2006

An attitude and perception study of wireless network usage in home environments

Patryk Szewczyk
Edith Cowan University

Edith Cowan University

Copyright Warning

AN ATTITUDE AND PERCEPTION STUDY OF WIRELESS NETWORK USAGE IN HOME ENVIRONMENTS

Patryk Szewczyk

Bachelor of Science (Computer Science)

This thesis is presented in fulfilment of the requirements for the degree of

Bachelor of Science Honours (Computer Science)

Faculty of Computing Health and Science
Edith Cowan University

September 2006

EDITH COWAN UNIVERSITY

USE OF THESIS

The Use of Thesis statement is not included in this version of the thesis.

ABSTRACT

Research on the use of 802.11 wireless networking and wireless security has in the past focused predominantly on corporations who generally have access to resources specifically allocated to computer and network security. Research has also focused on identifying the flaws in wireless network security, and developing stronger and safer methods which may be incorporated. To date there has been a lack of research into determining what the individual at home perceives towards wireless security. As broadband Internet connections are now predominantly chosen, the amount of available bandwidth open to exploitation is significantly higher than the now becoming obsolete dialup connection. The numerous researched yet unpublicised wireless network threats, is leaving an unaware individual vulnerable to various, easy to administer attacks which may result in identity theft or significant monetary loses.

To develop solutions aimed at protecting the home individual utilising 802.11 wireless networks, information needs to be collected on what individuals already know and perceive. Hence the scope of this study was to analyse the attitudes and perceptions individuals have towards wireless security. Utilising a quantitative online survey instrument the study was directed to those who specifically had an Internet connection and had enabled an 802.11a\b\g standard wireless network. Over the course of 21 days the online survey instrument had been completed by 163 anonymous respondents who volunteered to complete the questionnaire consisting of 29 questions.

The majority of respondents had utilised a broadband connection leaving a large amount of bandwidth available for exploitation. The results indicate that respondents are well aware of the basics of wireless networking. However, when confronted with specifics of wireless security (utilised authentication and encryption) their perception was not valid. The proactive behaviour respondents had towards wireless security varied and were dependant upon their level of concern and experience in wireless networking.

There is little distinction between those respondents who had worked in the IT industry and those who have not. The results from the study confirm with similar studies undertaken on the topic of computer security, also looking at the level of knowledge respondents had. The sources used by respondents vary significantly, although the study did not find that a particular source made a significant contribution to a user's perceived security.

DECLARATION

I certify that this thesis does not, to the best of my knowledge and belief:

(i) incorporate without acknowledgment any material previously submitted for a degree or diploma in any institution of higher education.

(ii) contain any material previously published or written by another person except where due reference is made in the text; or

(iii) contain any defamatory material.

I also grant permission for the Library at Edith Cowan University to make duplicate copies of my thesis as required.

Signature: ....

Date: .....28:09:06.....

ACKNOWLEDGEMENTS

I would like to take this opportunity to acknowledge and thank those who have helped me to complete this thesis.

I would firstly like to thank my supervisor Doctor Craig Valli for his endless enthusiasm and guidance over the past year. Despite his heavy workload and responsibilities he always managed to listen, discuss and encourage me in times of difficulty.

Big thanks to my girlfriend Nivia who always found time to provide support and advise when it was needed. You are a precious gift and I am grateful for your endless assistance.

Lastly, but most importantly I would like to thank my dad who made me realise I can achieve anything if I set my mind on it. His patience, motivation and inspiration during the year are greatly appreciated.

TABLE OF CONTENTS

List of Figures

List of Tables

Glossary of terms

802.11
A collection of radio frequency standards developed by the Institute of Electrical and Electronic Engineers for wireless data communications in computer networks.

802.11b
Radio based frequency network operating on the 2.4 GHz frequency range with a maximum theoretical transfer rate of 11 Mbps.

802.11g
Radio based frequency network operating on the 2.4 GHz frequency range with a maximum theoretical transfer rate of 54 Mbps.

ADSL
Asymmetric Digital Subscriber Line technology that uses existing copper telephone landlines and may be used in conjunction with a telephone or fax simultaneously.

SSID
Service Set Identifier consisting of a combination of 32 numbers and/or letters representing the name of wireless network which is required to access the network when SSID broadcast is disabled.

WEP
Wired Equivalent Privacy protocol designed to encrypt data in transmit and hence provided the equivalent security of that in a wired network.

WPA
Wi-Fi Protected Access which was designed to replace the flawed WEP encryption protocol using a strong Temporal Key Integrity Protocol encryption method.

CHAPTER 1. INTRODUCTION

1.1. Background to the Study

Wireless is a broad term often used to describe the process of mobility in a computing environment, and a method by which communication is transmitted by mobile phones (Kim, Mims & Holmes, 2006, p. 78). The distinguishing property of wireless in contrast to wired networks is the method by which communication is transmitted between nodes. Wireless communication includes microwave transmission between two nodes situated on the earth's surface, satellite transmission utilising a microwave transceiver which is in orbit around the earth and wireless networks using radio waves or infrared (Shay, 2004). All of the wireless communication methods operate without the use of any interconnecting wires. The study is limited to the communication between nodes via the wireless radio waves using the 802.11 protocol, operating in the licensed, but free to air in Australia, 2.4 GHz frequency band (Golmie, Dyck, Soltanian & Tonnerre, 2003, p.201).

Tests have shown that 802.11b/g wireless routers such as *Linksys WRT54g* or *Bountiful Router* have a range of approximately 180 – 370 meters, with no obstructions in place, before the signal is no longer detected (Henderson, 2005, p.51). The natural property by which radio waves unfurl, limits feasible operation to the distance from a device with a wireless card to the central point of communication the access point, and any interfering objects such as walls, trees and rain (Oppenheim, 2002, p.8). Any wireless device that wants to utilise a wireless network theoretically needs to be within distance of the 180 – 370 meter range, the security and connection requirements are discussed later.

The benefit of utilising wireless via radio waves is that they are able to propagate through walls, ceilings and floors, hence not requiring a direct line of sight unlike microwave or satellite transmissions (Ciampa, 2006, p.56). Radio waves are not interfered by sunlight unlike electromagnetic energy and thus may be used indoors and outdoors. For the home user, wireless radio transmissions transfer a large amount of data at a low hardware cost in contrast to microwave or satellite networks which operate at 10 - 300 Mbps (Shay, 2004, p.85) but require expensive hardware. The benefits of

radio transmissions also pose a security risk in that the radio waves cannot be confined to the environment of use such as a house or apartment. Although there are known methods to reduce radio wave propagation such as a Faraday cage (Yek, 2005), these methods are simply not feasible for home wireless networking.

The scope of the study is to examine wireless radio based networks and is, referred hereafter, as 802.11 wireless networks. An 802.11 wireless network is usually comprised of at least one access point (AP), acting as the central device of communication (Rubin, 2003, p.28). Figure 1 illustrates a client with a wireless card, communicating with the central AP via an antenna located in both devices (Peterson, Heninger, Lindstrom & Romney, 2004, p.52). Wireless networks are utilised in locations such as shopping centres, educational institutions, medical centres and corporations (Hänninen, 2003). This study however, will examine wireless networks strictly in home environments.

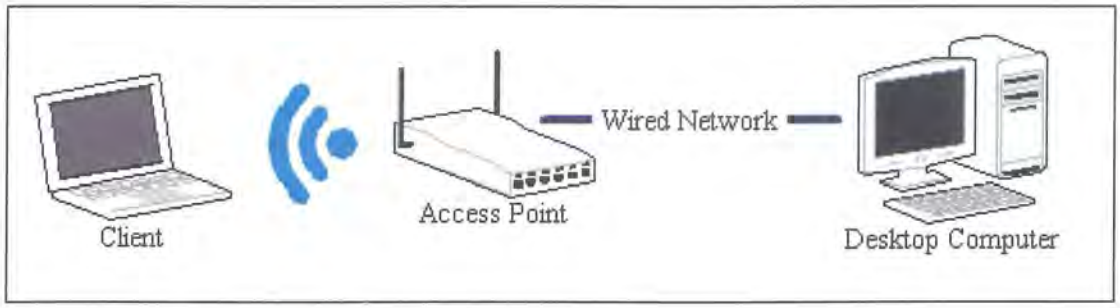


Figure 1 Wireless Local Area Network (Ciampa, 2006, p.6)

The increasing popularity of wireless networks in homes is due to the simplicity and time efficient configuration process to enable the network (Peterson, et al., 2004, p.53). Vendors supply out-of-the-box installations with hardware configured so the user can instantly become mobile. The examined studies show that few individuals and corporations secure their wireless network (Furnell, 2005; Lim, 2003; Schultz, 2005; Shipley, 2001) and vendors are not enforcing security measures in their manuals. A benefit of wireless has been the minimal expense of establishing the network (Rubin, 2003, p.28) as oppose to laying Ethernet cable through a building. In some instances this may prove difficult, time consuming, expensive or illegal when carried out in heritage listed properties. Wireless networks have become increasingly used in home networking environments where users are able to share files, printers and an ADSL

Broadband Internet connection amongst numerous individuals simultaneously (Burness, et al., 2003, p. 38).

1.2. The Significance of the Study

Numerous publications have been released with research covering how exposed businesses are becoming with their day-to-day networking usage. In one study only 24 percent knew how to deal with malicious activity on their computer (Hu & Dinev, 2005) whereas in a separate investigation businesses were using either flawed or no wireless security methods (Webb, 2003a). Chapter 2 will outline a thorough literature analysis, however in summary the statistical trends show that businesses are in fact exposing themselves to attacks and fraud, based on the wardriving experiments which have taken place in many cities around the world. Corporations generally have allocated computer specialists and network administrators unlike home users who may solely rely upon their own intuition. Companies and individuals at home are today more dependant on the availability of the Internet than ever before (Lally, 2005, p. 14). Conversely "you can't secure what you don't understand" (Jensen, 2005, p. 49), and thus this study will determine if individuals are aware of the need for security, are too lazy to implement the appropriate secure methods outlined in vendor literature, or simply do not understand the literature required to secure an 802.11 wireless network.

As the threats towards government critical infrastructure is increasing, several European countries are passing legislation authorising and demanding that Internet Service Providers (ISPs) collect and store their client's Internet usage history (Swartz, 2005, p. 10). Thus, it is essential that in particular end-users who have installed a wireless network in their home, secure it appropriately to prevent an individual whom is near by from accessing confidential data or inappropriate material which could lead to false prosecution. Firstly, this research is important to determine if individuals are exposing themselves to wireless network attacks by inadequate knowledge, understanding and thus security. Secondly, the study investigates if individuals are concerning themselves more so with devices which are easy to configure and use (plug and play), or if they do in fact make an effort to secure their wireless network.

As critical infrastructure utilises wireless networking methods indispensable services such as electricity and hospitals, could have their data and confidential information hijacked and used unethically. Chapter 2 shows the weaknesses of many wireless security methods however cities are continuously implementing wireless networks as part of low-cost housing development (Fritze, 2005). Individuals are persuaded by manufactures and retailers to install wireless hardware in their home for a marginal additional cost, regardless of whether they require the technology or not. However, there is no mention of who will be educating the users to adequately understand and be aware of the wireless network risks. Furthermore, there is no mention of who will configure security methods and ensure safe networking procedures. Just like large corporations, individuals at home who utilise wireless equipment are susceptible to session hijacking and sniffing attacks (Bahli & Benslimane, 2004, p.245). These attacks may leak confidential information to a third party, or may be used to abuse and steal bandwidth resulting in a large expenditure.

In high-rise buildings such as those found in the central city district a wireless signal may leak too many more individuals compared to if it were an access point in open space. As the growth and popularity of wireless continues, the media has begun disclosing basic wireless security information such as recommending WEP be used to prevent outsiders from accessing a private network (Fenech, 2006, p.5). The media is presenting false solutions to ill-advised individuals, as WEP encryption is flawed as will be discussed in the literature review. Alternatively, unviable solutions such as window tinting film or aluminium foil are considered ideal methods for reducing the strength of radio based transmissions although may not be appropriate for a home user financially (Spiga, 2004, p.118). Although various sources do provide options for wireless networking, in some instances window tinting a house may be too expensive, while using a flawed encryption method may provide little or no security to skilled wireless network intruders.

1.3. The Purpose of the Study

The purpose of the study is determine attitudes and perception by determining if individuals who use a wireless network at home have implemented appropriate security, understand the risks, and undertake associated proactive actions, to prevent a wireless attack. Studies examined in Chapter 2 indicate that businesses are wide open to wireless

attacks and that individuals at home are generally not implementing security methods for their home computer, and thus are open to malicious software and computer attacks. Furthermore, the study aims to investigate the materials used to setup and configure the wireless hardware the individual has acquired, finally determining if the experience was positive or negative.

Currently limited research has been found into wireless security analysis in home environments. Current trends see that vendors and research groups are focusing on corporations for expansion of wireless security and are neglecting the home user.

It is hypothesised that individuals are insecure, due to a lack of quality literature by vendors. This result will have implications that may lead further research into developing methods to ensure end-users are implementing security or choosing alternative home networking methods. Alternatively further research may investigate the discrepancy between the knowledge and behaviour of home and corporation users of wireless networks.

1.4. Research Questions

The research questions are aimed at determining the extent of knowledge towards wireless security, end-user perceptions and attitudes, and the utilised literatures by the individuals.

- What are identifiable behaviours and perceptions of individuals who use wireless networks and wireless security at home?
    - Are individuals who use wireless networks at home concerned with the risks, and is this explained by their behavioural attitudes?
    - Has configuring and using the wireless network been positive or negative experience for the home user?
    - What sources are being used by home users to setup and secure their wireless network?

CHAPTER 2. REVIEW OF THE LITERATURE

This chapter examines the relevant literature in relation to this wireless network study. A large proportion of the existing literature is targeted at large corporations and businesses. When researching the literature relevant to the study, limited publications were available discussing wireless networking in home environments. This chapter is broken into the fundamentals of wireless networking including background of networks, how wireless networks operate, the security methods and flaws with current 802.11 wireless security methodologies. The chapter then outlines and analyses the vendor assigned manuals for wireless broadband products, and finally concludes on relevant security literature specific to wireless networking which further iterates the requirement of the study.

2.1. Defining the Concepts of the Study

An individual can have a perception towards a given subject, such as believing wireless is secure. However, this belief may in fact be completely false (Swanson & Holton, 1999, p.134). An individual's perception may be assessed and studied, however a perception may also be falsely altered by companies attempting to sell products. This research endeavours to determine what perceptions and beliefs individuals' have towards their 802.11 wireless network and wireless security.

In numerous instances consumers have had their perceptions altered to believe a product is advantageous over others by planned marketing. Television advertising for example, shows vehicles dropping from the sky, not breaking on impact, showing endurance and robustness (Swanson & Holton, 1999, p.135). Wireless products can be marketed in a similar misleading manner, as fast and functional yet most importantly highly secure, giving the impression that security does not need to be configured but rather that the product is secure by default (Mussulman, 2002, p.7). The uninformed individual perceiving the product as secure would not need to question the security functionality as they are flooded with computing jargon consisting of symbols and numbers. This extensive use of data showing security parameters such as Wired Equivalent Privacy

(WEP) or Wi-Fi Protected Access (WPA) could possibly confuse the consumers and give them false beliefs towards how secure the product may be.

Ones perception may lead someone into believing that the wireless product is secure and thus not vulnerable to attacks, although the attitudes may challenge this. Attitudes are the positive or negative values that one has towards objects, situations or other individuals (Eagley & Chaiken, 1993, p.1). Investigations into the correlation between ones attitude and the associated behaviour were conducted during the 1960's, and found that a positive attitude towards an area shows a tendency to behave in an associated positive manner (*ibid*, 1993, p.159). As Westen (2002, p. 594) states: for individuals' attitudes to impact their ongoing positive behaviour of a subject, they must have a clear understanding and awareness of that area also. Thus, an individual must not only understand the working process of the wireless product, but must also be aware of the numerous flaws and risks before they may investigate and thus enforce security measures.

2.2. Advancements from Wired to Wireless in Home Networking

The historical approach for individuals at home to browse the Internet utilises the existing land line of a house using a dialup connection to an ISP (Sybex, 2001, p.328). The hardware required consisted of an analogue modem which converts the analogue signal of the phone line to the digital signal that the computer utilises (*ibid*, 2001, p.329). The typical security setup in such a home networking environment was a software approach consisting of a simple firewall and antivirus software. The antivirus software protects the computer from malicious software and the firewall filters incoming and outgoing traffic, and malicious connection attempts, which prevents a hacker or unauthorised individual gaining access to the computer resources (Blank, 2004, p.40). The dialup approach is now becoming less popular due to the bandwidth limitations and the deployment of cheap broadband services such as ADSL or cable.

