loss of public confidence, embarrassment, or legal action against the SOHO organization.

b) Impact upon integrity: Integrity is lost if unauthorized changes are made to the data or the system by either intentional or accidental acts. If the loss of system or data integrity is not corrected, continued use of the contaminated system or corrupted data could result in inaccuracy, fraud or erroneous decisions. Violation of integrity may be the first step in successful attack against system availability or confidentiality.

c) Impact upon availability: If a mission critical system is unavailable to its end users, the SOHO organization's mission may be affected. Loss of system functionality and

operational effectiveness may result in loss of productive time, impeding the end user's performance of their functions in supporting the SOHO organization's mission.

The magnitude of impact can be:

a) Very High: SOHO WLAN is completely unable to operate.
b) High: The SOHO WLAN cannot meet its objectives. There is loss of credibility and confidence in organization.
c) Moderate: We have limited damage to reputation of the SOHO organization.
d) Low: Impact on the SOHO organization is rapidly absorbed. There is no long term consequences
e) Very low: There is minimal disruption to routines in SOHO organization.

After determining the risk likelihood and the impact, the administrator would like to know the level of risk to the SOHO organization. A risk matrix is used to determine this.

Step five: Determine the level of risk

The purpose of this step is to determine the level of risk to the SOHO WLAN organization. Through a 5X5 risk level matrix the administrator would be able to determine risk ratings by multiplying threat likelihood and threat impact.

The risk rating can be categorized can as:

a) High: Risk event is expected to occur. No strategy is available in the SOHO organization to counter the risk event occurring. A high level of management attention is necessary because corrective action plan must be put in place a soon as possible.
b) Medium: Risk event may or may not occur. However corrective actions are needed and a plan must be developed to incorporate these actions within a reasonable period of time.

c) Low: Risk event is less likely to occur. The management can decide to put corrective actions or accept the risk.

The output of this process can help the administrator in the SOHO organization to advice the management on the importance of using the organization's resources in implementing controls to reduce the level of risk exposure the organization is exposed to.

Step Six: SOHO WLAN controls recommendation

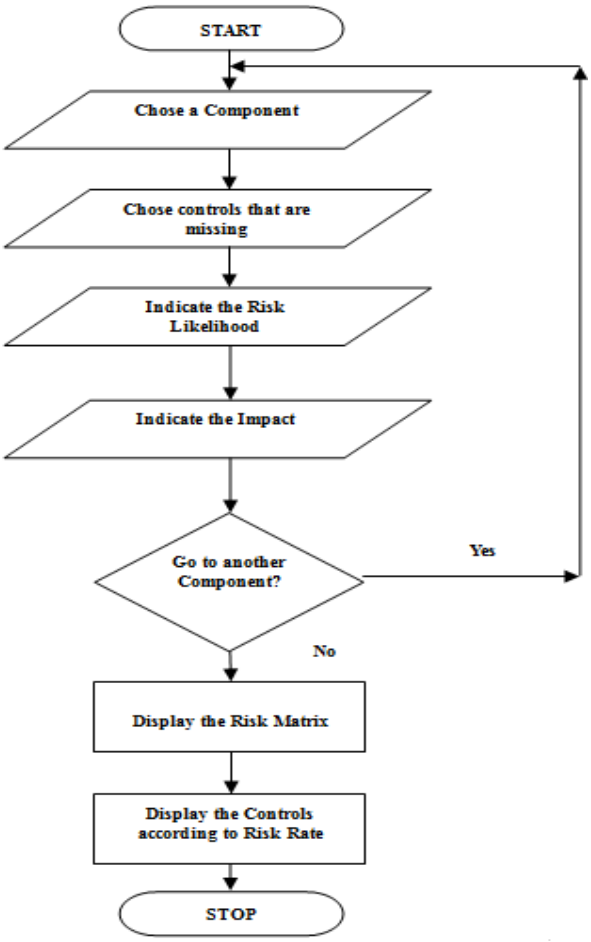
Recommendations on how to reduce the level of risk exposure to the SOHO WLAN organization are tackled in this section. All the controls missing for the various components are presented to the management according to their risk rating. The management of SOHO organization is expected to make decisions on how to reduce the risks to an acceptable level. The choices are:

a) Mitigate the risks in the SOHO WLAN environment: This involves using organization's resources in implementing the missing controls until the risk is at a manageable or acceptable level.
b) Accepting the risk: This occurs in cases where the SOHO WLAN management chose to deal with the impact since they see it to be cheaper than overcoming it.
c) Transferring the Risk: the SOHO WLAN management can for instance chose to buy insurance cover to cover the risk.

3.1 Software Implementation of the SOHO WLAN Security Framework

A program was created using Visual Basic 2010 that can enable a SOHO WLAN administrator to setup a secure SOHO WLAN and also run it securely. The main components of the program are shown in the flow chart below:

Figure 6: Software Implementation of the Framework



A section of the code for the program is shown in the appendix D.

3.2 Field Implementation of the Proposed Framework

A field implementation of the program developed was done. From Communication Commission of Kenya we were able to get a list of organizations that use WLAN and from this list, we were able to survey 13 SOHO WLAN organizations in Nairobi. The survey is shown in Appendix A

The survey had 12 items. The first part of the survey consisted of 8 items. In this part we wanted to find out what the level of security awareness was in the organization. The

second part consisted of 4 items. This part was used to determine the perception of the SOHO WLAN organizations towards the framework.

Senior management's commitment to information security initiatives is the single most critical element that impacts an information security program's success (Bowen et al, 2007). The first question was used to determine management's commitment towards SOHO WLAN security. Ultimate responsibility for managing information security is borne by corporate management, which provides the resources and sets the requirements on the basis of which the IT security manager promotes and coordinates security activities (Kajava et al, 2006). They are the decision makers.

The second question wanted to find out whether roles and responsibilities are clearly spelt out in the organization. Managers who 'own' their management reports and action them well are able to provide justified assurance to CEOs and CFOs on the condition of the enterprise. The reverse—unsuitable or irrelevant management reporting—poses the question as to how the managers manage if they are wholly or partly uninformed (Parkes, 2006).

Information technology has become part of the business and without it organizations will be unable to meet their business functions. It's key towards achievement of business objectives. The third question wanted to find out whether the management in the organization is aware of the importance of information technology towards the achievement of their business needs.

The information security program brings structure and governance to the information security function within an organization. This structure and governance allow the information security organization to function as a key element within the enterprise to support its business goals (Pironti, 2005). The fourth question was concerned with identifying the security structure in the organization. If there is a well defined structure, then the probability that the

organization is employing proper security practices are high. They are aware of the vulnerabilities present and more likely to spend resources towards providing security.

An information security program involves the overall combination of technical, operational and procedural measures and management structures implemented to provide the confidentiality, integrity and availability of information based on business requirements and risk analysis. An information security program depends heavily on the processes established as a result of information security governance efforts in the organization (Sethuraman, 2006). Establishing an IT Security Program is not a one-time event, but an ongoing venture that follows a cyclical process. The fifth question wanted to find out how security is implemented in the organization. After security measures have been put in place, are they reviewed to ensure that they still meet their obligations?

The sixth question wanted to discover whether the organization had a security framework hence be in a position to provide reliable results on the performance of the SOHO WLAN security framework.

In the event that an attack occurs the impact for instance to the reputation of the organization should be known. Question seven wanted to determine whether the organization is concerned with what the impact would be if an attack was successful. If so, the management will be more willing to spend resources towards reducing the risk exposure.

With the rising cost and increasing frequency of data security breaches, companies are starting to reevaluate how they protect their data (Mattsson, 2011). Question eight wanted to determine whether the organization closely studies a security product before spending money on it. Do they determine the benefits of the security solution with cost? What other solutions are out there.

For a long time, simply having tools to do the job was sufficient. Security managers were so caught up with the latest threat that they could not take time to stop and think about whether these tools were doing the best job, what this means to the business and what they would do with them in the long term (Pauls, 2005). Question nine was used to determine whether the control framework when compared to others provide reliable results in a timely manner.