The increasingly popular method of Internet connectivity is ADSL via a digital router modem and continually utilising the existing hardware infrastructure of the house via the telephone land lines. Individuals connect to the network via an Ethernet cable from each computer to the inbuilt router in the modem (Sybex, 2001, p.338). The Ethernet

protocol is capable of transmission speeds up to 1000 Mbps (*ibid*, 2001, p.341). The cabled approach does restrict mobility and incurs a high installation cost when cabling a home or office. The security methods when using ADSL still require software on each individual's computer to prevent malicious attacks. The router has inbuilt security functionality such as NAT which hides real IP addresses with server assigned dynamic or manual static addresses (*ibid*, 2001, p.342).

Wireless networks although not completely wireless do utilise the existing house wiring of telephone lines for the modem/router hardware of an ADSL connection. The common hardware of a wireless network at home utilises the ADSL hardware with an inbuilt wireless card and antenna. Additionally a wireless card is required in each device which will be connecting to the access point and thus network (Sportack, 2005, p.260). A wireless network does provide the mobility and cost efficiency which the Ethernet approach does not permit, although wireless does leave it self vulnerable to other issues which are discussed further.

2.2.1. Principles of Wireless

Unlike the methods of networking in wired networking environments, which generally use copper or fibre optic cables, two wireless devices communicate via invisible sine based radio waves (Ciampa, 2006, p.74). Radio waves are transmitted via an antenna made of copper cable and shielded within a plastic compound. The size of the antenna is a quarter the size of the wavelength which is being propagated from the radio (*ibid*, 2006, p.74). The default antenna which is typically connected to the access point in home wireless routers is omni directional which distributes the signal in a horizontal pattern (*ibid*, 2006, p.98).

The 802.11b/g protocols issue a beacon frame at regular intervals which is transmitted through the access point via the antenna as a radio wave with a broadcast IP address, destined to all wireless devices. The beacon frame provides information to a wireless device including; the Service Set Identifier (SSID) representing the name of the network, the speed at which the particular network operates, a synchronisation of clock times between the access point and wireless device, the modulation method which is

being used, and the requirements for the wireless device to connect to the network (*ibid*, 2006, p.161).

In order to connect to the network a process of 'authentication' and 'association' occurs between the access point and the wireless device which is attempting to connect to the network represented by Figure 2. In Open System configuration, no actual authentication takes place rather the MAC address of the wireless device is transmitted to the access point (Maufer, 2004, p.225).

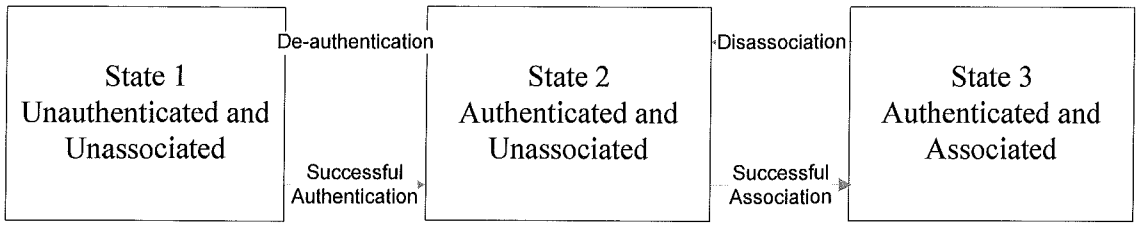


Figure 2 Connectivity States Between Wireless Device and Access Point (Maufer, 2004)

In Shared Key authentication, both devices have a secret, technically referred to as a Shared Key. The AP sends a challenge text to the wireless device which encrypts the text with the Shared key, which is then decrypted by the AP and authentication accepted (*ibid*, 2004, p.230). The second process, referred to as 'association', is a process of the wireless device successfully connecting to an AP. An association request and response frame is transmitted between the AP and wireless device. The frames contain information including: status codes such as acceptance or rejection of connection, an association identifier as a reference to the particular association, and supported data rates by the particular AP such as 1, 2, 5.5 and 11 Mbps in the case of 802.11b (*ibid*, 2004, p.236). Once the association process is complete, the AP and the wireless device may transmit network frames to each other.

2.2.2. 802.11 Wireless LAN Types

The Institute of Electrical and Electronic Engineers (IEEE) who governs the standards for wireless networks has released three standards which are used today they are 802.11a, 802.11b and 802.11g (and a projected 802.11n which is to be released in late 2006) (Ciampa, 2006, p.53).

The 802.11a and 802.11b standards for wireless networking were created within the same time span, yet only the 802.11b standard products were released soon after (*ibid*, 2006, p.53). The 802.11b standards permits a data transfer rate of 1, 2, 5.5 and 11 Megabits per second (Mbps), whilst the 802.11a standard has a far higher theoretical data rate of 6, 9, 12, 18, 24, 36, 48 and 54 Mbps (*ibid*, 2006, p.56). The frequency by which the 802.11a standard operates is between the 5.150 – 5.350 GHz range providing a total of eight non over lapping channels for communication (Bowmanm, 2002). Alternatively, the 802.11b standard frequency range is between 2.401 – 2.4835 GHz providing three non over lapping channels of communication; unfortunately the frequency range encompasses the 2.45 GHz range on which microwave ovens, cordless home phones and wireless audio visual equipment operate causing interference (*ibid*, 2002). Table 1 has a detailed comparison of each of the 802.11 protocols.

Table 1 Comparison of 802.11 Protocols (Maufer, 2004, p.96)

	802.11a	**802.11b**	**802.11g**
Theoretical maximum transmission rates dependant on distance from AP (Mbps)	6, 9, 12, 18, 24, 36, 48, 54	1, 2, 5.5, 11	1, 2, 5.5, 6, 11, 12, 18, 24, 36, 48, 54
Frequency range (GHz)	5.15-5.25, 5.25-5.35, 5.725-5.825	2.401-2.4835	2.401-2.4835
Modulation method	OFDM	DSSS	OFDM
Non-overlapping channels	8	3	3
Theoretical distance (meters)	30	115	115
Compatible with…	-	802.11g	802.11b

Although the 802.11a standard does allow transmission speeds of 54Mbps in contrast to 11Mbps of 802.11b, the cost of hardware production is significantly greater than that of 802.11b. The 802.11b protocol has been more widely accepted due to the range, which allows up to 115 meters whilst the 802.11a standard has a maximum theoretical range of approximately 30 meters, although these distances are reduced with interfering objects and weather conditions (Ciampa, 2006, p.57).

Due to the advantages and disadvantages of the 802.11b and 802.11a standards, the IEEE soon developed the 802.11g standard encompassing the advantages of both previous standards. The final product released provided speeds of up to 54 Mbps as

does 802.11a and ranges of up to 115 meters as those set out by 802.11b (*ibid*, 2006, p.57). 802.11g is able to achieve the same transmission speeds as 802.11a by using the same modulation method being Orthogonal Frequency Division Multiplexing (OFDM) (Kagan, 2003). OFDM divides the given frequency range into a number of smaller frequency channels, thus allowing more data to be transferred simultaneously in a parallel manner (ibid, 2003). As will be outlined in section 2.4 the majority of vendors have released wireless products for home use utilising the 802.11g standard with 802.11b compatibility.

2.3. Fundamentals of the Study

Wireless networks have increased in popularity over the past few years and are set to increase further as the cost of hardware decreases (Turner, 2003; Webb, 2003b). In turn the research conducted analyses both detection and prevention methods of wireless threats (Woodward, 2004a). Before any specific analysis of the literature similar to the current study can be presented, the research on wireless network risks and appropriate security methods must be considered. The following two sections discuss the risks of using a wireless network and the fundamentals of the proposed study. The security methods outlined will present a case for their implementation in certain circumstances, as well as outlining the flaws and difficulties of implementation. The literature about threats and countermeasures is not finite, and new methods are constantly being developed. However, the discussion presented here provides principal information on the risks individuals may face in a home or small office environment.

2.3.1. Wireless Network Threats

Access to a wireless network for individual users is not restricted to the placement of an Ethernet cable. Thus one of the principal threats is eavesdropping or, more specifically, an individual being able to capture, analyse, decrypt and read all incoming and outgoing traffic on the network (Hänninen, 2003; Lough, 2001). The radio waves transmitted by the sender and receiver generally propagate in a spherical (omni directional) form and are able to traverse through non metallic objects (Ciampa, 2006, p.76), permitting an individual to be within distance of the wireless signal and capture the traffic (Tagg, 2003). Open source software such as Ethereal (Ethereal, 2006) or Airview (Airview, 2006) required to capture network traffic, is freely available and can be used by any

inexperienced computer user. Eavesdropping with the use of software tools also permits an individual to capture enough traffic to gain unauthorised access to the network. Such an attack may be carried out from many kilometres away and easily deciphered when sent in clear text or using a weak encryption such as WEP (Lim, 2003). Eavesdropping using AirSnort (AirSnort, 2006) and then acquiring access to the network is also referred to as masquerading (Tagg, 2003).

2.3.1.1. Denial of Service

The denial-of-service (DoS) attack is a method of disrupting the communication signal between at least two wireless network nodes (Perrig, Stankovic & Wagner, 2004, p. 55). A DoS attack may be caused by devices that operate on similar 2.4 GHz frequency ranges (Barnes et al., 2002, p. 226) such as microwave ovens, cordless home phones and wireless audio visual equipment, thus interfering with transmitted data. DoS attacks may also be the cause of a deliberate attack on a network via an intentional flood of network traffic which renders communication between the access point and client useless (Barnes et al., 2002, p. 226).

As a wireless device transmits, an association request frame initialising it to the wireless network, a disassociation frame is transmitted by a wireless device when it wishes to terminate the connection (Ciampa, 2006, p.158). A wireless DoS attack may transmit disassociation frames from the wireless device to the AP causing it to continuously disassociate and thus requiring the wireless device to re-transmit and association request frame again (*ibid, 2006*, p.280). Alternatively an attack may jam the radio signal by flooding the 2.401 - 2.4835 frequency range, giving the impression to other devices that traffic is being transmitted. Since wireless networks utilise Carrier Sense Multiple Access / Collision Avoidance, no other device will transmit traffic until the initial traffic ceases (*ibid*, 2006, p.281).

The popularity of DoS attack tools has increased as have wireless networks. Tools including AirJack (AirJack, 2006) and Void11 (Wirelessdefence, 2006) have been noted to disrupt communication with proper equipment to a range of 32 kilometres (Woodward, 2004b, p.365). Such tools are capable of un-authenticating legitimate wireless devices and seizing a session (*ibid*, 2004b, p.366) thus permitting the intruder to falsely authenticate and use the wireless network. A DoS attack on a wireless

connection will not impact the wired connection to the network thus not necessarily impacting productivity. Alternatively when a wireless connection is solely used, a DoS attack will not only disrupt productivity in a home environment but may also be difficult to control or repair by an ill advised individual.

2.3.1.2. Man in the Middle Attack

Losing integrity in data transmission is the result of altering or modifying the validity of a message being transmitted via a "man in the middle attack" (Lim, 2003). It may result in a loss of confidentiality (Tagg, 2003) as the third party who is propagating the traffic through their own computer may record and monitor all data flow. An attacker usually achieves this attack by using a fake AP by which all network traffic is propagated before being retransmitted to the intended recipient. In a home or small business environment, the offender may locate themselves outside of a building and potentially monitor all traffic flow. This traffic may include banking transactions, personal information, Internet browsing data and information stored on every wireless enabled device connected to the wireless network.

2.3.1.3. Bandwidth and Information Theft

Wireless networking threats do not end at traffic being monitored or modified by an individual who is in the vicinity of the wireless network in a car, truck or at a nearby park. In numerous situations the offender may be a neighbour or occupant in an adjacent location (*ibid, 2003*). Apart from an individual being able to modify and/or monitor traffic accidentally or intentionally the individual may steal the wireless network's bandwidth (*ibid*, 2003). The dilemma is that the unsuspecting and ill-advised individual may connect to an inadequately configured and secured adjacent wireless network, abusing the bandwidth unknowingly (*ibid*, 2003). Internet service providers provide a limit as to the amount of data that may be downloaded each month, and/or slow the connection once the limit is reached, or charge a fee for each excess megabyte downloaded. Hence, the home user may be in a situation where their broadband connection is not at all operating at broadband speeds for which they pay for, or find themselves being charged for unknown excessive use.

The offender may also knowingly connect to an unauthorised network and download illegal software and multimedia such as music and video (Pollard, 2003). In independent scenarios in England and United States of America, two unrelated individuals stole something they could not see nor touch and were later arrested and charges were laid (Lawson, 2005). The two individuals made use of a wireless signal which was propagating beyond an occupant's house, something which is left uncontrolled in many instances (*ibid*, 2005). Not only were the individuals abusing the wireless network on a broadband connection, but also accessing files stored on other wireless enabled devices connected on the network.

2.3.1.4. Insertion Attack

Insertion attacks are a common method of performing attacks on a wireless network in which fake data is inserted into the network (Gittlen, 2005, p. 66). AirJack (AirJack, 2006) a wireless tool together with File2Air permits an individual to create 802.11 packets and inject the raw frame into the network (Gittlen, 2005, p.67). Not only does the freely available software permit individuals to test how access points react to certain packet types, it also permits the individual to permit a DoS attack, rendering the connected wireless devices useless.

2.3.2. Wireless Security Methods and Associated Vulnerabilities

The previous section examined common wireless network security threats. To counter these threats various security methods have been developed to prevent the possibility of these threats being exploited. Maxim and Pollino (2002, p. 239) explain the wireless security product lifecycle (see Figure 3) that was created during the introduction and boom of wireless networks into homes. Since customers using wireless networks demand strong wireless security methods, the supplier in turn needs to incorporate added security functionality to prevent the end-user from choosing an alternative networking supplier (Maxim & Pollino, 2002, p.239). As was explained previously (section 2.1) an individual's perception is altered by sophisticated marketing, making one product seem superior over the other. This study will attempt to determine if home end-users are demanding safer security standards, as well as utilising current technologies to the fullest. This study will also aim to determine if the suppliers who are

incorporating security functionality are providing sufficient understandable information so the end-user is able to utilise the security methods effectively.

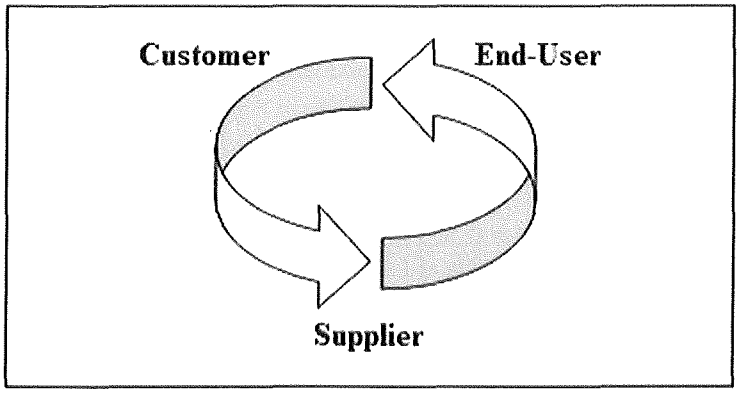


Figure 3 Wireless security lifecycle (Maxim & Pollino, 2002, p.239)

Wireless network technology has included both software and hardware security measures such as encryption, and reduction of antenna strength as a means to secure the device. A basic, yet unused, means of security in wireless networks is a thorough knowledge of flaws, risks and the appropriate methods which can be used to counter these threats (Woodward, 2004a). The end-user demanding safer security functionality and well produced manuals should in turn encourage the vendor to incorporate these into future products. As the current vendor provided literature shows little emphasis on security encouragement, the study aims to further determine the purchasing behaviour of consumers towards wireless products.

2.3.2.1. IEEE 802.1x

IEEE 802.1x Access Control is a security method based on authenticating and authorising a device to a network (Hänninen, 2003; Tagg, 2003). This is achieved via a Remote Authentication Dial-In User Service (RADIUS) authentication server, which in turn verifies a successful authentication. The RADIUS server stores each authorised users credentials and sends acceptance responses to the AP which is then forwarded to the individual requesting authorisation (Ciampa, 2006, p.309). Using this authentication measure is suitable for large corporations however a pre-shared key (PSK) mode can be used for home environments (Arbaugh, 2003). Hänninen (2003) discusses the flaws of 802.1x authentication and that it is possible to seize authenticated sessions. In the interest of this study, aimed at home users, Hänninen (2003) explains that 802.1x has not been adequately designed for home users as the majority of individuals would not

understand, nor have the expertise to configure and maintain a RADIUS server. A RADIUS server requires an additional computer or server with a configured database of credentials. In a home environment, individuals may possibly have one or two computers at most, and hence another computer may be too expensive or difficult to implement.

2.3.2.2. Wired Equivalent Privacy

WEP (see section 2.1) is a part of the 802.11 standard used to encrypt data during transmission in between two wireless devices. WEP has undergone research to determine the percentage of wireless networks in Perth, Western Australia utilising the technology (Webb, 2002). WEP is designed to provide the confidentiality of a wired network (Cam-Winget, Housley, Wagner & Walker, 2003) by scrambling or encrypting data during transmission using the RC4 encryption technique.

Before WEP may be utilised, an individual must manually configure and enter a key into the wireless access point and each wireless device. The key comprises of 5 or 13 ASCII characters (e.g. 'string' for a 5 character ASCII key), or 10 or 16 hexadecimal characters (eg 'B024D0A16E' for 10 a hexadecimal key) in length (Ciampa, 2006, p.266). The process of WEP encryption follows a series of five steps outlined by Ciampa (2006, p.269) as follows:

1. A cyclic redundancy check (CRC) value is devised from the data which is to be encrypted and appends this value to the end of the initial data. The CRC value is used to detect malicious or accidental alteration in packets during transmission.
2. The key which was set and created of ASCII or hexadecimal characters is combined with an initialisation vector (IV) which is changed each time a new packet is encrypted.
3. The combined IV and key which were appended together in step 2 are then placed through an algorithm generating a "pseudo-random data sequence" of binary 1's and 0's (Karygiannis & Owens, 2002).
4. The "pseudo-random data sequence" and the initial data which was to be encrypted and CRC value go through an exclusive OR (XOR) function which generates the cipher text.

5. The 24-bit IV which is not encrypted is appended to the beginning of the cipher text and finally transmitted wirelessly across the network.

The flaws of the heavily utilised WEP are due to the length of the encryption stream which is 40-bits as per the standard although manufactures provide an option of a 104-bit secret key also. The secret key length is 64 or 128-bit minus the unencrypted IV which creates a 40 or 104-bit secret key (Ciampa, 2006, p.276). Thus as the secret key becomes shorter the encrypted packets become quicker and hence easier to decipher.

As the IV is only 24-bits in length this permits a total of 16, 777, 216 unique IV values which may be created (*ibid*, 2006, p.276). An access point which is constantly in operation may transmit as many as 700 packets a second, therefore within hours the IV will begin repeating (*ibid*, 2006, p.277). An attack is possible when enough packets are captured, in conjunction with the correct equipment which may crack the secret key that was entered into the devise and lead to an offender abusing the wireless network. Newer methods of WEP attack methods include statistical attacks which utilise a brute force and dictionary based attack on the captured network traffic which will present anomalies such as a repeating IV (Guarnieri, Noonan, Pacifico & Taitelbaum, 2005). As was previously mentioned once an offender does gain unauthorised access to the network they may steal bandwidth, download illegal material and access inappropriate information.

2.3.2.3. Wi-Fi Protected Access

Due to the flaws in the initial development of WEP version 1.0, an improved security method WPA (see section 2.1) was introduced. WPA addressed both authentication and encryption (Hänninen, 2003) issues and permitted aged network hardware to utilise the standard with a firmware update. Hänninen (2003) outlines the two modes of WPA, including a corporation based method utilising a RADIUS server, and a personal home method, WPA-PSK (Pre Shared Keys) where keys are entered manually similar to process used in WEP.

WPA uses the temporal key integrity protocol (TKIP) encryption which replaces the weak 40-bit encryption key used by WEP. TKIP uses a per-packet 128-bit key in

contrast to WEP where a manually entered 40 or 104-bit key was used (Ciampa, 2006, p.296). Furthermore WPA includes message integrity check (MIC) which is similar to the CRC in WEP. However, MIC does not fall short in situations where an attacker may alter the initial data and the CRC being transmitted, thus leaving the recipient believing that the packet was not tampered with as the CRC would confirm no alteration (*ibid*, 2006, p.298). TKIP utilises a similar procedure as used by WEP by following the steps outlined by Ciampa (2006, p.305).

1. Rather than combining an IV with a secret key, a 128-bit temporal key goes through an XOR function with the sender's MAC address.
2. The value from step 1 is then combined with a sequence number (previously the WEP IV) which is now 48-bits and run through a function creating a pseudo-random data sequence, as was the process with WEP.
3. Finally the MIC key derived from the initial data (previously the CRC of the data), along with the senders and receivers MAC address are transferred once again through the MIC function which is appended to the initial data and finally placed through an XOR function creating the cipher text.

The flaws associated with WPA have been documented and targeted towards both the personal and enterprise group. Although the enterprise level flaws are beyond the scope of this research, the home user targeted flaws are with the pre-shared key (PSK) (Woodward, 2005, p.161) and cracking tools such as *Cowpatty*. As a PSK is used in home WPA networking instead of 802.1x, during the authentication process via the 4-way handshake the master key may be recovered via a pre-defined function. The master key may be recovered by appending the network name (or SSID) and SSID length to the pass phrase which is then hashed 4096 times identifying the 256-bit master key (*ibid*, 2005, p.161). Hence, even the reported secure approach has associated flaws, thus the home individual may not protect themselves completely. Furthermore, aged network hardware may require a firmware update. An ill-advised individual may turn the wireless router into a non-functional, irreparable device by improper update procedures, destroying the initial working firmware.

2.3.2.4. Wi-Fi Protected Access Version 2

Wi-Fi Protected Access Version 2 (WPA2) is an upgrade from the existing WPA utilising the stronger encryption algorithm, Advanced Encryption Standard (AES) (Tagg, 2003). The Wi-Fi Alliance created WPA2 also known as IEEE 802.11i, has been described as a safer implementation than WPA (Hänninen, 2003). WPA2 utilises 802.1x authentication which as been described as requiring a RADIUS server to authenticate. The encryption method used is that of AES which utilises a 128, 192 or 256-bit key dependant on the level of security required (Ciampa, 2006, p.307). The AES encryption algorithm rearranges and substitutes bytes within the given bit string a number of times depending on the length of the bit string used (Ciampa, 2006, p.295). When a 128-bit key is used bytes are substituted and rearranged a total of nine times, ensuring the encrypted data is free from decryption.

In order for a device to use WPA2 security, it must only support 128-bit keys as a minimum to be WPA2 compliant. This new standard requires newer hardware, which is presumably more expensive for the home user. The technology also requires increased computing requirements which may not run on legacy home equipment.

2.4. Review of Current Specific Literature

It was felt necessary in this research to include the vendor provided literature as a basis for the literature review. As certain aspects could not be retrieved from each manual and suggested as ideal or flawed, best practice design methods were used as the basis for reviewing a set of selected manuals.

2.4.1. Evaluation of Structure and Presentation

The literature which were analysed consisted of vendor manuals and quick start guides provided with home wireless routers. The manuals and guides which were chosen are based on the wireless routers available at Internet Service Providers (ISP) with broadband plans, and those available through retail outlets. A manual has a set of procedures. However, an excellent set of procedures will generally reduce errors, provide information on the most effective way of completing a task, and be suitable for

both a skilled and novice user (Wieringa, Moore & Barnes, 1993, p.3). The manuals were retrieved freely from the vendor websites, although may have been slightly different from original rewritten hardcopy versions, where the author was unable to acquire both versions. Detailed below are five points which are considered essential in any manual of high quality.

1. Perelman, Paradis and Barrett (1998, p. 143), elucidate that a well written manual or guide will utilise descriptive headers, an index, and a table of contents to locate required components with ease.
2. The document should outline the reasons for its creation, the objective and the intended audience, including the required level of expertise (*ibid* et al., 1998, p. 3).
3. A glossary is essential in a document which utilises technical or uncommon terminology (*ibid* et al., 1998, p. 184), such as those found in computing and hardware manuals.
4. White space of at least one inch on all four sides, will make the document presentable, and emphasise points and arguments (*ibid* et al., 1998, p. 36).
5. Graphics, especially screenshots, should be large, to present all information clearly, and where required a separate close up shot used (*ibid* et al., 1998, p. 143).

Table 2 Criteria for evaluating vendor manuals

Manuals	Criteria				
	Headers, Index, Table of Contents	***Objective, Audience, Expertise Level***	***Glossary***	***Layout***	***Graphics***
Billion 7202G (Billion, 2005)	No index page and the contents page, does not have headings for each chapter, and there is a lack of headers on each page.	No objective of manual, no recommended audience or required expertise level outlined.	No glossary of terms.	Paragraphs are not indented, vital points not emphasised.	Graphics are small and not explained in detail.
D-Link G604T (D-Link, 2004)	No index page, the contents page has appropriate headings for each section, and appropriate headers are used for each page.	Clear objective of the manual is provided, however audience and expertise are not included.	No glossary of terms.	Large margins for clarity, although paragraphs are not indented.	Large, clear graphics explained and presented.
Motorola SBG900 (Motorola, 2003)	No index page, the contents page has appropriate headings for each section, and appropriate headers are used for each page.	No objective of manual, no recommended audience or required expertise level outlined.	A detailed glossary page is provided.	Large margins for clarity, although paragraphs are not indented.	Graphics are small and not explained in detail.
NetComm NB5PlusW (NetComm, 2005)	No index page, the contents page has appropriate headings for each section, and appropriate headers are used for each page.	No objective of manual, no recommended audience or required expertise level outlined.	A detailed glossary page is provided.	A lack of white space in margins, and paragraphs and critical points are not indented.	Large, clear graphics explained and presented.
Netgear DG834G (NETGEAR, 2005)	No index page, the contents page has appropriate headings for each section, and appropriate headers are used for each page.	Clear objective of the manual is provided, however audience, a basic to intermediate skill level is required.	A detailed glossary page is provided.	A lack of white space in margins, and paragraphs and critical points are not indented.	Graphics are small and not explained in detail.
Siemens 6520 (Siemens, 2004)	No index page, the contents page has appropriate headings for each section, and appropriate headers are used for each page.	No objective of manual, no recommended audience or required expertise level outlined.	No glossary of terms.	Large margins for clarity, although paragraphs are not indented.	Graphics are small and not explained in detail.

The vendor manual literature according to Table 2 does not conform to any specific publication standards. A glossary of terms is provided in only three of the six manuals, although there is no evidence of an index page in any manuals, which is considered essential in good quality manual design (Perelman et al., 1998, p. 143). In four of the six manuals the graphics appear small in contrast to the other two manuals which are clearly representable and critical elements are easily identifiable. Only one manual outlines the objective and intended audience, with a basic to intermediate knowledge requirement indicated to understand and further configure the wireless router. With the lack of standardisation, and common requirements such as an index and glossary page, both home users and businesses may be running insecure wireless networks and computers by insufficient material in vendor provided manuals. Thus, if home users whom have less time and monetary expenditure, and no access to corporate resources such as trained information technology (IT) staff, could be at a greater security risk than their business counterpart. The study will question and determine what percentage of those sampled solely relied on the vendor provided quick start guide or manual, and their related positive or negative experiences from configuring and utilising the product.

A study conducted by Schriver (1997, p.212) found that of 201 respondents 15 percent would read a manual from cover to cover, 35 percent would use the source as a reference only, and 46 percent would briefly scan through the document stopping at interesting and appropriate headings (*ibid*, 1997 p. 213). The study continued by conducting a case study by designing a very poorly written set of instructions as an example. When the end-users were unable to complete the task, they blamed themselves and rated the experience as negative for not being able to understand the instruction, rather than its content or design (*ibid*, 1997 p. 221). Furthermore, the study revealed that 86 percent of the individuals thought users should be provided with clear, standardised manuals designed specifically at the novice user (*ibid*, 1997, p. 223). The high proportion of individuals requesting well designed manuals contrasts with the lack of standardisation and quality of those provided by the vendors. These are indicators that could possibly identify reasons if individuals or businesses are utilising insecure wireless networks.

2.4.2. Evaluation of Content

A review of literature in section 2.4.1 saw the lack of standardisation throughout manuals, including small, unclear image sizes, no evidence of detailed glossaries and no apparent use of an index in any examined manual. This section will examine the content of the given literature in an effort to determine default security levels, passwords, enforcement of security controls by the vendor, and any security and/or crime statistics provided to further persuade the audience to enforce security methods. The security techniques should be usable (Furnell, 2005, p. 276) whilst not overloading the end-users memory with relevant information which may deter them from implementing the techniques. A positive attitude of understanding the information clearly will encourage the individual to be proactive and implement the required level of security for their use.

'Sniffing' software is used on wireless networks to obtain usernames and passwords to gain access to the network (Karygiannis & Owens, 2002, p. 21). Yet, of the six literature manuals, all were easy to access from the vendors online website, which contained the usernames and passwords required to access the wireless router in the default security state. The manuals show that 60 percent of access points are run with default settings (Shipley, 2001), with the most common username and password combinations consisting of "admin" and "admin" (Billion, 2005; D-Link, 2004; NetComm, 2005). The NetComm and Siemens manuals (NetComm, 2005; Siemens, 2004) do not suggest changing the username and/or password at any point. Thus, anyone using either of the two manufactured devices with no encouragement to change passwords, are leaving themselves open to an offender connecting and changing settings as required, such as increasing the antenna strength.

In regards to the general security structure of the literature, the Netgear wireless router makes constant reinforcements for the need of security (Netgear, 2005, p. 49) such as stating that wireless radio frequencies may expand beyond required ranges, exposing the network to abuse. One area in which the Netgear manual is unique in contrast to the other five is the suggestions for password choice and creation. Unlike the other manuals Netgear suggests not using dictionary based words in any language, with a minimum of eight characters in length, consisting of lower and uppercase letters, numbers and symbols (*ibid*, 2005, p. 61). The method by which this information is presented is closely linked to the requirement of educating users of proper security methods and thus

preventing end-users from choosing passwords of four alphanumeric characters which may be cracked generally within 60-seconds (Hanna, 2005, p. 68).

The vendor wireless router literature provides the default settings for the wireless radio and wireless security. From the six manuals only one vendor has turned off the wireless radio by default (D-Link, 2004). Based on the remaining five manuals four clearly specify that the wireless radio is enabled. The Motorola manual states (Motorola, 2003, p.64) that the default settings allow the end-user to immediately connect wirelessly without the need for altering any settings. Netgear on the other hand specifies the default settings for the wireless router for all features except the in-built wireless (Netgear, 2005). No security features are enabled by default on any of the wireless routers according to the manuals and the Billion (2005) makes no recommendations or enforcement of security measures especially for wireless at any points throughout the manual.

The manuals suggest that in most cases an offender may locate various wireless networks and authenticate and associate with the network, with little or no expertise. With the minimal cost increase of a wireless router in contrast to a router without wireless makes wireless capability an ideal choice for anyone purchasing broadband equipment. The individual may at first think advanced equipment may be beneficial for any future requirements, not knowing that by default wireless and associated insecurities are present on default installations. Initially, the consumer may only use the router for its broadband functionality, although not utilising wireless, leaving it on as by default. The individual may then perceive that by not actually using the wireless technology that they are not at risk, knowing little that an offender may still connect and abuse the network.

2.5. Similar Previous Studies

Over the past few years, numerous studies have been conducted and various articles written to determine how safe and secure consumers and businesses are with regard to computing, networking and the more recent wireless technology (Frisk & Drocic, 2004; Webb, 2003a). Section 2.3 outlined various wireless security methods available for wireless networks, and some of the common flaws and implementations available. Section 2.4 then discussed the structure and quality of content in wireless router vendor

manuals. Section 2.5 is more specifically aimed at previous studies which have been conducted on perceptions, understandings and physical tests to determine how exposed individuals are to the various threats.

2.5.1. Computer Security Relevant to Wireless Networks

A thesis by Frisk and Drocic (2004) conducted a case study to determine individuals' understanding of general computer security and whether they actually were aware and used available security. The sample included ten individuals from 20 – 61 years of age and of various professions including IT professionals, clerks, students and farmers (*ibid*, 2004, p. 81). Although 80 percent of individuals knew what operating system they were using, only 40 percent understood the term administrator mode (*ibid*, 2004, p. 80). Many individuals did not use any form of passwords, and did not know how to implement a strong password (*ibid*, 2004, p. 81).

Findings from the study revealed that an individual who had to permit permission by the use of yes/no on the firewall for each application, decided after the tiresome experience it would be better to uninstall the firewall rather than lowering security settings (*ibid*, 2004, p. 82). Although the case study did focus on a small sample and may not be representative of the majority of users, it does provide an indication of the lack of awareness of individuals and their degree of knowledge in computing and security. These results may be further represented in wireless networking, where respondents may choose to implement no method of authentication due to the hassle of pre-entering keys into each wireless device.

A similar online survey in this area was carried out by AOL and the National Cyber Security Alliance (Schultz, 2005). The study was carried out between, September 15 and October 8 2004, and targeted 329 dialup and broadband users in the United States of America, aged at least 18 years of age, with various income and educational levels (*ibid*, 2005). The study revealed that 84 percent of individuals stored sensitive information on their computer, yet 63 percent did not utilise a firewall. Only 16 percent of respondents understood the difference between antivirus software and a firewall (*ibid*, 2005). The study did not focus on wireless security but revealed that 62 percent of individuals believed they used WEP. Wi-Fi Protected Access (WPA-PSK) was not used

(*ibid*, 2005). The survey failed to ask individual users about their understanding of the risks of using wireless or WEP, or any other security implementations. Whilst this study did focus specifically on users of the Internet, there is a trend of individuals not utilising appropriate security for their computer whilst storing sensitive information. Those individuals with broadband who do have wireless capability in-built into their router, without enforcing appropriate security are allowing offenders to access personal data on their computer. This is simple achieved by criminals sitting in cars and truck in nearby areas using unsophisticated wireless equipment.