A security solution should be easy to use while performing its intended task correctly. The framework should not be too complex or sophisticated for the user, the menu structure should be simple to use and the results should be easily accessible for reporting and analyzing. Question ten was used to determine this.

Staying ahead of the bad guys is not an easy task; doing so requires organizations to deploy security strategies that protect all sensitive data fields across the entire enterprise (Mattsson, 2011). Since the SOHO WLAN security framework has subdivided the WLAN environment into 6 logical components and used controls from a recognized standard, ISO 27002 standard, question eleven wanted to determine whether the framework provides the right results in a short period of time. As one goes through the process does it make it easy to know which controls are missing and whether the organization needs to spend its resources on those controls?

Today business is more tactical; the decision makers examine the value proposition toward controlling the enterprise's IT risk (Sathiyamurthy, 2008). The cost spent on a security product should be justifiable. The product should meet the expectations of the organization. Question twelve was used to determine whether the framework provided satisfactory results hence an organization can spend its resources on it.

The screen shots of the application are shown in appendix C.

Chapter 4

4.0 Discussion of the results

Level of Security Awareness in the SOHO WLAN Organizations

Senior management has to recognize that the integrity of the enterprise depends on their commitment to information security and set the example for the organization. It is important to note that management commitment does not guarantee success, but its absence will certainly increase the likelihood of failure (Lee, 2001).

Of the 13 organizations selected for the survey, all of them indicated that their organization's top management considered information and technology to be one of the key pillars towards achieving their goals and are aware of the need to provide full supports towards protecting the WLAN from attacks.

In regards to the individual concerned with approving their security policy, 86% indicated that the manager of IT department or head of the IT department is the one who provides the direction in formulation of security policy. 4% of the organizations contacted indicated that they had a security administrator who is responsible of the security policy.

Due to limited resources many SOHO WLAN organizations, 86%, contacted have an IT Manager who performs all of the functions regarding the setting up and operation of the WLAN. The IT manager has to take many roles including how to effectively manage the WLAN, how to successfully setup a secure WLAN, trouble shooting among others. A SOHO WLAN Security framework can therefore aid this manager in setting up and running a secure WLAN. For the 4% that have a security administrator, the administrator would appreciate a framework that have subdivided the WLAN into components, indicates which controls are necessary for each component and be able to determine the level of risk the WLAN is exposed to if some of the controls have not been implemented.

In relation to what drives spending on security initiatives, 31% indicated that it was from security breaches from external sources. For instance they would install antivirus software and regularly update it mostly when the viruses become unbearable or attack a critical system. 31% indicated it was due to improved business practices. They regularly perform risk assessment to gauge whether the WLAN is able to meet its objectives and act accordingly. Some organizations, 31% indicated that they were driven by Industry standard and frameworks and adhered to what is stipulated in those standards. 8% indicated the protection of brand or institutional image as the driving force.

When it comes to information security structure in their organization the majority, 62%, indicated that staff within the organization with a secondary job function of information security handled IT security. They did not have an individual whose sole purpose is WLAN security. An individual would both manage the WLAN and its security as well. 31% indicated that they had dedicated staff within the organization whose primary job function is information security. The individual had the required skills and certifications to manage WLAN security. 8% said they seek outside experts and outsourcing agreements on a yearly basis. The consultant would advice on what was lacking and they would implement it.

On the question on how the security is implemented, 23% indicated that although they have some security in place, they react to threats as they arise. They did not have risk management processes in place hence did not have data regarding their risk exposure. 46% had products in place such as security frameworks and train staff where they perceived there were weaknesses. They said they encourage their staff to take security certification courses. Another 23% asses their IT systems in terms of risk to attack and loss in the event of compromise and focus resources according to that assessment. 8% conduct yearly risk assessment using an external consultant and followed the recommendations of the consultants.

In regards to whether they use a security framework or standard for governance and management of enterprise IT assets and services, 54% said yes, while 46% said no. Most of those who used a security framework said the most popular was Control Objectives for Information and Related Technology (COBIT). The security administrators or managers indicated that they had Certified Information Systems Auditor (CISA) certification and could therefore implement COBIT. The other 46% said they relied on the technological security on the devices used in the WLAN.

For IT problems/incidents experienced in the last 12 months, 38% had experienced other problems not listed. The problems were mainly attacks by viruses and other malicious software. Where else network failures occasionally occurred, they stated that the problem was corrected quickly before it could severely affect the organization. 23% indicated that they had incurred unexpected expense and customer satisfaction affected. Most indicated that they didn't have back up power supply and in power blackouts they could not meet their business objectives, they lost revenue due to this and since the customers were not served, customer satisfaction was reduced. 8% said their reputation was harmed in cases where there was long power outage.

When it comes to qualities of a security product or technology 62% indicated performance. With performance they indicated the need for the security product that can ensure that the WLAN data is not viewed by unauthorized entities, the security product ensures the WLAN is available when it is required and that the data processed and transmitted is always secure, it cannot be easily intercepted or modified. 23% indicated ease of use. With ease of use they required a product that is easy to use while providing reliable results. They said the security product should be easy to learn and it should be easy to interpret the results. They said the interface provided should be easy with all the tools in well laid out menus. When it comes to integration with existing networks and hosts, 15% said they

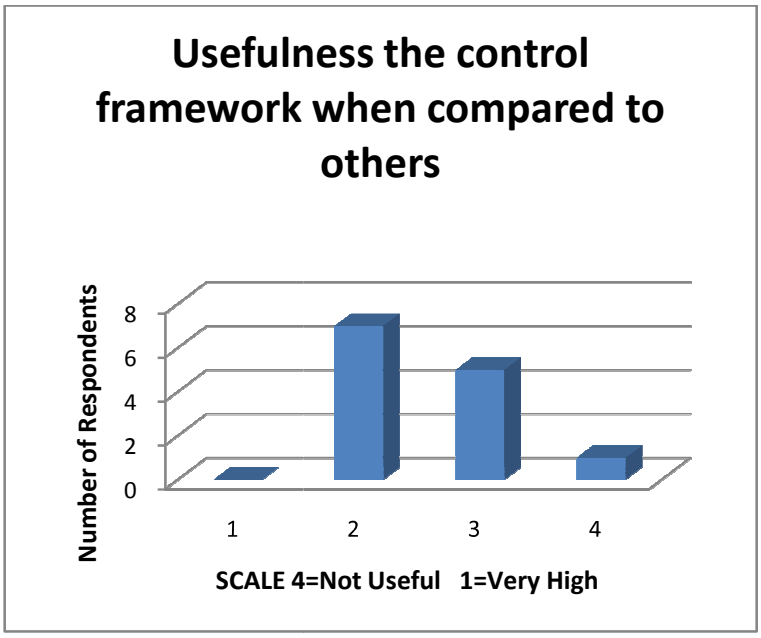
would like a product that easily integrates with the technological security in the network and host machines hence supplementing what is already there. The security product should not be platform dependent.

Performance of the SOHO WLAN Security Framework

The second part of the survey wanted to find out how the SOHO WLAN security Framework was perceived in terms of aiding the management of security in a SOHO WLAN organization. The results were translated to a four-point Likert scale (i.e. 4- Very High, 3- High, 2- Moderate and 1-not useful) to rate their level of importance.

Usefulness the control framework when compared to others

Figure 7: Usefulness the Control Framework

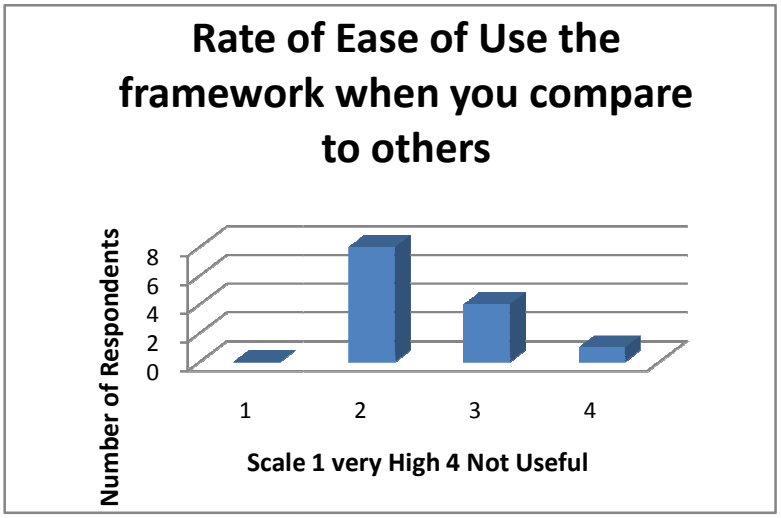


55% said that is highly useful. The framework organizes the controls needed nicely on each component, and then the user indicates for each component the controls missing. Through the use of risk likelihood and impact analysis, one was able to know the level of risk of the SOHO WLAN. All of these steps followed an easy to understand sequence of steps. The report generated could be made available to the management for them to be aware of the

organization's level of risk. 43% said it was moderately useful. The reason was that the framework is controls based. They indicated that they use other means of gauging the security level such as the amount of viruses captured by antivirus software and the performance of the firewall. 2% said it was not useful because they do not use security frameworks in their organization.

Rate of Ease of Use the framework when you compare to others

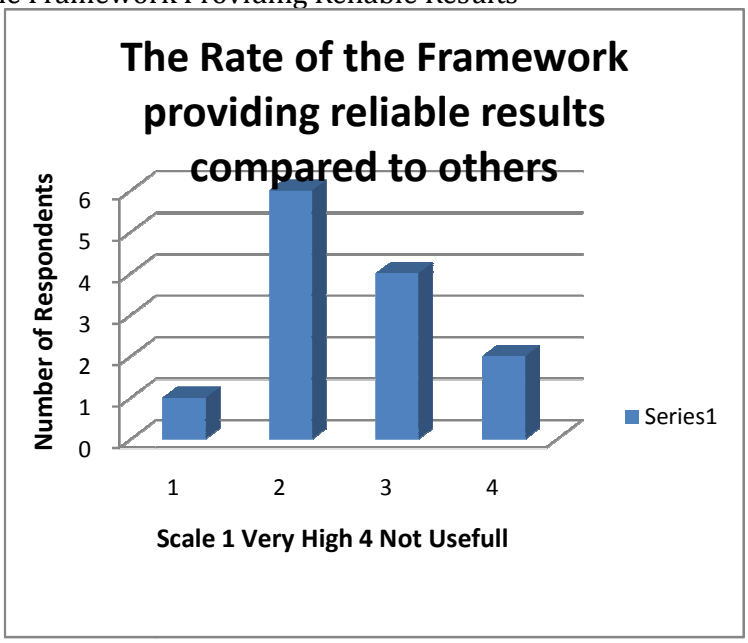
Figure 8: Rate of Ease of Use the framework



When it comes to ease of use of the framework, 60% found it highly easy to use. The interface it provided was easy. The logical components enable one to concentrate on one area before moving to the next, ensuring each area had the relevant controls. The report generated at the end was useful and easily understood with the three levels of high risk, medium risk and low risk enabling one to know whether urgent action was need or not. 35% said they found it moderately easy to use. They stated that the controls were many and not all were known to them and with time it can become easy to use when one thoroughly understands the importance of each control. 5% found it difficult to use. They stated that the use of risk matrix to determine the level of risk for an organization was a bit difficult to use because their security solutions are not wholly based on controls.

The Rate of the Framework providing reliable results when you compared to others

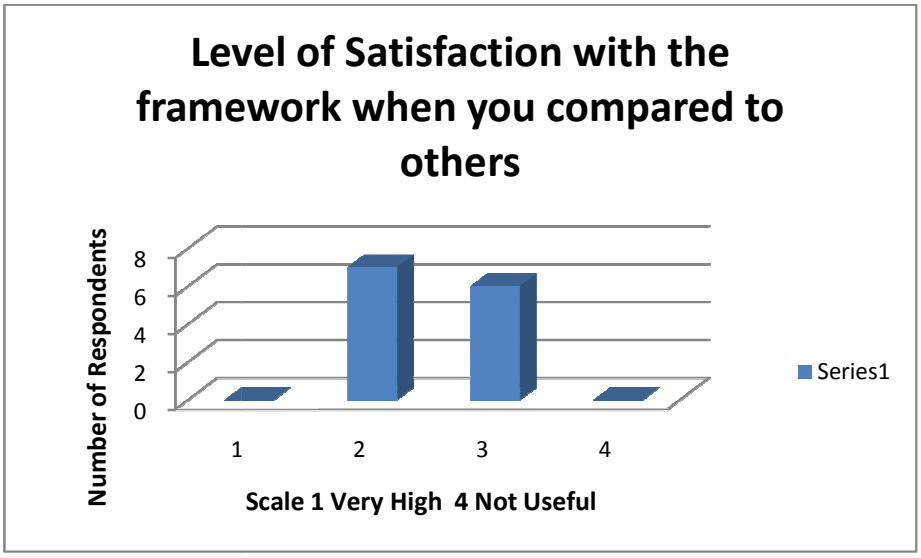
Figure 9: Rate of the Framework Providing Reliable Results



In terms of ease providing reliable results, 57% said it highly provided reliable results because it is based on the international standard, ISO 27002. Thorough testing of the framework would however make the framework more acceptable. The use of NIST Special Publication 800-30 risk management process and NIST Special Publication 800-37 risk management framework in coming up with the SOHO WLAN Security Framework also gave these organizations confidence with the framework. They were more willing to trust the results provided and act accordingly. 36% said it moderately provides reliable results. The reason was due to lack of thorough testing of the SOHO WLAN Security Framework. 7% said it does not provide reliable results because it only measured security on the basis of controls. They indicated that in their organization, they relied on technological security and it was sufficient in ensuring that the SOHO WLAN met its objectives.

Level of Satisfaction with the framework when you compared to others

Figure 10: Level of Satisfaction with the Framework



53% said they were highly satisfied with the framework. They stated that it was easy to use, the sub division of the WLAN into 6 logical components made it easy to know which controls are needed and through risk management, it was possible to know the level of risk of the organization if some of the controls were not implemented. The interface provided also made it easy to use while the report generated made it easy for the organization to know its level of risk and whether resources were required to put additional controls in place. 46% said they were moderately satisfied with the framework. While they indicated that the framework could be used to manage WLAN threats, the frameworks that they have in place such as COBIT was thoroughly tested hence they had more confidence in it. Also it has been operational for a long period of time and revised regularly. They indicated that with time and thorough testing the SOHO WLAN Security framework can become accepted. 1% said the framework was not useful. They said the SOHO WLAN Security framework has not been approved by any recognized organization hence they could not trust it.

Chapter 5

5.0 Conclusion

From the study it has become clear that for a SOHO WLAN organization to meet its objectives and operate securely, the three tenets of security; confidentiality, integrity and availability must be achieved. This requires a SOHO WLAN Security Framework that comprehensively covers all the area in the organization.

By subdividing the SOHO organization in to 6 logical components and deriving the controls needed for each component from the international standard ISO 27002, we were able to greatly simplify the management of security in the organization. The administrator can easily and quickly determine the level of security within the organization and presents the results to the management for further action.

In a SOHO WLAN technological security is not enough. Organizations often rely on enforcing information security policies and implementing controls to safeguard their physical and information assets (Lin et al, 2011). The base or the foundation of an information security program needs to be accepted in the information security industry and applicable to the organization's environment (Sweren, 2006). Due to the fact that the SOHO WLAN Security Framework was based on NIST Special Publication 800-30 risk management process, NIST Special Publication 800-37 risk management framework and ISO 27002, the controls chosen for each component give confidence to the WLAN Organizations contacted that the risk management process was done in a professional manner.