It does appear from another study that individuals who have a tertiary computing background may better understand and know how to protect themselves from malicious activity on their computer. In this study, 70 percent of the 140 participants who had a tertiary computing qualification understood the risks, as opposed to 47 percent of business employees (Hu & Dinev, 2005, p.62). However from the 140 participants in the malicious activity survey only 16 percent acted upon and removed malicious software on a continual basis, even when they knew the risks and procedures (*ibid*, 2005, p.63). In a separate study consisting of 1167 respondents, 62.5 percent did not use a combination of alphanumeric characters for their passwords, 48.5 percent had not changed their password in at least six months, and 27.9 percent had their passwords written on paper next to their computer (Stanton, Stam, Mastrangelo & Jolton, 2004). These two separate studies show that in relation to security matters, individuals are not aware of, or do not understand, the risks of malicious applications and basic security techniques such as passwords. It is also interesting that individuals with a tertiary computing background, who did understand the risks and procedures for security, still failed to implement proper protection. The literature suggests that individuals are not securing their computers effectively and utilising basic security procedures, due to a lack of awareness or education about the risks involved.

2.5.2. Wireless Security and Wardriving

The majority of investigations carried out as described in the literature consisted of academics pursuing the area of research, or commercial entities wishing to gain market research in a particular area. The tools which were used in this research included low end laptop computers using *Microsoft Windows 98*, *Mandrake Linux 9.0* or *FreeBSD-*

Stable (Shipley, 2001; Webb, 2003b; Noble, 2001) and freely available software including *Netstumbler*, *dStumbler* or *Kismet*; and a wireless network card. All these items are available for everyday use, and most come with an instruction manual, allowing the knowledgeable academic conducting research or a random offender wanting to steal bandwidth with easy-to-obtain information about the wireless network in use.

Numerous investigations have been carried out in determining the growth rate and insecurity of wireless networks in Perth, Western Australia (Bolan & Yek, 2004a; Bolan & Yek, 2004b). In an investigation by Bolan and Yek (2004a), a surge in the utilisation of wireless networks by a ten fold figure was detected. In January 2003 only 260 detectable wireless networks were discovered compared to the 2668 wireless networks in place by August 2004 (Bolan & Yek, 2004a). Although the results do show the increasing deployment of wireless devices in the Perth Central Business District (CBD), the study did not determine security measures, nor did it cover wireless networks in the outer Perth suburbs.

Similar to investigation by Bolan and Yek (2004a), an earlier study also investigated the growth of wireless networks as part of a thesis and a conference paper (Webb, 2003a; Webb, 2003b), although in this particular study the wireless security techniques were also analysed. Webb (2003b) conducted a scan in the Perth Central Business District (CBD), over the course of a five day period. The study was designed to determine what proportions of the detectable wireless networks had enabled the flawed WEP and were using either the default or a masked SSID. The wireless scan results indicated that over 60 percent did have WEP enabled (Webb, 2003a). Although the study shows that just over 60 percent have WEP that appears to be secure, the amount of information on flaws in WEP (Section 2.3.2.3) must question whether those businesses that were WEP enabled are really all that secure. A paper by Bolan and Yek (2004b) analysing the security techniques used by businesses in the CBD of Perth discovered similar results with almost 50 percent of businesses utilising WEP as their primary method of wireless security. If these results are translated into how secure home wireless networks are then the figures would represent that six of ten networks are open to abuse. Furthermore, as corporations have network administrators and technical staff unlike home users, then the figures for home users should prove only worse.

The results of studies in Perth, outlining exposed insecure wireless networks coincide with a similar study which took place in the Brisbane CBD on a smaller scale. The study in Brisbane which took place in 2003 was conducted with two scans separated over a 12 months period (Pollard, 2003). The initial scan had discovered 35 wireless networks, whilst the second scan just over a year later, had identified 87 wireless networks of which 32 percent were not using WEP (*ibid*, 2003). Figure 4 and Figure 5 (shown below) show the comparison of the results from the Perth and Brisbane CBD and resemble almost identical results. Those without WEP are highly exposed while those with WEP are utilising a flawed means of protection.

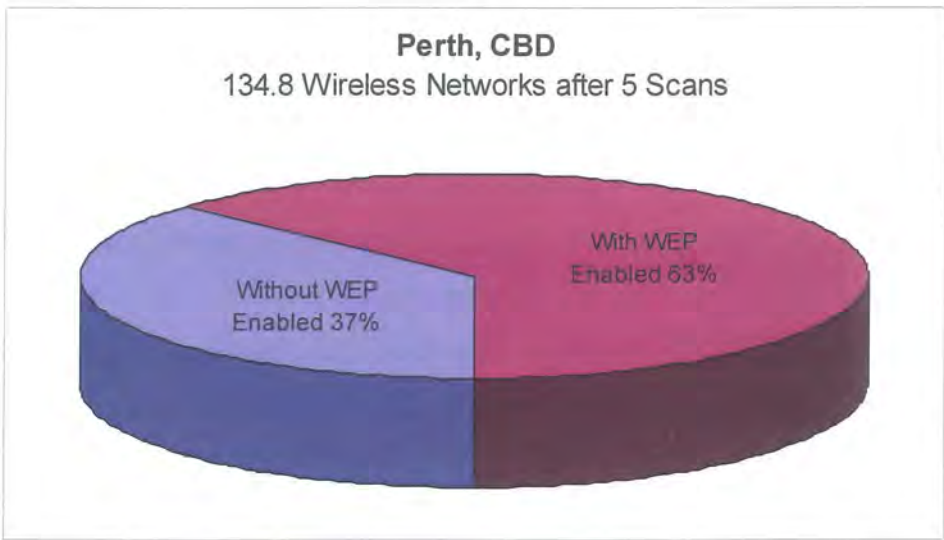


Figure 4 Portion of detectable wireless networks in Perth, CBD without WEP (Webb, 2003b)

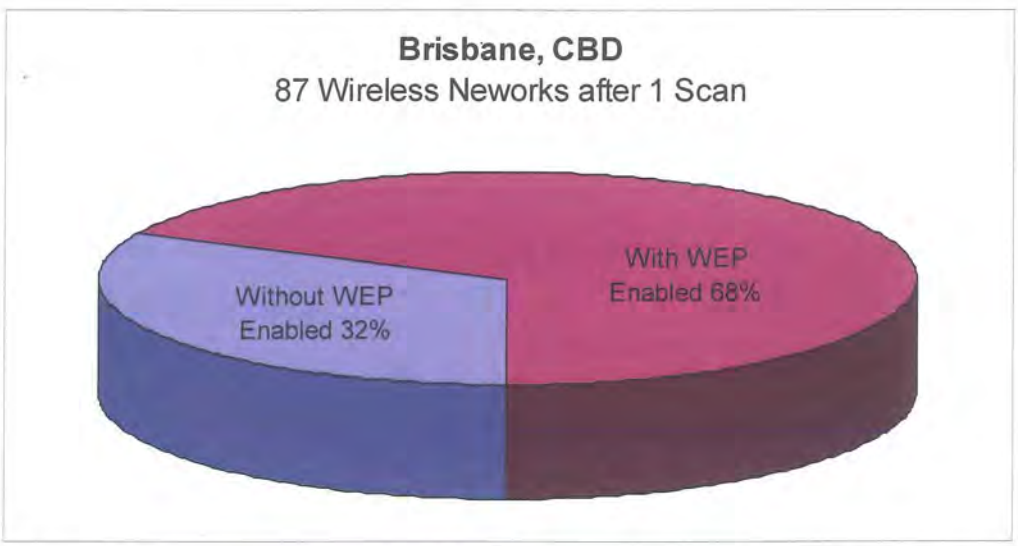


Figure 5 Portion of detectable wireless networks in Brisbane CBD without WEP (Pollard, 2003)

Not only are the wireless networks vulnerable to various means of attacks, the scan in Brisbane was also able to identify particular companies and organisations, acquire the default settings, and identify the hardware manufacturers. The study identified 29 wireless networks that were utilising an SSID which with little difficulty could be used to identify the company or organisation (Pollard, 2003). Each manufactured wireless router has known publicised exploits, with the scan revealing that 55 of the wireless networks detected were using either a Cisco, D-Link or Netgear access point (*ibid*, 2003). Likewise for home users an attacker may identify the particular access point manufacturer which is being used. This information may be used to find the known exploits against the access point, with various side affects including a DoS, leaking of private information or corrupting the firmware.

A wardriving study in the USA on the utilisation of security techniques in wireless networks was carried out from the year 2000 over an 18 month period (Shipley, 2001). Over the course of the 18 month period approximately, 60 percent of the access points located were active in their default configuration mode (*ibid*, 2001). Furthermore, 85 percent of the 9000 networks detected, did not utilise WEP, while of those actually using WEP, 7 percent were using the default vendor encryption key. The vulnerable wireless networks existed within households, banks, hospitals and shopping centres (*ibid*, 2001). Each scan collected Global Positioning System (GPS) co-ordinates, security configuration, channel frequency, signal strength and the SSID. These figures are very high considering the high publicity in the media regarding the threats in deploying wireless networks (McCue, 2001; Noble, 2001; Ward, 2002). The behaviour of high profile entities such as banks and hospitals represents that security is not a major concern, and thus the cause of little or no implemented wireless security. If this same representative behaviour is forwarded to the home user, then presumptions would show that home users would also neglect the threats as a concern and hence would not implement wireless security.

In Reykjavik, Iceland, wireless network coverage to access the Internet is provided for numerous neighbourhoods (Clyde, 2003, p. 44) which was first introduced as a trial and now is a permanent addition. Clyde (2003, p. 45) explains how various telecommunication companies around the world such as British Telecom, introduced manuals and guides, explaining the process of configuring a wireless network with step-

by-step procedures. Although the step-by-step procedures are provided, there is no mention of the policies governing those individuals who do not wish to have wireless capability at home. Wireless security cannot be initially implemented in products throughout these neighbourhoods as the default settings may be unsuitable for many end-user needs (Furnell, 2005, p. 275). Furthermore, many users will not utilise a significant portion of the available security on products due to a lack of accurate or inaccurate understanding of the functionality and required procedures.

Lim (2003) had conducted a wireless network deployment survey between the 21st and 31st of January, 2003 in the effort to determine the use and structure of wireless networks within organisations. The study revealed that only 45 percent (*ibid*, 2003, p. 18) of the 46 responding organisations had implemented a clear wireless security policy. The research also discovered that 61 percent of organisations were using wireless networks as a means of connectivity to confidential resources, while only 46 percent of respondents in any category had, or planned to implement the various available wireless security techniques (*ibid*, 2003, p. 19). Further results of this study are presented in Table 3.

Table 3 Results from a wireless network deployment survey (Lim, 2003)

Question	Percentage
Changing default SSID, default passwords, default channel, cryptographic key	46%
MAC access control list	35%
Turning of the Access Point when it is not being used or after hours	11%
Conducting of site surveys to prevent wireless coverage beyond the required range	28%
Implementation of WEP with rotation of keys and a minimum key length of 128-bits	35%
Ensuring end-users are trained and aware of computer security and wireless risks	43%

The results from the survey by Lim (2003) indicate a low awareness and implementation of wireless security within businesses and organisations. The wireless studies show a consistently negligent attitude to the implementation of wireless security within organisations and businesses that commonly have an IT department and would

assumingly have resources allocated to secure the networks. Assumingly home users do not have resources to allocate towards wireless network security, staff or professional maintenance, and thus rely heavily on well written documentation as a reference. Furthermore, home users are not at any point informed of the risks in utilising wireless, and thus, there is no motivation for an individual to implement appropriate wireless security methods.

A revised commercial study carried out in November 2003, and earlier in 2001 by NOP World Technology on behalf of Cisco Systems (Cisco, 2003) compared wireless usage among end-users, Information Technology (IT) staff and company managers. A major outcome of this study revealed that end-users were not concerned with wireless security (possibly due to a lack of awareness), unlike IT staff. Furthermore end-users rated mobility as the greatest personal benefit, while the difficulty of installation as the greatest of concern (*ibid*, 2003). Unfortunately the study did not examine why end-users were not concerned with security, or their awareness of the wireless network threats.

All the studies in wireless network security represent insufficient security implementations by many of the businesses in Perth, London and the USA. As mentioned previously, in a targeted towards home users of their perception and knowledge of computer security, it appeared that home individuals were lacking the implementation of computer security just as businesses are now lacking wireless security. The 2005 Australian Computer Crime and Security Survey (AusCERT, 2005) shows that since 2001 businesses have implemented a higher level of computer security such as implementing new security standards, which rose from 37 percent in 2003 to 65 percent in 2005. Detailed studies on wireless networks at home do not appear to have been conducted or reported in the literature, although it appears home individuals are always a step behind businesses in being informed and thus implementing appropriate security. This study determines whether wireless security knowledge in home environments is equal to, or less than the security measures employed in businesses.

In an investigation of wireless network security knowledge and reactions, comments that were gathered during the interview showed a lack of understanding towards the risks. Individuals who participated in the study had reported that risks were present but would be easily fixed by the vendors in the near future (Webb, 2003b, p.82). The wide

range of comments show a lack of publicly available information and awareness with individuals stating that no one should be utilising an 'out of the box' wireless network configuration (*ibid*, 2003b, p.83). However, another individual stated that they did not know of any risks when utilising a wireless network (*ibid*, 2003b, p.84). The comments suggest that individuals are not being informed of the wireless security risks, nor are they researching the risk in utilising the technology themselves.

2.6. Literature Summary

The literature review covered a broad range of topics showing the issue of using 802.11 wireless networks at home. Wireless networks do use any interconnecting wires between devices which are communicating. This technology is being used in numerous locations consisting of homes and businesses right through to hospitals who store sensitive, private patient data. In the locations listed, the wireless technology may appear to be a cheaper approach in contrast to laying out cable throughout an entire home or hospital. Alternatively in certain buildings such as heritage listed homes, laying cable may be illegal and hence using a wireless network is the only option available. Whilst the reasons for implementing a wireless network by individuals are endless, the technology requires a sound understanding of the risks and security requirements, which few individuals may have.

Wireless networks use radio waves hence an attacker does not need to be directly connected to the network via a cable. The various attacks present include DoS which can disrupt productivity and render a wireless AP useless for the duration of the attack. A man in the middle attack may leak private information to a third party, hence losing confidentially and as such could be used to commit bank fraud or identity theft. Whilst the threats are present, so are countermeasures which by default are disabled by vendors to create an easy configuration process for the home user. Default or basic security features are easy to implement, and may provide a hassle free configuration process, although do not provide strong security to a skilled intruder due to design flaws. In contrast high-end security such as WPA or better still WPA2 require additional knowledge for proper configuration, and in some instances newer, more powerful hardware.

The literature review covered the lack of emphasis and persuasion by vendors in their manuals to implement security. The provided literature encompassing the purchased hardware did not follow any standard, and hence the majority lacked basic features including a glossary or large clearly defined graphics which are considered essential in good manual design standards. The individual choosing to implement a wireless network is not presented with the risks or vulnerabilities in the manuals, nor is the recommended security features discussed in detail. The ill informed individual is not discouraged from implementing a wireless network, and literature review then saw that home users and businesses are in turn utilising insecure wireless networks and computers.

Previous studies saw that both businesses and home users were utilising computers and wireless networks with security implementations or in some instances no security. Wireless networks are operational that are utilising a flawed encryption standard however vendors are not educating users to stay clear of such methods. Alternative studies identified that even though individuals perceived their hardware to be secure, physical tests which were undertaken proved otherwise. This research aimed to determine the extent of wireless security knowledge of users in home environments, and their perceptions and understandings of utilising the technology.

CHAPTER 3. RESEARCH METHODOLOGY

Chapter 1 and 2 discussed why the study needs to be undertaken, including the benefits of wireless networking and identified literature underpinning the wireless security dilemma. The literature further detailed the increase in home wireless networking products, yet a lack of literature explaining the requirements, security and usage instructions. This chapter identifies the paradigms and research methodology used to carry out the research. It then leads into the justification of the research method, including identification of the weaknesses and how these are countered. Finally the chapter concludes on the identified issues of confidentiality and ethics, and how these are maintained and ensured throughout the duration of the research.

3.1. Research Method

Quantitative and qualitative research is subject to two different philosophies of thought, and manipulate the means by which a researcher collects, analyses and interprets the data (Ary, Jacobs & Razavieh, 2002, p.22) A research paradigm is based on a model that leads our understanding and furthermore governs the researchers philosophical approaches and actions towards a given area (Babbie, 2005, p. G7). The philosophical approaches used in this project are of quantitative research based on the positivist paradigm.

Positivism is a philosophical point of view developed in the 19th century, and adheres to the belief that principles and laws govern the social and physical world, and thus permits generalisation and predictability from the analysed gathered results (Ary, Jacobs & Razavieh, 2002, p.22). The positivist approach investigates relationships, causes and effects (*ibid*, 2002, p.23) using deductive reasoning which is then tested for its validity. As is indicated by the literature review, a majority of businesses whom use corporate wireless networks are insecure. Furthermore individuals at home using a computer are insecure in relation to general computer security, thus the theory that individual's using wireless networks at home are insecure may be tested and validated.

Knowledge to a positivist is a 'thing' (Hinchey, 1998, p.39) which can be both tested and verified for its factuality. As Blaikie (1993, p.95) explains the positivist generates very general statements and theories which enable the researcher to predict behaviour and phenomena. The predictions developed by the author and his positivist views may be tested via a means of experimental or non-experimental research. Experimental research encompasses manipulation of one or more independent variable in order to determine the result this has on a dependant variable through observation (Ary, Jacobs & Razavieh, 2002, p.276). Alternatively the non-experimental approach was chosen for this project where variables are chosen although not manipulated. Various quantitative non-experimental methods exist including *ex post facto* and *correlation* although the author has chosen the survey research method was chosen and is justified in the following section.

3.2. Survey Research

Survey research utilises various instruments including questionnaires and interviews in order to acquire a degree of information about a group of individuals (*ibid*, 2002, p.25). By utilising a survey approach on a sample population, the researcher may generalise and also determine in what manner the sample may represent a given population. Surveys are similar to a wide nation census being different in that a survey will target a sample representative of a specific population (Babbie, 1990, p.36). Survey research reportedly dates back to ancient Egyptian civilisation time, when rulers used the approach to gather data about their people (*ibid*, 1990, p.37). Today survey research is common in marketing strategies, political polling and is used extensively in academic based research.

Survey research may target various characteristics of individuals although the author has identified two important topics relevant to the research. Individuals will generally have the same attitude towards an area for weeks, months or even years (Alreck & Settle, 1995, p.11), and this is only altered when the individual learns new information or gains experience through interaction. An attitude may be broken into three parts including; what an individual knows, their feelings and experience towards a topic, and the corresponding action the person will take in relation to their attitude (*ibid*, 1995, p.11). The author thus ensured that the survey instrument incorporated all three of the

attitudinal measurements in order to understand the attitude individual's posses towards wireless networking at home.

The identified characteristic common to this research is that of an individual's attitude and thus behaviour towards wireless networking at home. Ones attitude may identify their awareness of the wireless risks and hence feel vulnerable and proactive towards wireless security, whilst the behaviour may show otherwise. Behaviour in survey research may be identified by the following (*ibid*, 1995, p.19):

- The actions of an individual.
- The time before the action took place.
- If the action is persistent.
- Where the action finally took place.

The survey instrument questions if the individual queried security during the purchase of the good, if they themselves configured the device or relied on someone else and lastly whether or not they have checked their current security status.

3.3. Strengths and Weaknesses of Survey Research

Survey research has strengths and weaknesses like all research methodologies and has the potential to be worthless or worth vast amounts to various parties depending if quality research practices are adhered to (*ibid*, 1995, p.7). As discussed by Czaja and Blair (2005, p.35), the various forms of major survey research include mailed questionnaires, Internet surveys, telephone surveys and fact-to-face interviews. The three criteria for evaluating survey research include; resources, questionnaire characteristics, and quality of data. The strengths and weaknesses will be discussed, although the identified weaknesses are not necessarily a negative aspect in this study.

Internet surveys are comparatively advantageous in terms of resource allocation to the cost of mailed questionnaires and telephone surveys (*ibid*, p.35; May, 1993, p.73). Whilst Internet based surveys generally have a data collection period of up to three weeks, other methods have been rated as requiring anywhere from four to twelve weeks thus requiring more resources. As time is a factor in this study to collect the largest sample the data collected needs to maintaining a high response rate.

Questionnaire characteristics include survey length, complexity, visual aids and sensitivity of questions (Czaja & Blair, 2005, p.35). Internet surveys have been rated poorly in terms of the length of the questionnaire where respondents are willing to permit 15 minutes maximum (Czaja & Blair, *2005*, p.36; May, 1993, p.74). This negative limitation does not disadvantage the utilised survey instrument as the pilot study which was conducted identified that the survey required a maximum of 10 minutes to complete. Telephone and face-to-face interviews are difficult methods to present graphical images for questions, whilst the Internet survey can present large, coloured graphics which is a requirement for the research. Although Internet surveys are the worst means by which to ask sensitive, personal information (Czaja & Blair 2005, p.36; Alreck & Settle, 1995, p.7), no questions of this type are asked throughout the survey.

The quality of data issue relates to the response rate, the quality by which responses are recorded and bias towards a topic (Czaja & Blair 2005, p.36). The greatest disadvantage with Internet surveys is that the response rate is bias towards a group of individual's whom have access to the Internet. It was acknowledged that this may be a problem in other research investigations, although this study is aimed at individuals whom use wireless networks at home. Wireless connectivity in a home environment requires a wireless access point which is in-built into broadband routers as discussed in chapter 2. Thus, the individuals participating in the study have both Internet access and wireless connectivity. The quality of recorded data is high as data is entered directly into a database and thus does not require the researcher to note down responses or translate mailed questionnaires into a database.

As Alreck and Settle (1995, p.8) point out, survey research will not generate definitive answers to research questions. Rather survey research will provide indicators and trends thus allowing generalisations applicable to the population to be determined. Ethics is explained in greater detail in the next section although survey research has the advantage of being confidential and anonymous, so long as the respondents are selected in a manner which will not identify the individual (Babbie, 1990, p.341). The author has taken into consideration confidentiality, and thus an anonymous survey will ensure a high response rate, so that the indicators are most accurate.

3.4. Confidentiality and Ethics Considerations

Ethics and confidentiality were identified as an important aspect in undertaking the study. Not only are their ethical requirements set by the Edith Cowan University Ethics Committee, but there are ethics which govern best practise research techniques. Ethics is the acceptance and thus, abiding by, the standards of a profession or group (Babbie, 2002, p.56). An ethics application was submitted. The ethical considerations outlined in the application and those by the research considered: allowing voluntarily participating, preventing harm and endangerment, ensuring anonymity and confidentiality, and finally ensuring integrity in the analysis and reporting of results (Babbie, 1990; Czaja & Blair, 2005, p.239).

The people in the sample were informed that participation was voluntarily and the survey may be ceased at any point. As Babbie (1990, p.339) outlined, survey research has a high potential to be intrusive into individual's lives, yet the researcher may prevent this extremity. The participants were informed that the final results will be stored in a secure encrypted environment and that in no manner will respondents be identified.

Survey research has the potential to question participants on matters with which they may normally not concern themselves (*ibid*, 1990, p.341). Although in some instances, it is possible for respondents to be harmed or put them in danger by their responses, the study does not identify nor cause any harm to individuals. Babbie (1990, p.342) points out that anonymity and confidentiality are vital in any survey research to both protect ones identify and ensure they are not endangered. Unlike interviews the questionnaire was completed anonymously, meaning the author cannot connect a set of responses cannot be lined to a given individual. Secondly, confidentiality was ensured throughout the study as only the author has access to the data collected which is stored securely.

3.5. Survey Instrument

The survey research instrument for used in this study was a questionnaire consisting of 29 questions (See Appendix A). The questions consisted of dichotomous response, Likert scale, filter and contingency, and demographics which are ideal in good survey

research (Trochim, 2001). The structure of the survey ensures that the opening questions are easy to answer whilst maintaining an unbiased tone towards the remainder of the survey. Alreck and Settle (1995, p.88) present three characterises which questionnaires should follow including; focused, clearly expressed, and use brief questions. It was ensured that each question was focused on a single element per question rather than asking many issues at once. Secondly, each question was brief and did not require the respondent to read over the question numerous times before they chose an answer, as this may possibly confuse or alter their opinion. Lastly, it was ensured that each question was clearly represented, and thus no technical terminology in questions has been used. The questions were designed to prevent multiple interpretations from questions.

A pilot study is an informal survey of a small group of participants which test the survey instrument and ensure its feasibility (*ibid*, 1995, p.69). The pilot survey allowed the determination of the time requirement to complete the survey as well as the complexity and hence level of understanding respondents had of each question. The process was iterated numerous times and feedback was provided by participants. The survey was altered and re-issued to ensure that wording was at a level that all participants would understand and thus would not confuse the individuals with complex computing terminology. A further pilot study was then conducted on the online survey instrument which was a replica of the paper based questionnaire. This second pilot test ensured that the web page and database were functional, and that negative experiences were not encountered.

The survey structure was separated according to the topic being investigated. Just as marketing surveys are grouped according to purchasing behaviour, product appearances, and lifestyle choice (*ibid*, 1995, p.153), the survey instrument was sorted by general information, knowledge and associated behaviour, perceptions, and basic demographics. By grouping topics of research together the respondents focused on the same issue and thus would respond to similar items with ease (*ibid*, 1995, p.154).

The first section consisted of five questions on the survey instrument which asks general information of the user and determines if they may proceed with the remainder of the survey depending on their responses. The second section determined the amount of

knowledge the individual has of wireless networking by questioning their choice of security methods, and placement of their wireless router. Following is a section aimed at determining the individual's perception towards wireless networking, and how vulnerable they believe they are by utilising the technology. Lastly, the fourth section describes the basic demographic data including, age, sex and postcode.

3.6. Justification of Survey Instrument Questions

This section will briefly present and justify each question in brief, of the survey instrument presented in full in Appendix A.

Question 1 permits the respondent to continue with the survey, or will stop and thank them for not meeting the requirements.

1. *I have a wireless connection for my home or small office computer*

Question 2 is aimed at determining the available bandwidth which may be abused in an insecure wireless environment.

2. *I use the following connection type to connect to the Internet at home or in my small office.*

Question 3 will determine if respondents are investigating an Internet Service Provider, and if the trends show that the commercialised providers are predominantly chosen.

3. *I use the following company when connecting to the Internet.*

Question 4 will be used to make comparisons among those working in the IT industry and those who do not. The comparisons will endeavour to determine if those working in the IT industry are more conscious of security when utilising an 802.11 wireless network.

4. *I am currently working or have worked previously in the **IT industry**.*

Question 5 determines the percentage of respondent who have previously configured a computer network successfully and hence used in conjunction with further questions to determine if this has made a significant difference in their perception of wireless security.

5. *I have **successfully** configured a computer network*

Question 6 provides a 'check' to determine if respondents are aware of both benefits and negativities associated with configuring and using a wireless network.

6. *I chose wireless rather than using a cable to access the Internet because.*

Question 7 was provided to determine if salespeople have discussed security issues while the respondent was purchasing the wireless product.

7. *Was **any** security discussed with you when you purchased the wireless computer product?*

Question 8 determines if the respondent considered security a priority, and hence, if they enquired about specific features before purchasing the product.

8. *When you purchased your wireless computer product, did you enquire about **any** security?*

Question 9 provides common options for respondents to choose which they considered important for the product to have. This determines if respondents required basic security methods or advance uncommon methods such as WPA2.

9. *If you chose 'yes' to question 8 which specific security features were important to you?*

Question 10 provided the option for respondents to choose who setup their wireless network. This was to determine if respondents were relying upon themselves and hence would have some knowledge of what security features and were sources used.

10. *Who setup your wireless computer product?*

Question 11 allows respondents to select the sources of information used to configure the wireless network, and thus, would be used to compare sources of information used and their knowledge and level of implemented security.

11. Where was information obtained from to setup the wireless product ***(choose all that apply)?***

Question 12 was to be used in conjunction with question 11 and the initial question to determine who has a valid, accurate understanding of the security features they had implemented along with the sources of information used.

12. *Which of the following security features are on your wireless computer product?*

Question 13 provided a graphic of a house allowing the respondents to select the position of the AP which would then determine the respondent's susceptibility to such attacks bandwidth abuse.

13. *The physical placement of the wireless box in my home or small office is* ***(choose most appropriate)***.

Question 14 was to be used in conjunction with question 13 to further determine susceptibility levels, and to determine if respondents who have worked in the IT industry are more conscious of simple security checks.

14. *The physical placement of the wireless box in my home or small office is* ***(choose most appropriate)***.

Questions 15 through to 19 were attitude concern, 4-point Likert Scale questions on issues surrounding the wireless technology. These would be used to determine if there are one or more concerns which are prevalent and to provide a tallied score to each respondent of their overall concern.

15. *Money loss due to wireless fraud.*

16. *Theft of bandwidth.*

17. *Ensuring personal data is not exposed.*

18. *Ensuring wireless is always available.*

19. *Ensuring personal data has not been altered.*

Question 20 was a Likert Scale question determining respondents perceived vulnerability of their wireless product, which was to be compared with previous question on knowledge of implemented security features and purchasing behaviour.

20. *How* ***vulnerable*** *is your wireless product?*

Question 21 was to be compared with question 20 to determine if respondents who believed their product was vulnerable also believed they were at risk for using wireless to access the Internet.

21. Do you believe you are at risk by using wireless to access the Internet?

Question 22 and question 23 were 4-point Likert Scale questions of respondents utilising and configuring of their wireless product. This was to be used in conjunction with previous questions to determine if a positive attitude impacts the security methods or sources of information used.

22. What has been your experience of configuring you wireless product?

23. What has been your experience of using your wireless product?

Questions 24 through to 26 inclusive were basic demographic questions to determine if the sample is representative of the academic population and hence have a basic profile of the people who completed the survey.

24. Please specify your age group.

25. Gender

26. *Location.*

CHAPTER 4. RESULTS

This chapter will present the results which were gathered from the online survey instrument. The chapter has been divided into sections according to the main and sub questions created and explained in Chapter 1. The online survey instrument was accessible from 11 May 2006 to 2 June 2006, allowing a three week period for data collection. Over the twenty-one day period a total of 198 submissions were made of which, 9 responses were blank or invalid.

Further analysis of the data identified several cases where a respondent's submission had been duplicated. These duplicated results appeared as consecutive rows in the database with the identical content in two, three or four rows. After careful examination it was discovered that occasional delays may have been present between the server and a slow connection on the respondents end. In such a situation this meant that the respondent would click 'finish' multiple times hence resubmitting the results to the database repeatedly. A total of 26 duplicate submissions were found and removed, leaving a total of 163 legitimate submissions.

A sub-set of 163 people of the target population randomly chose to voluntarily undertake the survey. An invitation and a link to the online survey instrument were posted on the "news and events" section of ECU faculty websites. Of the sample group 61.3 percent belonged within the 18-24 age group, 22.7 percent within the 25-34 age group, 9.8 percent within the 35-44 group, 5.5 percent within the 45-54 group, 0 percent were within the 55+ group, and 0.6 percent were unspecified. The sample group consisted of 21 percent female, 78 percent male and 1 percent had unspecified.

Table 4 outlines the proportion of high-speed broadband use in contrast to dialup, amongst male and female respondents to the survey. The prevalent connection type is broadband which is utilised by 94.5 percent of respondents in contrast to dialup which is used by 3.7 percent. This evidence presents the current trend towards high-speed broadband Internet access, with the decline of dial-up users, consequently allowing increased bandwidth available to wireless network exploitation by offenders.

Table 4 Male and female respondents using broadband or dialup

N=163	**Male**	**Female**	**Unspecified**	**Total**
Broadband	119	33	2	*154*
Dialup	6	0	0	*6*
Other	2	1	0	*3*
Total	127	34	2	

4.1. Behaviours and Perceptions of the Collective Sample

This section will analyse the results for the complete sample (163 respondents). This is in contrast to section 4.2 which analyses subgroups within the complete sample.

4.1.1. Questions on Wireless Background Information

Question on Internet service provider popularity

The respondents were given the opportunity to select their ISP from five pre-determined options that were listed, as well as having an 'other' option. The predominant ISP choices among respondents were *iinet* and *Westnet* and providers not specified (other). *Telstra Bigpond* was also popular, while Optus and *Iprimus* were not often selected. Table 5 identifies that respondents are not choosing the highly commercialised ISP's such as *Bigpond, Optus, Iprimus* and *Dodo*. Evidence shows that respondents are being knowledgeable and hence aware of the various offers and options provided when choosing broadband. Thus respondents do not appear to be simply choosing those predominately shown on television advertisements.