Security management in a SOHO WLAN can be a daunting task. The SOHO WLAN Security framework was able to decrease the complexity of implementing security controls because the WLAN was categorized into six logical components and the administrators in the SOHO just needed to know which controls goes with which components.

In situations where controls were missing for a particular component the use of a risk matrix to determine the organization's level of risk enabled the SOHO WLAN administrator to know which part of the SOHO WLAN environment required urgent attention hence where to spend resources. By presenting the results grouped according to their impact to the SOHO organization it made it easier to convince the management on the need to spend the organization's resources in implementing the required controls.

Use of the SOHO WLAN security framework could also be eventually used to provide to a benchmark against a SOHO WLAN organization's competitors and to provide relevant information about IT security such as the risk level to vendors and customers hence provide assurance that the business functions are operated in a secure environment.

5.1 Recommendation

The study concentrated on WLAN security. Security for the data in the various storage locations such as databases should be looked into in a different study.

Also, there is generally lack of information on the adoption and use of WLANs in Kenya. A study should be undertaken on its impact to the Kenyan economy.

5.2 Future Work

While we have concentrated on infrastructure wireless networks, we have left out security in ad hoc wireless networks. Computing devices are becoming more and more portable with the capability of accessing the network wirelessly. In future, there is a possibility that ad hoc wireless networks will be in wide spread use. Therefore security of ad hoc wireless networks will be a key concern.

References

Cunt M White. (2011). Data Communications & Computer Networks, A Business User's Approach.

Professor Jaya Prasad. (2007). Wireless Security, Myth or Reality.

Hui Du, Ph.D., and Chen Zhang, Ph.D. (2006). Risks and Risk Control of Wi-Fi Network Systems.

Hui Pan. (2007). Wi-Fi/WLAN monthly newsletter.

Hui, Ph.D and Chen Zhang, Ph.D. (2006). Risks and Risk Control of Wi-Fi Network Systems.

James Bindseil. (2003) Wise Wireless: Securing the WLAN.

Mitchell Ashley. (2004). A Guide to Wireless Network Security.

S. Srinivasan. (2006). Information Security Policies and Controls for Trusted Environment.

Hui Lin, Ph.D, Meghann Abell Ceferatti, Ph.D and Linda Wallace, Ph.D. (2011). The prevalence of Information Security Controls: Perspective from IT Auditors.

Mike Garber. (2010). A higher Level of Governance-Monitoring IT Internal Controls.

Bruce Busta Ph.D, CISA, Kris Portz Ph.d, CPA, Joel Strong, Ph.D, CPA, and Roger Lewis CPA. (2006). Expert Consensus on the Top IT Controls for a Small Business.

Sia Sie Tung , Nurul Nadia Ahmad, and Tan Kim Geok. (2006). Wireless LAN Security: Securing Your Access Point.

Ahmed M. Al Naamany , Ali Al Shidhani, Hadj Bourdoucen. (2006). IEEE 802.11 Wireless LAN Security Overview. International Journal of Computer Science and Network Security.

Fred Gallegos. (2003). IT Audit Independence: What Does It Mean?

Vicente Aceituno Canal. (2008). Usefulness of an Information Security Management Maturity Model.

Hui Lin, Ph.D, Meghann Abell Cefaratti, Ph.D, Linda Wallace, Ph.D. (2008). The Prevalence of Information Security Controls: Perspectives From IT Auditors.

Christina Tsang-Reveche, CISA, CISM, PMP. (2005). Surviving Security—How to Integrate People, Process and Technology.

Susan Kennedy, CISA, CIW. (2004). Best Practices for Wireless Network Security.

Mark Egan. (2005). Information Security and the Human Factor.

Gary Hinson. (2003). Human factors in information security.

Rotvold Glenda. (2008). How to create a security culture in your organization.

Christina Tsang-Reveche, CISA, CISM, PMP. (2005).

Surviving Security—How to Integrate People, Process and Technology review.

Manuel Humberto Santander Peláez. (2010). Measuring effectiveness in Information Security Controls.

Sekar Sethuraman, CISA , CISM , CGEIT , CIA , CISS P, PMP, CS QA, CVA, Alagammai Adaikkappan, CISA , CISM , ACA , LCS . (2009). Information Security Program: Establishing It the Right Way for Continued Success.

Scott H. Sweren, , CISM, CISSP, PMP. (2006). ISO 17799: Then, Now and in the Future

Jorma Kajava University of Lapland, Juhani Anttila

Rauno Varonen University of Oulu, Reijo Savola VTT Technical Research Centre of Finland, Juha Roning University of Oulu. (2006). Senior Executives Commitment to Information Security – from Motivation to Responsibility.

Pauline Bowen, Elizabeth Chew, Joan Hash. (2007).Security Guide For Government Executives.

Hugh Parkes, CISA, FCA. (2006). Shifting Governance Roles and Responsibilities:Improving Management Reporting as Part of Corporate and IT Governance.

Sudhakar Sathiyamurthy, ITIL, MCSE. (2008). Is the IT Risk Worth a Control? Defining a Cost-value Proposition Paradigm for Managing IT Risks.

Sekar Sethuraman, CISA, CISM, CISSP, CIA, CSQA, BS 7799 LA. (2006). Framework for Measuring and Reporting Performance of Information Security Programs in Offshore Outsourcing.

Ulf Mattsson. (2011). Choosing the Most Appropriate Data Security Solution for an Organization.

Nicole Pauls, CISSP-ISSAP, ISSMP. (2005). Security Information Management: Not Just the Next Big Thing.

John P. Pironti, CISA, CISM, CISSP. (2005). Key Elements of an Information Security Program.

R. Daniel Lee. (2001). Developing Effective Information Systems Security Policies.

Jorma Kajava University of Lapland, Juhani Anttila

Pauline Bowen, Elizabeth Chew, Joan Hash. (2007). Security Guide For Government Executives.

Hugh Parkes, CISA, FCA. (2006). Shifting Governance Roles and Responsibilities: Improving Management Reporting as Part of Corporate and IT Governance.

Sudhakar Sathiyamurthy, ITIL, MCSE. (2008). Is the IT Risk Worth a Control? Defining a Cost-value Proposition Paradigm for Managing IT Risks.

Sekar Sethuraman, CISA, CISM, CISSP, CIA, CSQA. (2006). Framework for Measuring and Reporting Performance of Information Security Programs in Offshore Outsourcing.

Ulf Mattsson. (2011). Choosing the Most Appropriate Data Security Solution for an Organization.

Nicole Pauls, CISSP-ISSAP, ISSMP. (2005). Security Information Management: Not Just the Next Big Thing.

John P. Pironti, CISA, CISM, CISSP. (2005). Key Elements of an Information Security Program.

R. Daniel Lee. (2001). Developing Effective Information Systems Security Policies.

Appendix A: SOHO WLAN Security Framework Questionnaire

1. How important does your organization's top management consider information and technology to be to the delivery of your enterprise's strategy and vision?
    a. Not important at all
    b. Not very important
    c. Somewhat important
    d. Very important
    e. Don't know
2. Which of the following individuals are concerned in approving your security policy?
    a. President/Managing Director
    b. COO
    c. CIO
    d. CTO
    e. CSO (Chief Security Officer)
    f. CISO (Chief Information Security Officer)
    g. Manager/Department Head Information Security/IT
    h. Security Administrator

3. What drives spending on security initiatives?
    a. Security breaches from external sources
    b. Improved business practices
    c. Auditing regulations
    d. Legislative regulations
    e. Protection of brand or institutional image
    f. Security breaches from internal sources
    g. Industry standards
    Insurance requirements

4. Which of the following best describes the information security structure of your organization?
    a. Formal dedicated information security department or team
    b. Dedicated staff within the organization whose primary job function is information security
    c. Staff within the organization with a secondary job function of information security
    d. Dedicated individuals outside the organization whose primary job function is information security
    e. Dedicated individuals outside the organization whose secondary job function is information security
    f. Outside experts through and outsourcing agreement