Table 5 Internet Service Provider choice amongst respondents

Internet Service Provider	Number of respondents	Percentage
iinet	44	26.9%
Westnet	25	15.6%
Telstra Bigpond	19	11.7%
Optus	6	3.6%
Iprimus	6	3.6%
Dodo	3	1.8%
Other	60	36.8%

Questions on IT industry and networking experience

From the sample of 163 respondents 50 percent previously or are currently working within the IT industry, and almost 90 percent had configured a computer network (Table 6). Hence the results should show (although do not) a strong tendency for respondents to be both aware and not at risk when utilising a wireless network.

Table 6 Comparison of IT industry and networking experience

N=163	**Worked in IT**	**Not worked in IT**
Configured network successfully	84	60
Not configured network successfully	1	18

Question on reasons for choosing wireless

Respondents were provided five options to determine the reasons they chose a wireless connection. Two of these options, namely "speed" and an "easy setup process" were not valid reasons since they are not beneficial characteristics of a wireless network. The majority of respondents did not select and hence are possibly aware that speed and an easy setup process are not benefits of a wireless network (Table 7).

Table 7 Reasons for choosing wireless amongst the sample

Reason	Total number	Percentage
Convenience	114	69.9%
No messy cables	98	60.1%
Mobility	131	80.4%
Speed	6	3.5%
Easy setup process	19	11.7%

4.1.2. Questions on Knowledge and Behaviour

Questions on purchasing behaviour and experience

The 802.11 wireless network protocols are reasonably new and constantly changing with newer standards and security methods. The risks and countermeasures are not always publicised and so vendors and salespeople are in a good position to discuss security methods. An ill advised individual may not be aware of newer, secure encryption methods available on certain product types. Hence the salesperson may have the opportunity to play a vital role in informing the individual of beneficial security methods across various products. As the results indicate, salespeople are not making use of the opportunity to discuss security related matters. From the sample only 36 respondents (22 percent) had a salesperson discuss wireless security risks and countermeasures.

As salespeople are not advising or discussing wireless security risks and countermeasures, it is up to the respondent to be well informed and hence question specific security features. There were 67 respondents from the sample who had questioned security features at the time of purchase (41 percent).

Questions on Sources of Information for Configuration

Most vendors are releasing default out of the box configurations for broadband and wireless connectivity, although minor or a total reconfiguration may be required. Respondents were asked who setup their wireless product (Table 8), and what sources

of information were used (Table 9). Table 8 shows that the majority of the sample had configured the wireless network themselves.

Table 8 Resource used to configure wireless products

Person who setup wireless product	Number of respondents	Percentage
Myself	140	85.8%
Household friend	12	7.4%
Outside friend	5	3.1%
Technician	5	3.1%

Prior knowledge and the previously discussed flawed vendor quick start guide (See Chapter 2) were relied upon predominantly. The "other" sources included; working in the field, completing a course in wireless, and a trial and error approach (Table 9).

Table 9 Sources of information used amongst respondents

Source of information	Number of respondents	Percentage
Prior knowledge	110	67.5%
Vendor quick start guide	61	37.4%
Internet	18	11.0%
Support from friend	11	6.7%
Technician	2	1.2%
ISP Support	2	1.2%
Other	10	6.1%

4.1.2.1. Questions on Security Features and Susceptibility

The sample had the choice of selecting predetermined security features which they perceived to have on their wireless product. As discussed in the literature review, *Open System* and *Shared Key* are the common methods of authentication used by respondents at home. Cryptographic techniques including *WEP*, *WPA/WPA-PSK* were among the encryption techniques provided. Those who provided an invalid response i.e. selected

Open System and *Shared Key* authentication, or *WEP* and *WPA/WPA-PSK* encryption have been noted as a false response. If the respondent had left the answer blank or selected "don't know" this was categorised as unspecified.

Table 10 shows that the majority of respondents did not know (63 percent) the authentication method on their wireless product, even though the majority had used prior knowledge as a source of information (section 4.1.2.2). False responses were the second highest response recorded which accounted for 18 percent of the sample.

Table 10 Authentication methods used by sample

Authentication method	Number of respondents	Percentage
Open System	12	7.4%
Shared Key	20	12.3%
Don't Know / Unspecified	102	62.5%
False Response	29	17.8%

Table 11 indicates that the majority of respondents did state a valid perceived encryption method. Although a number of false responses were tallied (39 percent), there was a marginal percentile difference between those using WEP or WPA/WPA-PSK (22 and 18 percent respectively).

Table 11 Encryption methods used by sample

Encryption method	Number of respondents	Percentage
WEP	36	22.1%
WPA/WPA-PSK	30	18.4%
Don't Know/ Unspecified	34	20.9%
False Response	63	38.7%

4.1.2.2. Questions on AP Positioning

Of the 163 respondents from the sample, a graphical question was asked aimed at investigating the physical placement of the AP. As Table 12 presents the majority of respondents (51 percent) positioned their AP in the centre of the house. Hence, since the wireless radio wave must traverse through interfering walls, the majority of respondents would be reasonably free from signal leakage. A second question determined if the individual had checked if the AP was positioned in a manner that was propagating a signal beyond their property. The majority of respondents (53 percent) have checked if wireless coverage was available beyond their property.

Table 12 Position of wireless AP

AP Position	Number of respondents	Percentage
Street front	22	13.6%
Side or rear of house	57	35.2%
Centre of house	83	51.2%

4.1.3. Questions on Perception and Attitudes

4.1.3.1. Questions on attitude concern towards wireless security

Respondents were presented with five 4-point Likert Scale questions to test their attitude concern towards wireless security issues. Of the 163 respondents, 158 completed all the Likert Scale questions. Table 13 shows that there is an almost equal low dispersion of concern among respondents towards money loss due to wireless fraud and theft of bandwidth. In contrast, respondents had stronger concerns scores towards other issues including ensuring personal data is not exposed, ensuring availability of their wireless network, and ensuring that their personal data is not exposed. The evidence suggests that respondents may believe that money loss, and bandwidth theft occur less frequently, and hence are concerned predominantly with threats which may impact them instantly.

Table 13 Attitude concern towards wireless security issues

Wireless Networking issues	Number of respondents			
	Not concerned	Slightly	Moderately	Extremely
Money loss due to wireless fraud	48 (30%)	33 (21%)	30 (19%)	47 (30%)
Theft of bandwidth	35 (22%)	33 (21%)	47 (30%)	43 (27%)
Ensuring personal data is not exposed	23 (14%)	22 (14%)	39 (25%)	74 (47%)
Ensuring wireless is always available	7 (4%)	25 (16%)	56 (35%)	70 (45%)
Ensuring personal data is not altered	16 (10%)	22 (14%)	43 (27%)	77 (49%)

Questions on perceived vulnerability

Respondents were asked if they believed they were at risk for using wireless to access the Internet, and further if they perceived their wireless AP to be in a vulnerable state. From the entire sample, 161 respondents had answered both questions. As Table 14 shows, 49 percent (combining percentages of "extremely" and "moderately" vulnerable) believed their wireless AP was moderately or extremely vulnerable to a wireless attack. When asked if they were at risk, only 75 respondents (47 percent) believed they were at risk when using wireless to access the Internet.

Table 14 Perceived vulnerability of wireless AP

Perceived vulnerability of AP	Number of respondents	Percentage
Extremely vulnerable	11	7%
Moderately vulnerable	68	42%
Not vulnerable	59	37%
Don't know	23	14%

Experience configuring wireless network

Respondents were given the opportunity to state their positive or negative experiences for both configuring and using their wireless network, using a 4-point Likert Scale (Table 15). From the sample, 161 respondents had completed both Likert Scale

questions. The results indicate that the majority of respondents have had positive experiences utilising and configuring the wireless network.

Table 15 Respondents experience configuring and using wireless networks

	Positive	**Slightly Positive**	**Slightly Negative**	**Negative**
Experience using	87 (54%)	60 (37%)	11 (7%)	3 (2%)
Experience configuring	83 (52%)	58 (35%)	17 (11%)	4 (2%)

4.2. Behaviours and Perceptions of Specific Groups

4.2.1. Breakdown of Networking and IT Industry Experience

A respondent who has worked in the IT industry and successfully configured a computer network assumingly has a better understanding and awareness of the issues surrounding the wireless technology. In light of this the 163 respondents were divided into four groups (referred to as A, B, C, D) depending if the respondent currently or previously worked in the IT industry, and secondly if they had at any point successfully configured a computer network.

- Group A consisting of 83 respondents have worked in IT and successfully setup a computer network.
- Group B consisting of 1 respondent had worked in IT and has not successfully setup a computer network.
- Group C consisting of 61 respondents have not worked in IT and have successfully setup a computer network.
- Group D consisting of 18 respondents have not worked in IT and have not successfully setup a computer network.

Figure 5 shows a breakdown of respondents working in IT and having configured a network successfully. As Figure 5 presents there is an almost equal dispersion of respondents who have and have not worked in the IT industry.

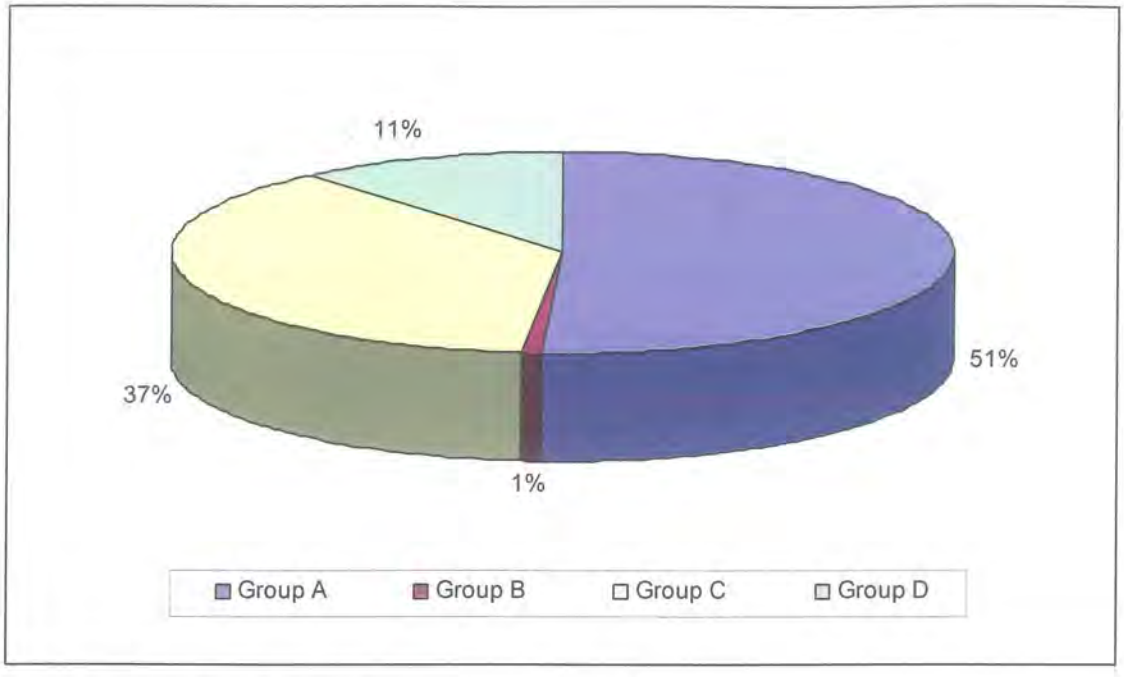


Figure 6 Pie chart of IT industry and computer network experience

4.2.2. Reasons for Choosing a Wireless Connection

This section will present the reasons respondents chose a wireless connection, according to the four groups outlined in section 4.2.1. To determine the reasons why respondents chose a wireless connection, the questionnaire provided five options where the respondent could choose as many options that applied. Two of the responses, namely 'speed' and an 'easy setup process' were deliberately implemented into the survey as they are not characteristic of wireless networks. These provided a validation to determine if respondents knew, or were aware of the basic characteristics of wireless networking.

Figures 7 to 9 illustrate the reasons respondents chose wireless. Group A shown in Figure 7 (83 respondents) identified the reasons for choosing a wireless connection which included convenience (56/83), mobility (68/83) and the lack of messy Ethernet cables (52/83). As expected within a group of experienced IT individuals few chose speed (1/83) and an easy setup process (8/83) as determinants for choosing a wireless connection. Group B (1 respondent) who had not worked in IT although had configured a computer network successfully chose convenience, no messy cables, mobility and an easy setup process as reasons.

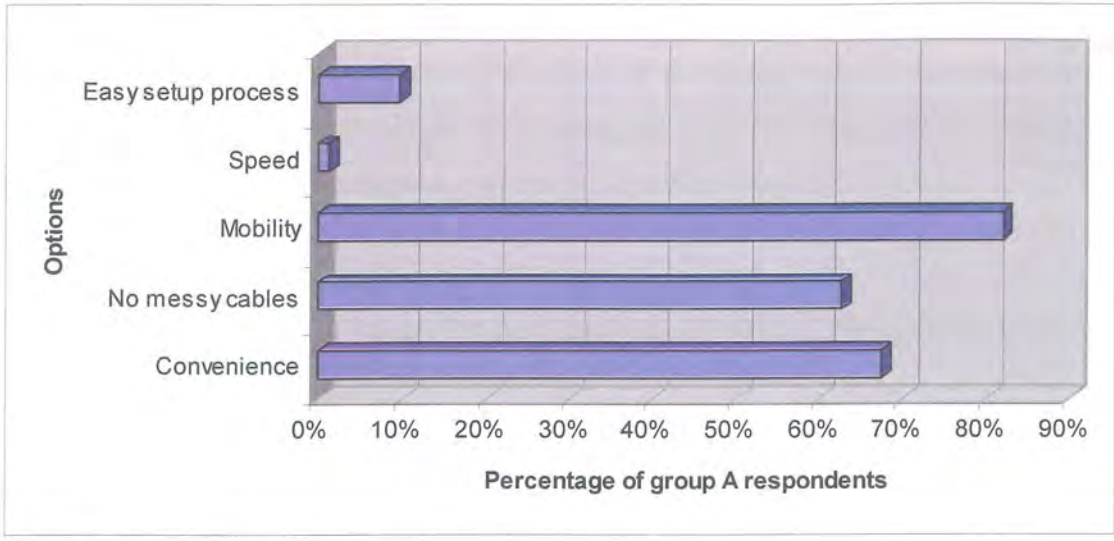


Figure 7 Reasons for choosing wireless amongst group A

Figure 8 shows group C (61 respondents) consisting of those not working in the IT industry although have successfully configured a computer network. Convenience (43/61), no messy cables (34/61) and mobility (50/61) were the dominant factors influencing individuals to choose wireless. Once again speed (2/61) and an easy setup process (7/61) were not widely chosen. The statistics show that a large percentage of respondents have valid reasons for choosing wireless with only a small number choosing non-beneficial reasons.

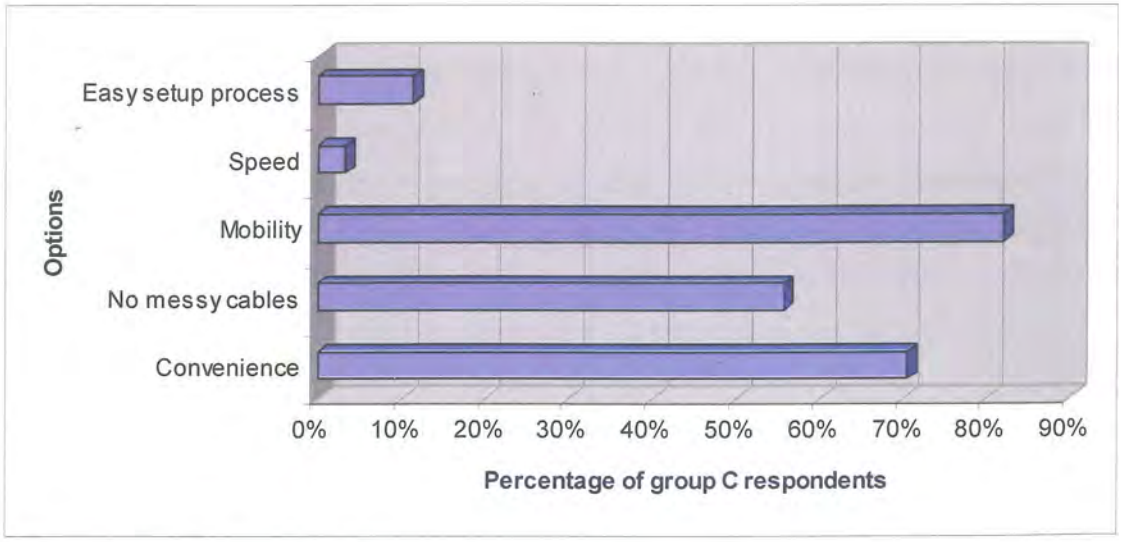


Figure 8 Reasons for choosing wireless amongst group C

Figure 9 shows group D (18 respondents) who have not worked in the IT industry nor have successfully configured a computer network. Convenience (14/18), the lack of messy cables (11/18) and mobility (12/18) were the main reasons individuals chose wireless against the traditional wired counterpart. Speed (3/18) and an easy setup process (3/18) were again marginal reasons for choosing wireless.

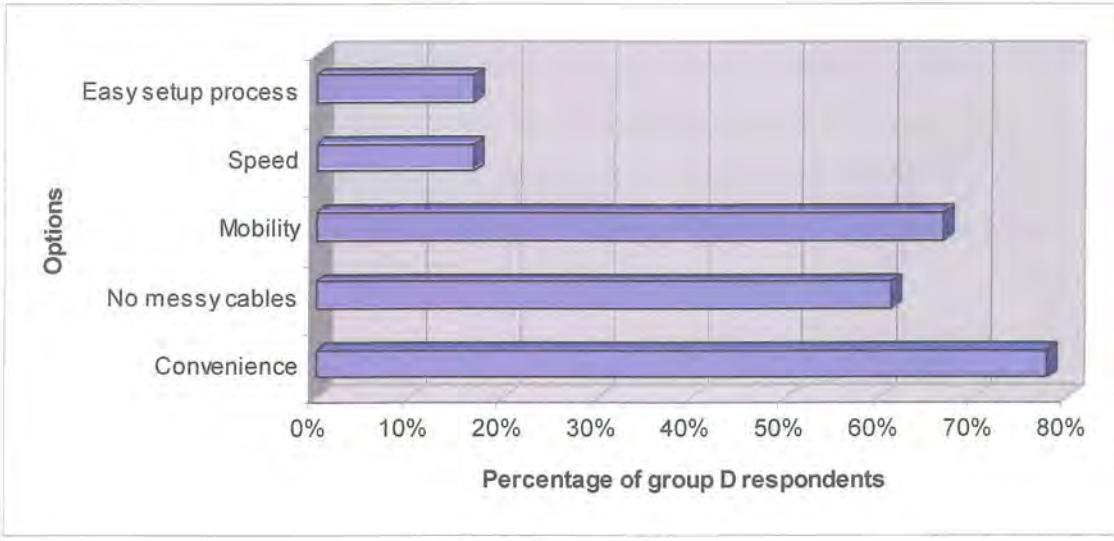


Figure 9 Reasons for choosing wireless amongst group D

Overall the respondents' reasons for choosing a wireless connection demonstrated that the majority of individuals were aware and had valid perceptions of their reasons for choosing wireless. Hence, the majority of respondents from each group (A, B, C and D) did not perceive an easy setup process and speed as beneficial characteristics of wireless, and therefore were not reasons for choosing a wireless network. When comparing each of the four groups the reasons for choosing wireless were not distinguishable. Therefore the respondents experience with wireless networking and the IT industry indicate they are not significant determinants for their reasons for choosing a wireless network.

4.2.3. Perceived 802.11 Security Methods in Place

This section will present the perceived authentication and encryption security methods that respondents believe they are using on their wireless routers. The purpose of the research was not to identify the actual authentication and encryption security methods used by respondents, and instead identifying only their perceptions. The online survey

instrument provided the opportunity for respondents to select from a list of security features they believed they have on their wireless router. Two of these features related to authentication methods (namely, Shared Key and Open System) and two related to encryption methods (namely WEP, WPA/WPA-PSK). Respondents were able to select all security methods that applied, or to not specify their security features or select that they do not know. Certain combinations of security features are not permissible (i.e. simultaneous WEP and WPA encryption), this provides a validation to see if respondents 'accurately' described and perceived their routers security. With the authentication security methods respondents choosing Shared Key and Open System features is not permissible and is noted as a false response. Similarly for encryption security methods a respondent choosing WEP and WPA/WPA-PSK is not permissible and hence noted as a false response. The four groups as outlined in section 4.2.1 will be utilised to compare each group's perceived authentication security method, and then their perceived encryption security method.

Figure 10 shows the perceived authentication methods used by group A, consisting of individuals who have worked in the IT industry and claim to have configured a computer network successfully. Few respondents believed they were using Open System (4/83), or Shared Key authentication (8/83). The majority (49/83) left the question blank or stated that they did not know, the remainder (22/83) stated they were using both Open System and Shared Key authentication and hence are false responses.

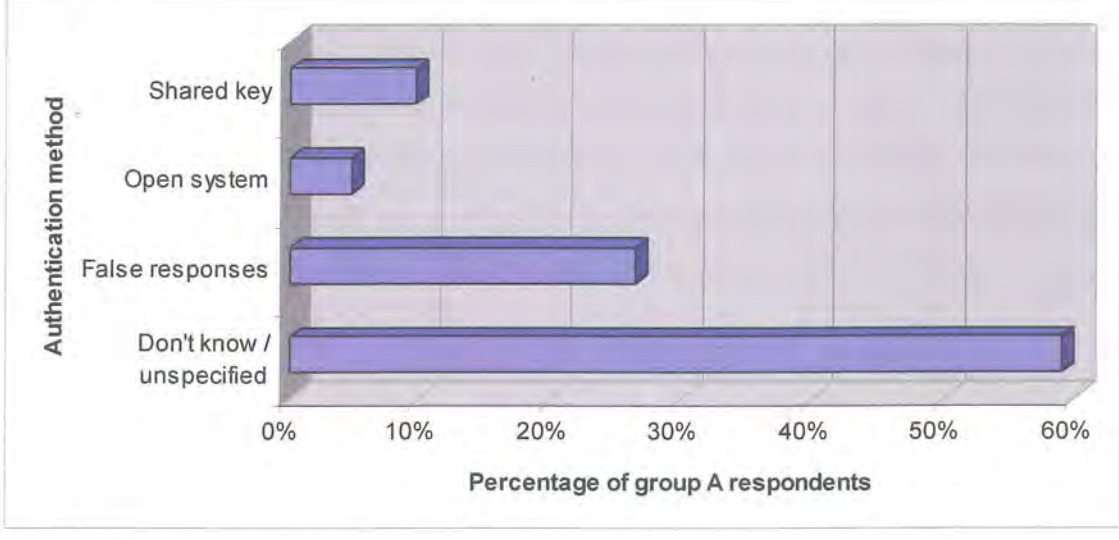


Figure 10 Authentication methods used amongst group A

Figure 11 shows the perceived encryption methods used by group A. Few individuals believed they were using WEP (20/83) and WPA/WPA-PSK (21/83). The majority of individuals believed they were using WEP and WPA/WPA-PSK (36/83) considered a false response. A minority (6/83) did not know or did not specify their encryption method.

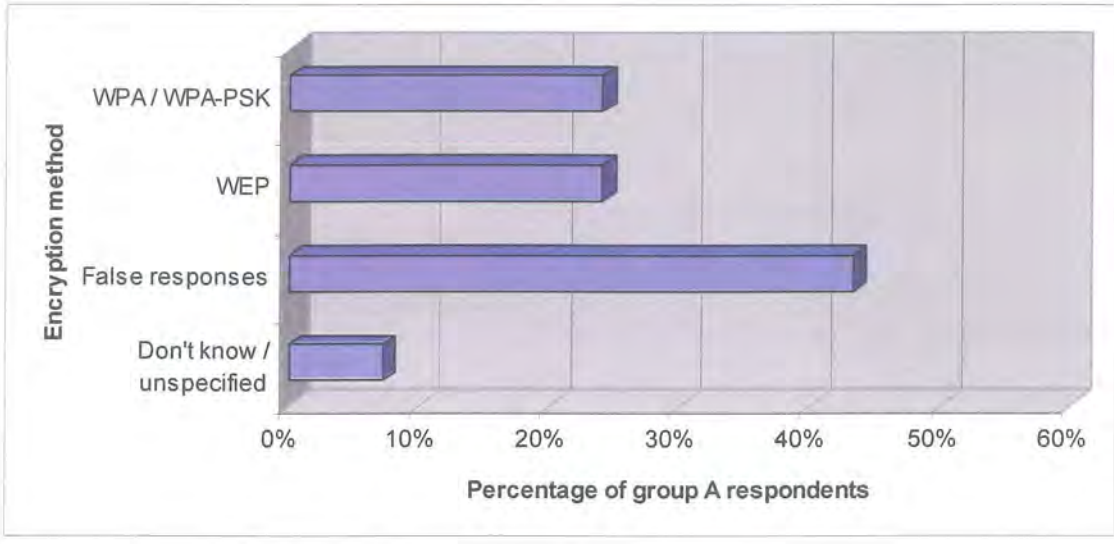


Figure 11 Encryption method used amongst group A

Group B (1 respondent) who had not worked in the IT Industry, although had configured a computer network successfully, did not know their authentication method and provided a false response for their encryption method.

Figure 12 shows the perceived authentication methods used by group C, consisting of respondents who have not worked in IT and have configured a computer network successfully. Few individuals believed they used Open System (8/61) or Shared Key authentication (10/61). The majority (36/61) did not know or did not specify their authentication method, and a minority (7/61) indicated they were using both Open System and Shared Key authentication considered a false response.

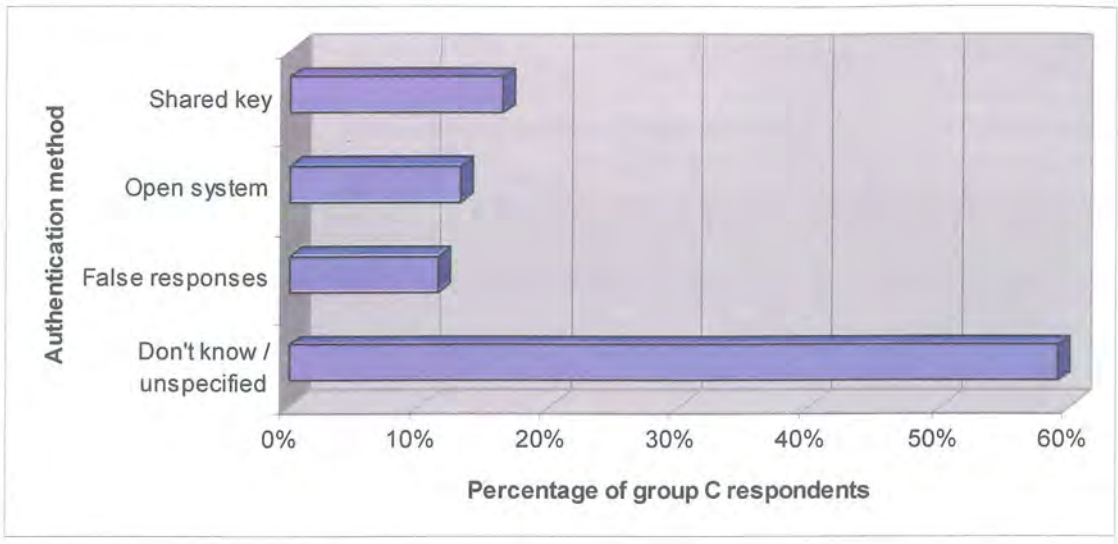


Figure 12 Authentication method used amongst group C

Figure 13 shows the perceived encryption methods used by group C. A minority believed they used WEP (13/61) encryption and less used WPA/WPA-PSK (9/61) encryption. A majority provided a false response claiming to use both WEP and WPA/WPA-PSK (24/61), whilst the remainder did not know or did not specify (15/61) their method of encryption.

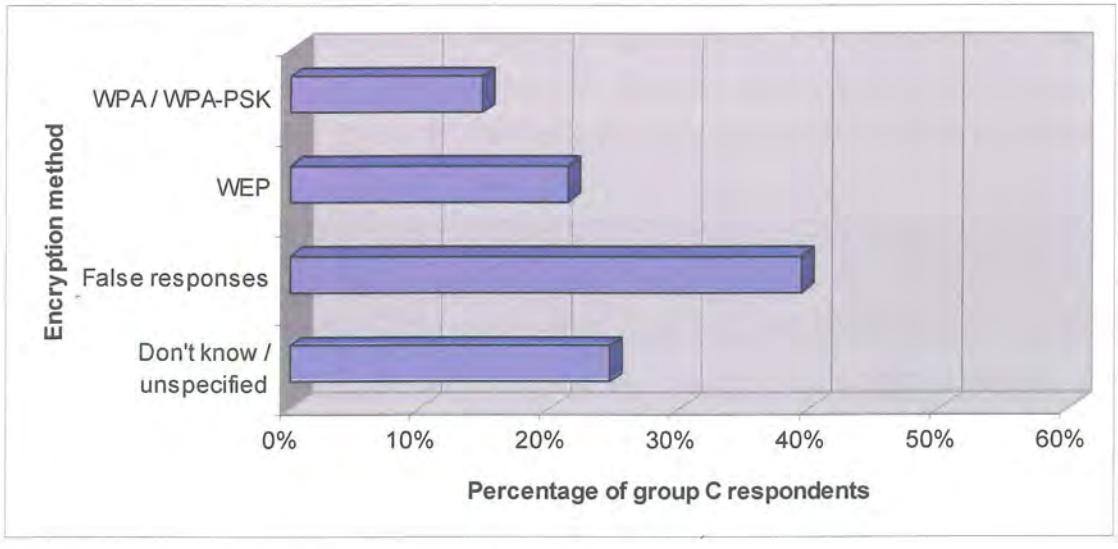


Figure 13 Encryption method used amongst group C

Figure 14 shows the perceived authentication methods used by group D, consisting of those not working in the IT industry and who have not configured a computer network successfully. Almost no respondents indicated they were using Shared Key (2/18) and no one believed they were using Open System authentication (0/18). No false responses

were noted amongst the group (0/18), however the remaining majority did not know or did not specify a selection (16/18).

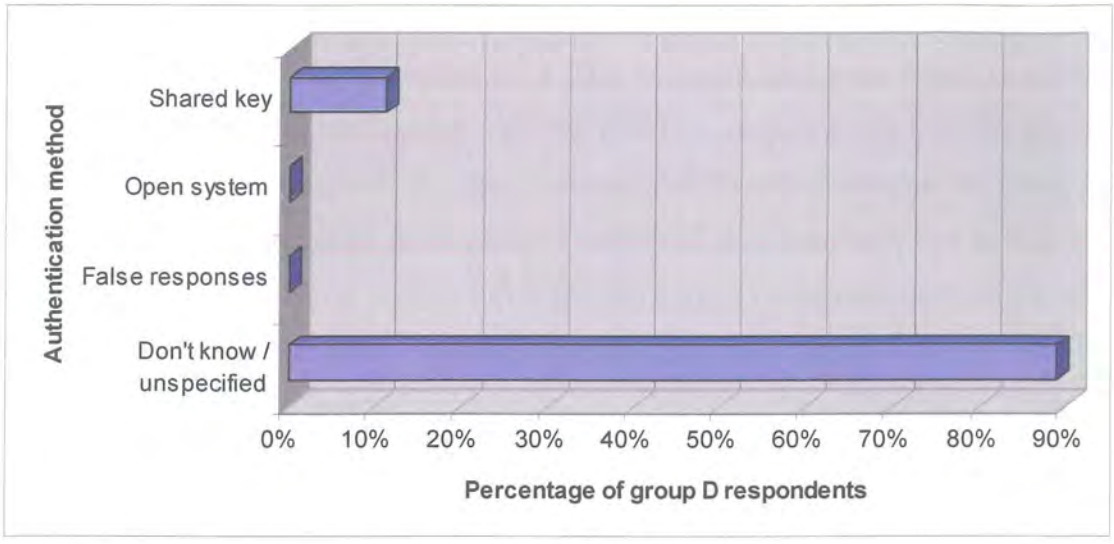


Figure 14 Authentication method used amongst group D

Figure 15 shows the encryption methods used by group D. Few respondents believed they were using WEP encryption (3/18) and no one believed to use WPA/WPA-PSK (0/18). A small portion believed they were using WEP and WPA/WPA-PSK (2/18) considered a false response. Again the majority of group D did not know or did not specify an encryption method (13/18).