5. How would you describe your security implementation process?
    a. We put products in place and or train staff where we perceive there are weaknesses.
    b. We have some security in place, but we generally react to threats as they arise.
    c. We asses our IT systems in terms of risk to attack and loss in the event of compromise and we focus resources according to that assessment.

    d. We follow the direction of our consultant or another institutional department.
6. Does your enterprise use a framework/standard for governance and management of enterprise IT assets and services?
    a. Yes
    b. No
    c. Unsure
7. Which of the following has your enterprise experienced in the last 12 months as a result of an IT-related problem/incident?
    a. Incurred unexpected expense
    b. Reputation was harmed
    c. Customer satisfaction was reduced
    d. Opportunities to reduce costs were delayed or missed
    e. A competitor beat my enterprise to market
    f. Other
8. Which qualities are most important when choosing a security product or technology?
    a. Performance
    b. High availability
    c. Integration with existing networks and hosts
    d. Integration with existing network management and help desk systems
    e. Ease of use
    f. Tiered access control
    g. Detailed audit logs
9. What is the Usefulness of this control framework when you compare it to the others?
    a. Not useful
    b. Slightly useful
    c. Useful
    d. Very useful
10. How do you rate the Ease of Use of this framework when you compare it with others?
    a. It is difficult to use
    b. It is slightly easy to use
    c. It is easy to use.
    d. It is very easy to use.
11. How do you rate the Ease of providing reliable results when you compare it with others?
    a. It does not provide reliable results
    b. It slightly provides reliable results.
    c. It provides reliable results
    d. It is very good in providing reliable results
12. What is your level of Satisfaction with this framework when you compare it with the others?
    a. I am not satisfied with it
    b. I am slightly satisfied with it.
    c. I am satisfied with it
    d. I am very satisfied with it

Appendix B: Necessary Controls for each Components

1. Data: Controls necessary to protect the data	**1.0: Information Classification** Information within the SOHO WLAN environment should be classified. Only those individuals with the right clearance should view or process the information. **1.1: Information Back-Up** Information and software should be regularly backed-up. The SOHO organization should have a back-up policy for taking backup and the steps for backup rehearsed. The backup data should be tested regularly to ensure that they can still be used. **1.2: Information Handling Procedures** Procedures for the handling and storage of information within the SOHO WLAN environment should be established to protect the information from unauthorized disclosure or misuse. **1.3: Input Data Validation** Data input to applications should be validated to ensure that this data is correct and appropriate. **1.4: Privacy of Personal Information** The SOHO organization should ensure that there is data protection and that privacy is ensured as required in regulations and contractual clauses.
2. Access Points (AP) For the AP to be protected against attacks, the following controls should be there:	**2.0: Monitoring System Use** Connections to the SOHO wireless LAN should be monitored. For any connection only authorized devices should be allowed. Use of privilege operations such as us of privileged accounts e.g. root or administrator accounts, system start-up and stop should be closely monitored. **2.1: Clock Synchronization** Due to the fact that correct settings of computer clock is important to ensure the accuracy of audit logs, the clocks of all relevant information processing systems within the SOHO organization should be synchronized with an agreed accurate time source.

	2.2: User Authentication for External Connection Appropriate authentication methods should be used to control access to the SOHO WLAN by remote users. **2.3: Equipment Identification in Networks** All connected devices to the SOHO WLAN should be only those that have been authorized. **2.4: Remote Diagnostic and Configuration Port Protection** Physical and logical access to diagnostic and configuration ports of the SOHO WLAN should be controlled. **2.5: Network Routing Control** Routing controls should be implemented for the SOHO WLAN to ensure that computer connections and information flows do not breach the access control policy of the business applications. **2.6: Limitation of Connection Time** Restriction on connection times to the SOHO WLAN should be used to provide additional security for high risk applications. Restricting connection times to normal office hours if there is no requirement for overtime or extended hours operation. **2.7: Key Management** Key Management should in place to support the organization's use of cryptographic techniques. **2.8: Electronic Messaging** Electronic messaging such as emails have an important role in exchange of information in an organization. Information involved in electronic messaging should be protected from unauthorized access, modification, repudiation or denial of service.
3. Administrator The following controls were found to be necessary to guide a SOHO WLAN administrator to carry out his/her duties without	**3.1: Security policy** The SOHO organization must have a security policy that demonstrates the management support for information security. The administrator should confirm that an information security document exist. It's approved by the management and is communicated to all employees.

compromising the system:	**3.2: Review of Information Security Policy (ISP)** The SOHO WLAN administrator should insure that there are planned dates at which the information security document is reviewed to ensure that it still meets the security requirements of the organization. **3.3: Management Commitment to Information Security Policy** The management should be committed to information security by providing direction, providing the resources needed, assign responsibilities for information security and implement a security awareness plan. **3.4: Review of Information Security** Controls implemented should be reviewed by an independent party at planned intervals. **3.5: Risks Due to External Parties** Controls should be in place to ensure that third parties such as suppliers are controlled. An assessment of exposure to risks whenever contact is made with third parties should be done. A third party products or services should not compromise the organization security. **3.6: Inventory of Assets** An inventory of all assets of an SOHO organization should be maintained. **3.7: Equipment Maintenance** Equipment should be regularly maintained to ensure that it operates at optimal levels. **3.8: Secure Disposal of Equipment** Devices such as hard disks should be securely disposed to ensure that sensitive information does not leak to unauthorized individuals. Where necessary, it should be physically destroyed. **3.9: Service Delivery** The SOHO organization should ensure that third parties maintain sufficient service capability to ensure that agreed service continuity levels are maintained. **3.10: Capacity Management** System resources should be monitored to ensure that they still

	operate as required. Projections should be made for future capacity requirements. **3.11: System Acceptance** There should be acceptance criteria for new information systems, upgrades and new versions. **3.12: Administrator and Operator Logs** Activities done SOHO WLAN administrators and system operators should be logged. The processes involved, time at which an event occurred and information about the event should be logged. **3.13: Fault Logging** Faults reported by SOHO WLAN users should be logged. The fault logs should be reviewed to ensure that corrective actions were taken. **3.14: Access Control Policy** An access control policy should be established, documented and regularly reviewed. Access control rules and rights for each SOHO WLAN user or group of users should be clearly stated in an access control policy. **3.15: User Registration** All users within the SOHO organization should be registered for instance through unique user Ids to enable users to be linked to and held responsible for their actions. **3.16: Password Management** Allocation of passwords should be controlled through a formal management process. **3.17: Privilege Management** The allocation and use of privileges should be restricted and controlled. **3.18: Review of Access Rights** User access rights should be reviewed regularly to maintain effective control over access to data and information services. **3.19: Policy on Use of Network Services** Unauthorized and insecure connections to network services can affect the whole organization. Users should only be provided

	with access to the services that they have been specifically authorized to use. **3.20: Security Requirements Analysis and Specifications** Controls required for the business to run should be regularly analyzed and corrective actions if necessary take. **3.21: Policy on the use of Cryptographic Controls** A policy on the use of cryptographic controls is necessary to maximize the benefits and minimize the risks of using cryptographic techniques and avoid inappropriate or incorrect use. **3.22: Outsourced Software Development** Outsourced software development should be supervised and monitored by the organization. **3.23: Responsibilities and Procedures** Individuals should be identified responsible for information security incident management. Procedures should also be available to handle different types of information security incidents. **3.24: Business Continuity and Risk Assessment** Measures should be put in place to ensure that if an attack occurs, the SOHO WLAN will still be able to run its critical services. **3.25: Testing Business Continuity Plans** Business continuity plans should be regularly tested to make sure that they will be effective. **3.26: Identification of Applicable Legislation** All relevant regulatory requirements should be clearly defined, documented and kept up to date. **3.27: Intellectual Property Rights** Appropriate procedures should be implemented to ensure compliance with regulatory requirements on the use of material in respect of which there may be intellectual property rights and on the use of proprietary software products. **3.28: Compliance with Security Policies and Standards** SOHO WLAN managers should ensure that all security

	procedures within their area of responsibility are carried out correctly to achieve compliance with security policies and standards. **3.29: Technical Compliance Checking** Information systems should be regularly checked for compliance with security implementation standards. **3.30: Information Systems Audit Controls** Audit requirements and activities involving checks on operational systems should be carefully planned and agreed to minimize the risk of disruptions to the SOHO WLAN.
4. Users The following controls were deemed necessary in controlling user's activities within the SOHO organization.	**4.0: Confidentiality Agreements** SOHO WLAN users should sign non disclosure agreements in order to protect confidential data. **4.1: Information Systems (IS) Responsibilities** The SOHO WLAN management should appoint asset owners whose responsibilities is to ensure that the assets are operated securely. **4.2: Acceptable Use of Assets** The assets within the SOHO organization have been invested is so that the organization can meet its objectives. Users should therefore use the assets responsibly to achieve these objectives. There should be rules for electronic mail and internet usages. **4.3: Screening** Background checks should be done on employees, contractors and other third party users. **4.4: Terms of Employment** Employees, contractors and third party users should agree and sign a contract which should indicate their and organization's responsibility for information security. **4.5: Security Training** All SOHO WLAN employees should be regularly trained on how to work securely and updated on the organization's security policy.

	4.6: Disciplinary Process There should be a disciplinary process that should be followed in cases where employees commit a security breach. All employees should be treated fairly. **4.7: Termination Responsibilities** There must be a termination responsibility that will be used to ensure employees exit an SOHO organization in an orderly manner. **4.8: Return of Assets** SOHO WLAN users should return all of the organization's assets upon termination of their employment. **4.9: Removal of Access Rights** Upon termination of employment all access rights that were associated with a user should be removed. **4.10: Operating Procedures** There should be documented procedures for system activities such as computer start up and close down, backup, equipment maintenance and so on. **4.11: Segregation of Duties** Duties should be segregated to reduce opportunities for unauthorized or unintentional modification of the organization's assets. **4.12: Password Use** Users should be required to follow good security practices in the selection and use of passwords. **4.13: Unattended User Equipment** Users should ensure that unattended equipment has appropriate protection. **4.14: Clear Desk and Clear Screen Policy** A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities should be adopted. **4.15: User Identification** All SOHO WLAN users should have a unique identifier (User

	ID) for their personal use only and a suitable authentication technique should be chosen to substantiate the claimed identity of user. **4.16: Mobile Computing and Communications** Users of mobile computing facilities in public places should take care to avoid the risk of overlooking by unauthorized persons. Equipment carrying important, sensitive and critical business information should not be left unattended. **4.17: Reporting Information Security Events** Information security events should be reported through appropriate management channels as quickly as possible. **4.18: Reporting Security Weaknesses** All SOHO WLAN users of information systems and services should be required to note and report any observed or suspected security weaknesses in systems or services. **4.19: Prevention of Misuse of Information Processing Facilities** Users should be deterred from using information processing facilities for unauthorized purposes. **4:20: Removal of Property** No equipment should be removed from the SOHO organization without authority. Where necessary spot checks should be done to detect unauthorized removal of property.
5. Environment The wireless LAN environment should have the following controls:	**5.0: Physical Security Perimeter** There should be physical security. The organization should be secured with barriers if necessary. Offices should be lockable. There should be manned reception desks and entry to the organization controlled. **5.1: Physical Entry Controls** There should be entry controls that ensure only authorized individuals are permitted access. Dates and times for entry and departure of visitors should be recorded. Visitors should be supervised. Access to sensitive areas should be restricted only to authorized individuals. There should be authentication controls for instance through a card and a PIN.

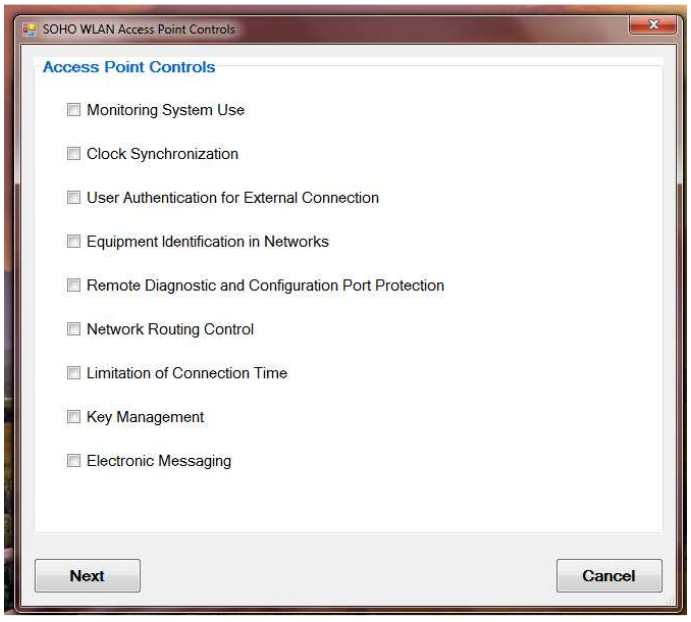
	5.2: Environmental Threats Protection Equipment should be adequately protected against damage from fire, flood, earthquake, explosions, civil unrest and other forms of natural or manmade disasters. Combustible and hazardous materials should be carefully stored at safe distances. There should be appropriate firefighting equipment. Drainage systems should be regularly maintained. **5.3: Equipment Siting and Protection** Equipment should be placed in locations that are secure from threats. Eating, smoking or drinking should be discouraged near information processing facilities. Temperatures and humidity should be monitored. Lightning protection should be applied. **5.4: Supporting Utilities** All supporting utilities such as electricity, water supply, sewage, heating/ventilation and air conditioning should be adequate. They should be regularly inspected. The uninterruptible power supply (UPS) should be installed. Backup generators should also be there. **5.5: Information Leakage** There should be regular monitoring to ensure that the radio signal is within the organization. **5.6: Sensitive System Isolation** Sensitive system should have an isolated computing environment.
6. Client Machines All client machines can be protected by implementing the following controls:	**6.0: Change Management** Changes to information processing facilities should be controlled. All significant changes within the SOHO WLAN environment should be recorded. The changes should be planned and tested. There should be approval for the changes. There should be fallback procedures in case of unsuccessful changes. **6.1: Controls against Malicious Code** There should be malicious code detection and repair software. There should be a policy within the SOHO WLAN environment prohibiting the use of unauthorized software. Regular reviews of the software and data content of systems supporting critical business process should be done.

	6.2: Audit Logging User activities within the SOHO WLAN environment should be logged with exceptions and information security events being produced to assist in future investigations. Audit logs should contain user Ids, dates, times, details of key events, terminal identity and so on. **6.3: Secure Log-On Procedures** Access to operating system should be controlled by a secure log-on procedure. **6.4: Session Timeout** Inactive sessions should shut down after a defined period on inactivity. **6.5: Control of Operational Software** There should be procedures in place to control the installation of software on operational systems. **6.6: Change Control Procedures** The implementation of changes within the SOHO WLAN environment should be controlled by the use of formal change control procedures. **6.7: Technical Review of Applications after Operating System Changes** When operating systems are changed, business critical applications should be reviewed and tested to ensure there is no adverse impact on the organizational operations or security.

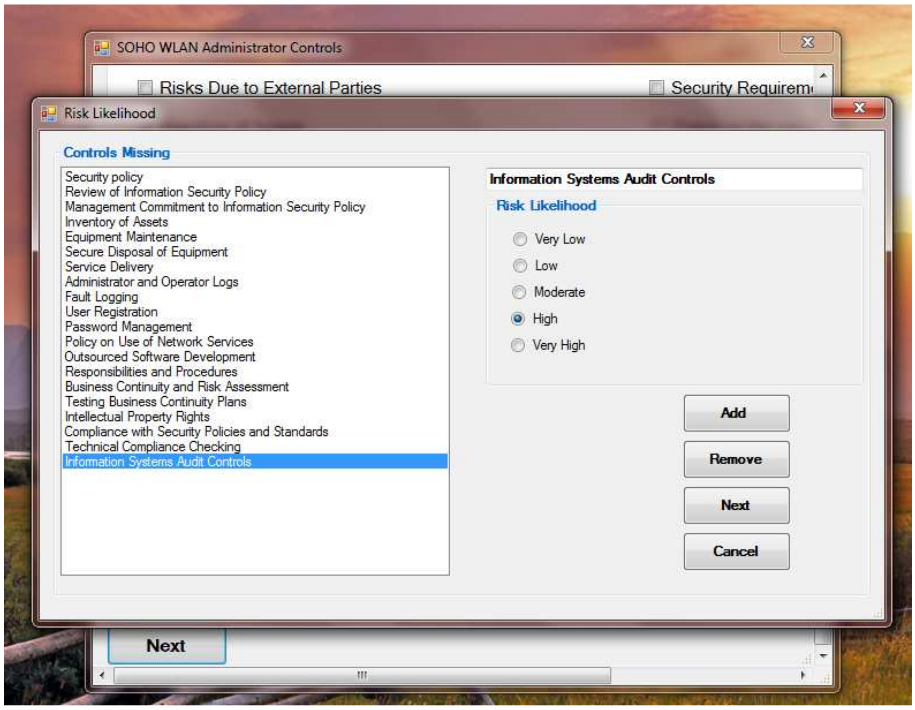
Appendix C: Screen Shots

The first step was to determine which controls are relevant to their organizations for each component. The screen shorts are as follows:

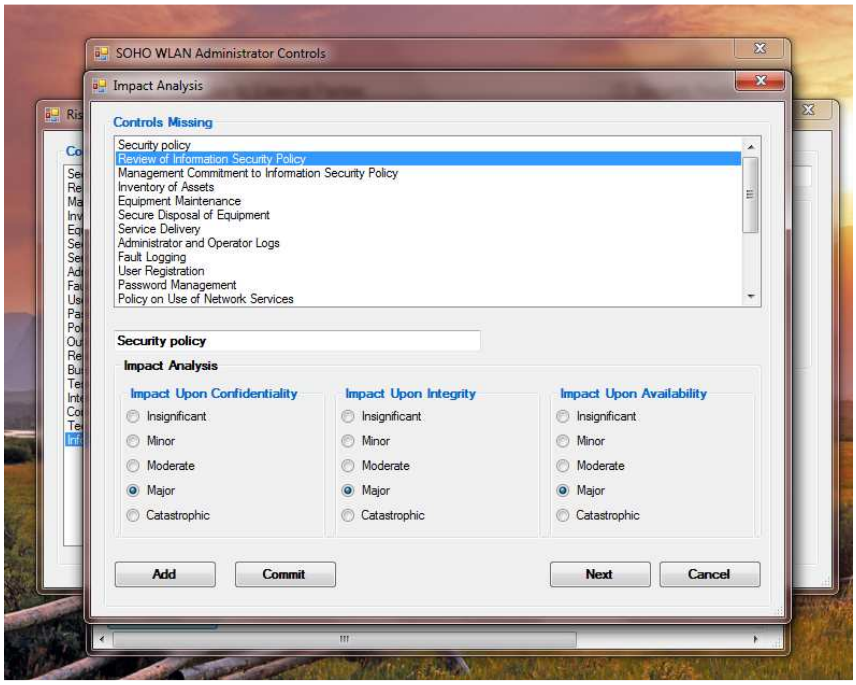
Controls that were deemed necessary but missing were then chosen:



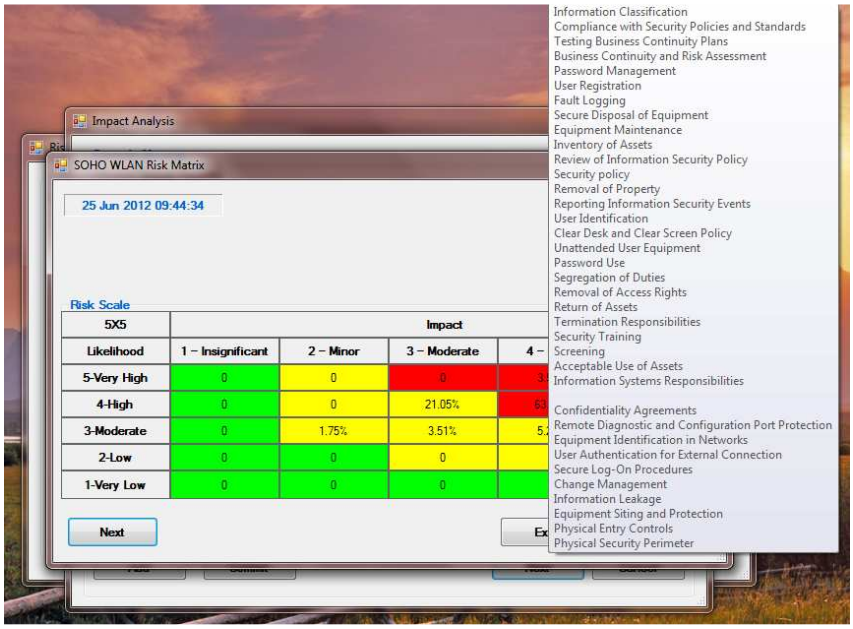
For each control, they indicated the possibility of a threat source exploiting a vulnerability due to lack of the control.



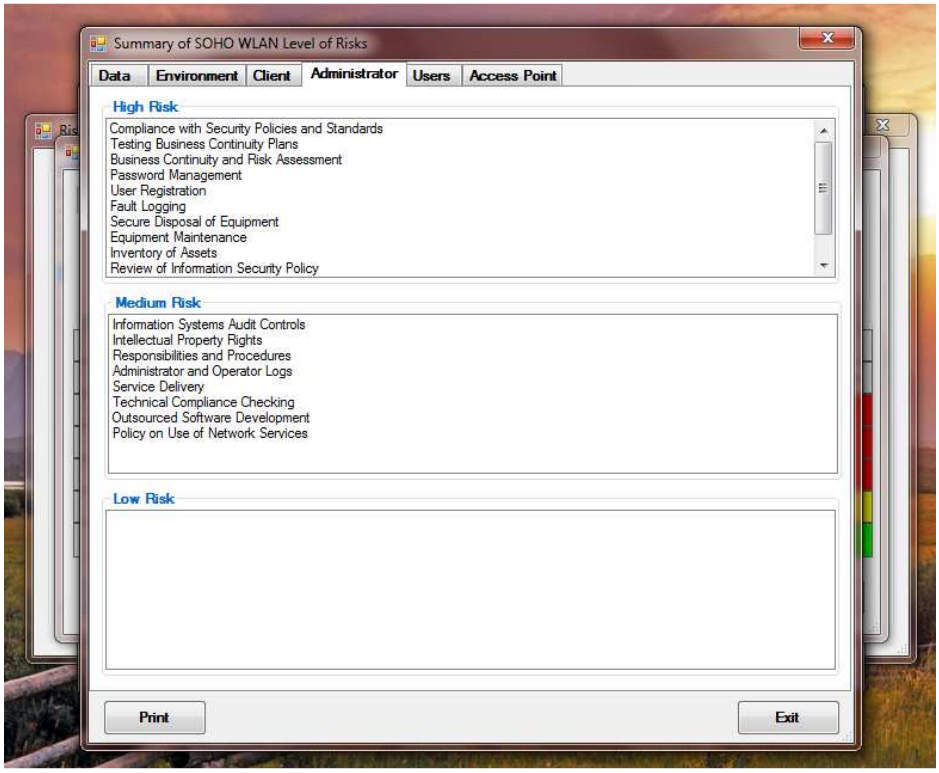
For each missing control, they indicated what the impact would be if an attack was successful.



A risk matrix was then used to determine which controls needed urgent attention.



The controls that were missing were then displayed as per the component. All the controls that were under medium and high risk were to be implemented to reduce the risk level.



Appendix D: Section of Code

```
Public Class AccessPointForm
    Public controlsMissingAPtemp As New List(Of String)
    Public checkAP As Integer = 0

    Private Sub CheckBox1_CheckedChanged(ByVal sender As System.Object, ByVal e As
System.EventArgs) Handles APMonitoringSystemCheckBox.CheckedChanged
        If APMonitoringSystemCheckBox.Checked = True Then
            If Form1.controlsMissingAP2.Contains(APMonitoringSystemCheckBox.Text) =
False Then
                Form1.controlsMissingAP2.Add(APMonitoringSystemCheckBox.Text)
                Form1.counterAll = Form1.counterAll + 1
            End If
        End If
    End Sub
    Private Sub APClockSynchronizationCheckBox_CheckedChanged(ByVal sender As
System.Object, ByVal e As System.EventArgs) Handles
APClockSynchronizationCheckBox.CheckedChanged
        If APClockSynchronizationCheckBox.Checked = True Then
            If Form1.controlsMissingAP2.Contains(APClockSynchronizationCheckBox.Text)
= False Then
                Form1.controlsMissingAP2.Add(APClockSynchronizationCheckBox.Text)
                Form1.counterAll = Form1.counterAll + 1
            End If
        End If
    End Sub
    Private Sub APUserAuthenticationCheckBox_CheckedChanged(ByVal sender As
System.Object, ByVal e As System.EventArgs) Handles
APUserAuthenticationCheckBox.CheckedChanged
        If APUserAuthenticationCheckBox.Checked = True Then
            If Form1.controlsMissingAP2.Contains(APUserAuthenticationCheckBox.Text) =
False Then
               Form1.controlsMissingAP2.Add(APUserAuthenticationCheckBox.Text)
                Form1.counterAll = Form1.counterAll + 1
            End If
        End If
    End Sub
    Private Sub APEquipmentIdentificationCheckBox_CheckedChanged(ByVal sender As
System.Object, ByVal e As System.EventArgs) Handles
APEquipmentIdentificationCheckBox.CheckedChanged
        If APEquipmentIdentificationCheckBox.Checked = True Then
            If
Form1.controlsMissingAP2.Contains(APEquipmentIdentificationCheckBox.Text) = False Then
                Form1.controlsMissingAP2.Add(APEquipmentIdentificationCheckBox.Text)
                Form1.counterAll = Form1.counterAll + 1
           End If
        End If
    End Sub
    Private Sub APRemoteDiagnosticCheckBox_CheckedChanged(ByVal sender As
System.Object, ByVal e As System.EventArgs) Handles
APRemoteDiagnosticCheckBox.CheckedChanged
        If APRemoteDiagnosticCheckBox.Checked = True Then
            If Form1.controlsMissingAP2.Contains(APRemoteDiagnosticCheckBox.Text) =
False Then
                Form1.controlsMissingAP2.Add(APRemoteDiagnosticCheckBox.Text)
                Form1.counterAll = Form1.counterAll + 1
            End If
        End If
    End Sub
```

```
    Private Sub APNetworkRoutingCheckBox_CheckedChanged(ByVal sender As System.Object,
ByVal e As System.EventArgs) Handles APNetworkRoutingCheckBox.CheckedChanged
        If APNetworkRoutingCheckBox.Checked = True Then
            If Form1.controlsMissingAP2.Contains(APNetworkRoutingCheckBox.Text) =
False Then
                Form1.controlsMissingAP2.Add(APNetworkRoutingCheckBox.Text)
                Form1.counterAll = Form1.counterAll + 1
            End If
        End If
    End Sub
    Private Sub APLimitationConnectionCheckBox_CheckedChanged(ByVal sender As
System.Object, ByVal e As System.EventArgs) Handles
APLimitationConnectionCheckBox.CheckedChanged
        If APLimitationConnectionCheckBox.Checked = True Then
            If Form1.controlsMissingAP2.Contains(APLimitationConnectionCheckBox.Text)
= False Then
                Form1.controlsMissingAP2.Add(APLimitationConnectionCheckBox.Text)
                Form1.counterAll = Form1.counterAll + 1
            End If
        End If
    End Sub
    Private Sub APKeyManagementCheckBox_CheckedChanged(ByVal sender As System.Object,
ByVal e As System.EventArgs) Handles APKeyManagementCheckBox.CheckedChanged
        If APKeyManagementCheckBox.Checked = True Then
           If Form1.controlsMissingAP2.Contains(APKeyManagementCheckBox.Text) = False
Then
                Form1.controlsMissingAP2.Add(APKeyManagementCheckBox.Text)
                Form1.counterAll = Form1.counterAll + 1
            End If
        End If
    End Sub
    Private Sub APElectronicMessagingCheckBox_CheckedChanged(ByVal sender As
System.Object, ByVal e As System.EventArgs) Handles
APElectronicMessagingCheckBox.CheckedChanged
        If APElectronicMessagingCheckBox.Checked = True Then
            If Form1.controlsMissingAP2.Contains(APElectronicMessagingCheckBox.Text) =
False Then
                Form1.controlsMissingAP2.Add(APElectronicMessagingCheckBox.Text)
                Form1.counterAll = Form1.counterAll + 1
            End If
        End If
    End Sub
    Private Sub Button2_Click(ByVal sender As System.Object, ByVal e As
System.EventArgs) Handles AccessPointFormCancelButton.Click
        RiskLikelihoodForm.RiskLikelihoodFormListBox.Items.Clear()
        controlsMissingAPtemp.Clear()
        Form1.controlsMissingAP2.Clear()
        Form1.tempRisklikelihoodList.Clear()
        For Each ctrl As Control In GroupBox1.Controls
            If TypeOf ctrl Is CheckBox Then
                CType(ctrl, CheckBox).Checked = False
            End If
        Next
            Me.Close()
    End Sub
    Private Sub Button1_Click(ByVal sender As System.Object, ByVal e As
System.EventArgs) Handles AccessPointFormSubmitButton.Click
        For i = 0 To Form1.controlsMissingAP2.Count - 1
            If controlsMissingAPtemp.Contains(Form1.controlsMissingAP2(i)) = False
Then
                controlsMissingAPtemp.Add(Form1.controlsMissingAP2(i))
            End If
```

```
        Next
        For i = 0 To controlsMissingAPtemp.Count - 1
            Form1.tempRisklikelihoodList.Add(controlsMissingAPtemp(i))
        Next
        For i = 0 To Form1.tempRisklikelihoodList.Count - 1

RiskLikelihoodForm.RiskLikelihoodFormListBox.Items.Add(Form1.tempRisklikelihoodList(i)
)
            checkAP = 1

        Next
          RiskLikelihoodForm.ShowDialog()
    End Sub
    Private Sub AccessPointForm_Load(ByVal sender As System.Object, ByVal e As
System.EventArgs) Handles MyBase.Load
    End Sub
    Private Sub AccessPointForm_FormClosed(ByVal sender As System.Object, ByVal e As
System.Windows.Forms.FormClosedEventArgs) Handles MyBase.FormClosed
        'Form1.controlsMissingAP.Clear()
        controlsMissingAPtemp.Clear()
        Form1.tempRisklikelihoodList.Clear()
        For Each ctrl As Control In GroupBox1.Controls
            If TypeOf ctrl Is CheckBox Then
                CType(ctrl, CheckBox).Checked = False
            End If
        Next
       End Sub
    Private Sub AccessPointForm_Activated(ByVal sender As System.Object, ByVal e As
System.EventArgs) Handles MyBase.Activated
    End Sub
    Private Sub AccessPointForm_FormClosing(ByVal sender As System.Object, ByVal e As
System.Windows.Forms.FormClosingEventArgs) Handles MyBase.FormClosing
    End Sub
End Class
```