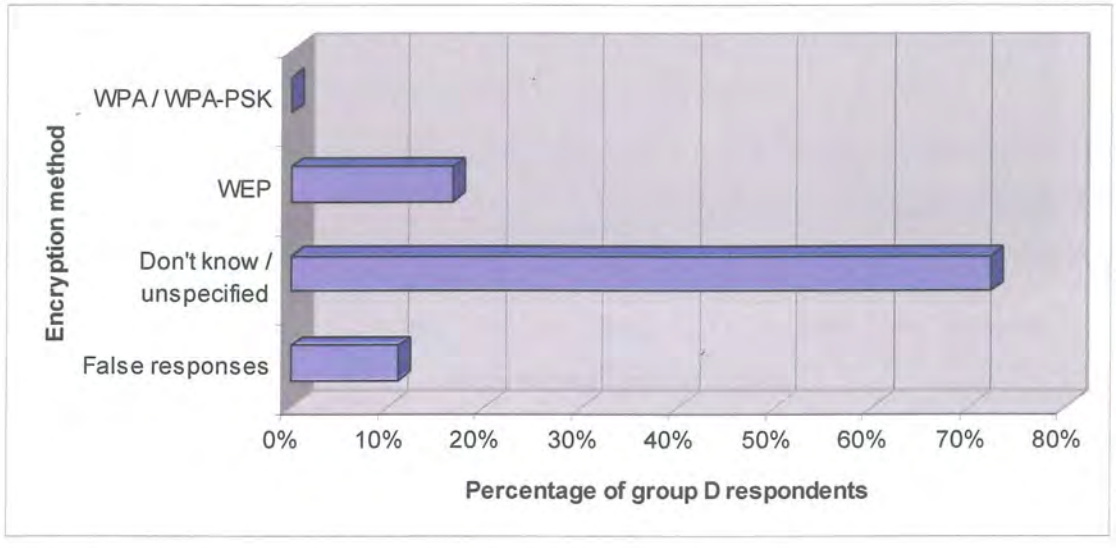


Figure 15 Encryption method used amongst group D

4.2.4. *Perception of Wireless Security Risk*

Figure 16 shows the percentage of respondents from each group who believed they were at risk when utilising a wireless connection to access the Internet. The four groups (A, B, C, and D) are outlined in section 4.1.1. One person from group A and one person from group C were omitted as they did not specify a response. Half of the group A respondents (41/82) perceived that they were at risk by using wireless to access the Internet. The one respondent from group B perceived that they were not at risk. Less than half of the respondents from group C (25/60) perceived they were at risk for using wireless to access the Internet, half of the respondents from group D (9/18) perceived they were at risk.

Behaviour in implementing sufficient security is firstly dependant upon a perception that there is a need for wireless security, and hence a wireless security risk exists. The level of awareness in wireless security assumingly increases among respondents who have worked within the IT industry. However, the perception of wireless security risks in group A are similar to that of group C and D, group B is an exception as there was only one respondent as presented in Figure 15.

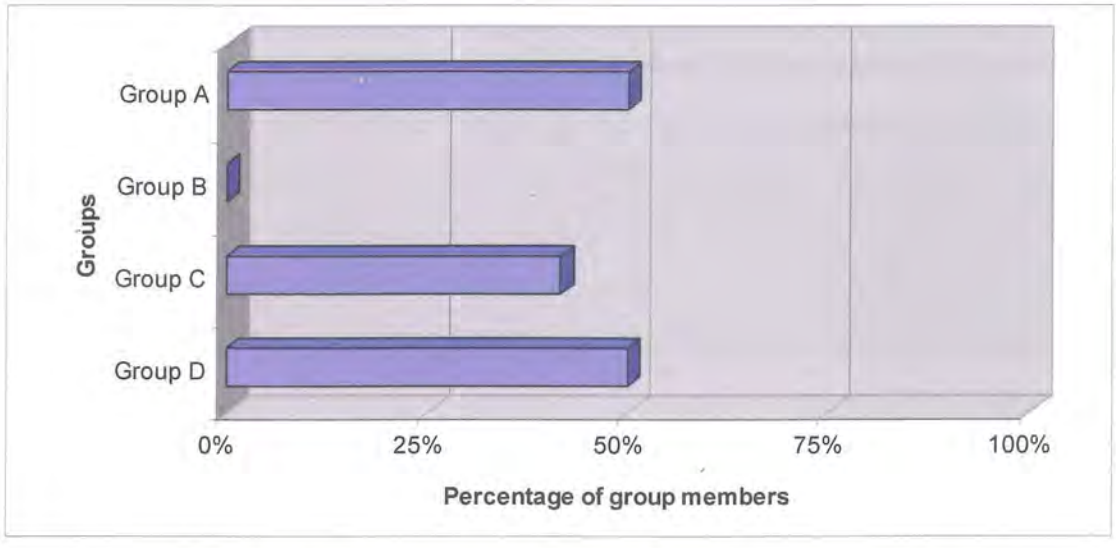


Figure 16 Respondents believing they are at risk for using wireless to access the Internet

4.2.5. Awareness of Risks and Associated Behaviour

A series of five 4-point Likert Scale statements were used in the survey instrument and questioned participants' attitude, specifically their concerns with issues surrounding wireless security. The questions related to the concern of money loss due to fraud, bandwidth theft, exposure of personal information, availability of wireless, and ensuring integrity of stored personal data. Respondents were asked to select their level of concern with each statement from four choices; "Extremely Concerned", "Moderately Concerned", "Slightly Concerned", and "Not Concerned". Using the Likert Scale analysis approach outlined by Ary, Jacobs and Razavieh (2002, p.225), each response to the five statements was assigned a numerical value ranging from 1 for "Not Concerned" to 4 for "Extremely Concerned". The total scale score is found by summing the responses given to each statement. A total score of '5' would be the lowest possible score where a respondent consistently chose "Not Concerned", alternatively a total score of '20' would be the highest possible score where a respondent consistently chose "Extremely Concerned".

Of the 163 respondents, five did not complete the Likert Scale statements, and hence were omitted as this may negatively skew the results by lowering the average scores. Thus 158 respondents were used to present the following results. Two new groups were formed to compare the level of concern between those who have currently or previously worked in the IT industry (83 respondents), and those who have not worked in the IT industry (75 respondents). Figure 17 shows the distribution for attitude scores for wireless concern of people who have worked in the IT industry. Figure 17 shows the distribution for attitude scores for wireless concern of people who have not worked in the IT industry. At first glance Figure 17 shows that respondents who have worked in IT have a slightly higher clustering of distributions in the upper region of the histogram.

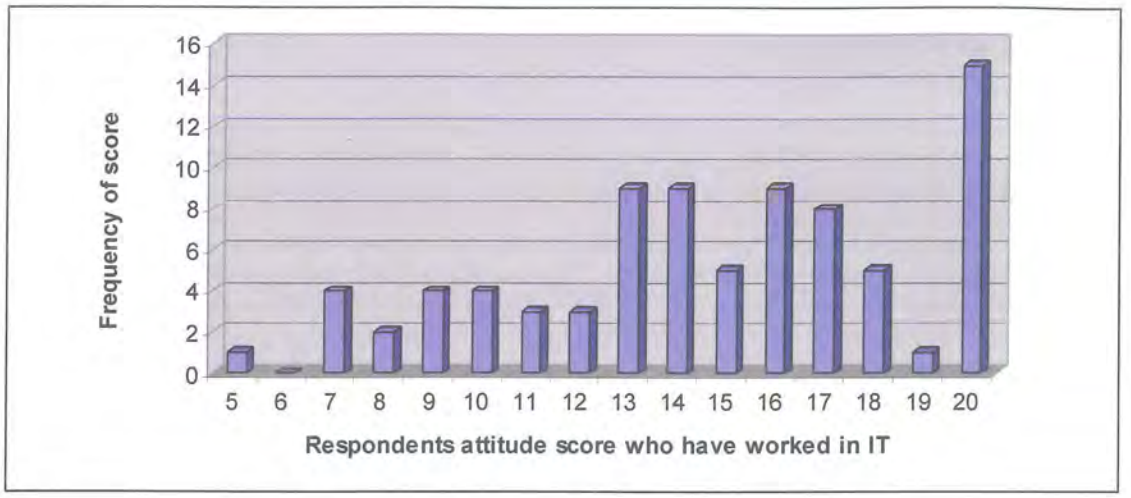


Figure 17 Frequency histogram of concern amongst respondents towards wireless security

In contrast Figure 18 shows that respondents who have not worked in the IT industry have a clustering towards the centre region.

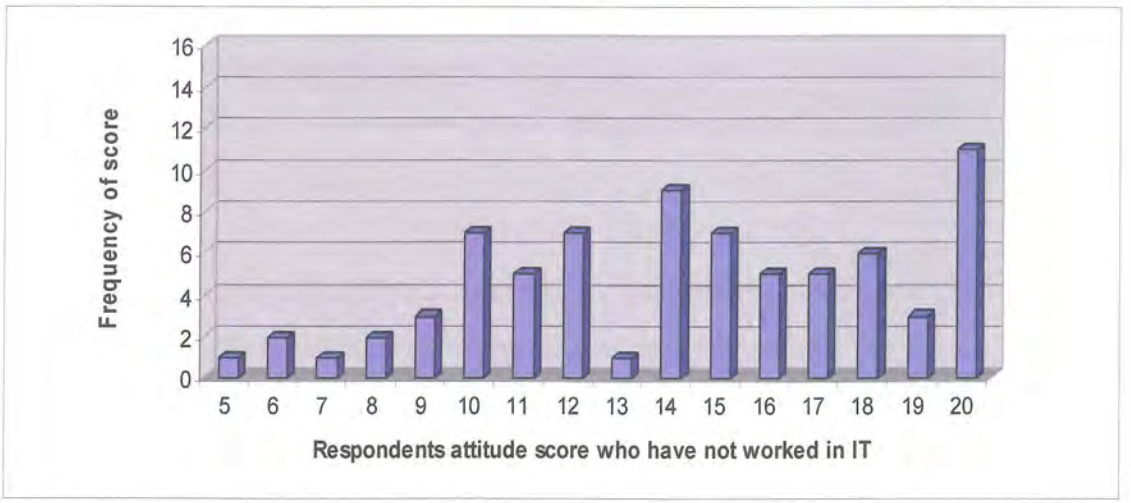


Figure 18 Frequency histogram of concern amongst respondents towards wireless security

To further analyse the two groups attitudes towards wireless security Microsoft Excel descriptive statistics where calculated, as shown in Table 16. This showed more clearly the difference between the mean attitude scores of those who worked in IT (14.67), and those who have not worked in IT (14.26). The standard deviations of those who have and have not worked in IT were 3.97 and 4.07 respectively. This shows that in most cases respondents (having or have not worked in IT) are somewhat concerned and hence aware of wireless security risks.

Table 16 Descriptive statistics of concern towards wireless security

Descriptive Statistics	Worked in IT results	Not worked in IT results
Mean	14.67	14.26
Standard Deviation	3.97	4.07
Variance	15.73	16.55
Standard Error	0.43	0.47

4.2.6. Purchasing Behaviour of Wireless Products

The results from section 4.1 indicate that almost 50 percent of respondents believe they are at risk when using a wireless network to access the Internet. These results are further evident in that the concern amongst individuals regarding the security issues at place is high (section 4.2.5). In order to examine wireless purchasing behaviour three new groups were formed depending on their Likert Scale attitude scores, which highlighted respondents attitude towards concern for wireless security (outlined in section 4.2.5). The characteristics of the three new groups are outlined below;

- Group A, respondents with an attitude score between 16-20.
- Group B, respondents with an attitude score between 11-15.
- Group C, respondents with an attitude score between 5-10.

Once again the five respondents who did not complete the Likert Scale statements have been omitted for this component of the results as the low scores may skew the results negatively.

Figure 19 shows the percentage of respondents from each group who experienced a salesperson discussing wireless security at the time of purchase. From group A (69 respondents) only 19 individuals had experienced the salesperson discussing wireless security upon purchasing their wireless equipment. Group B consisting of 58 respondents had only 12 individuals which had experienced the salesperson discussing wireless security. Group C (31 respondents), only had 5 individuals where a salesperson discussed security matters. The results indicate that those groups which have a higher attitude concern score also experienced a higher percentage of salespersons discussing

security at the time of purchase. However, the overall percentages were low among the three groups.

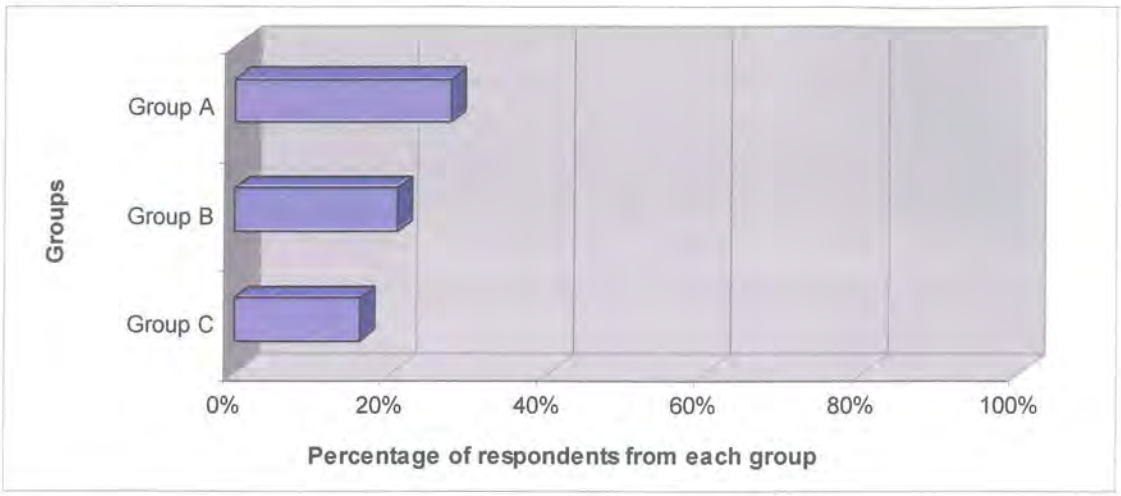


Figure 19 Percentage of each group experiencing a salesperson discuss wireless security

Seemingly few sales persons are discussing security issues with wireless products at the time of purchase, even though the majority of respondents expressed concerns with wireless security (section 4.2.5). This is combined with results thus far that show few people are aware of their security methods in place (that is. authentication and encryption methods). These combined factors could assumingly result in a poor standard of wireless security.

Figure 20 shows the percentage of respondents from each group who specifically enquired about wireless security methods. From group A 36 of 69 respondents stated that they specifically enquired about certain security features. Of group B 21 of the 58 respondents enquired about security. Finally in group C which had the lowest attitude concern score only 9 of the 31 respondents made a specific wireless security enquiry. Therefore the group who had a higher attitude concern score also enquired about specific security features most.

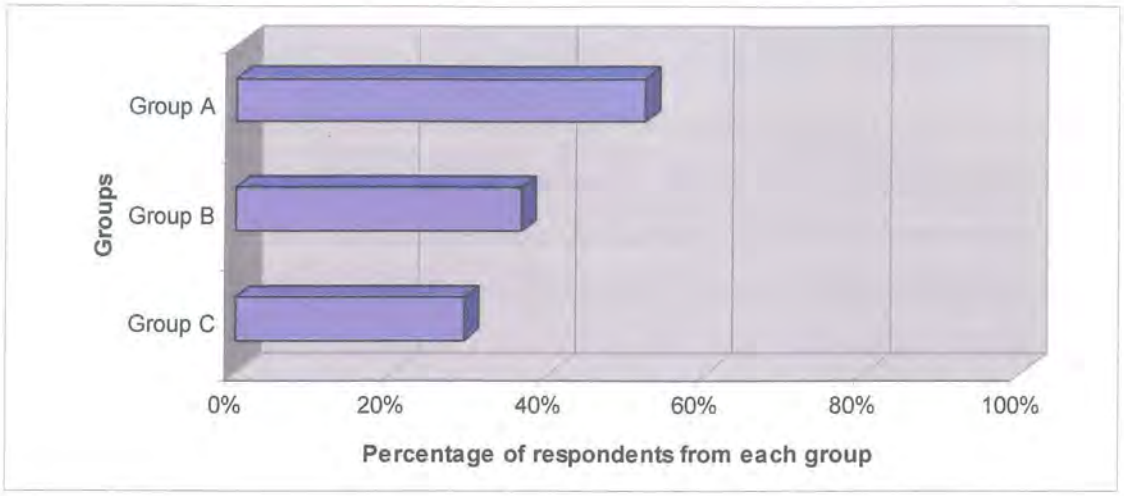


Figure 20 Percentage of each group enquiring about wireless security

As well as respondents being given the opportunity to state if they had enquired about security features during the time of purchase, they were also given the opportunity to select and state the security features that applied. The security features that were queried by all respondents (group A, B and C collectively) are presented in Table 17. Percentages and frequency do not add to 163 respondents or 100 percent as respondents may have chosen more than 1 response. WEP and WPA encryption are the prevalent queried features with MAC address filtering and encryption key length also being prevalent.

Table 17 Security features and frequency enquired about during time of purchase

Security requirement	Frequency (from 163)	Percentage
WPA encryption	51	31.2%
WEP encryption	41	25.1%
MAC address filtering	39	23.9%
Key length	27	16.6%
WPA2 capability	3	1.8%
Disabling SSID broadcast	2	1.2%
SPI Firewall capability	2	1.2%
Remote access management	1	0.6%
802.1x authentication	1	0.6%

4.2.7. *Proactive Behaviour of AP Positioning*

The security features on wireless products provide access control (authentication) and data encryption. However, simple proactive actions such as AP positioning and checking wireless coverage can determine the extent to which the wireless signal may be detected, and hence potentially stolen and leading to false fraud. Respondents were asked where the physical placement of their "wireless box" was within their home and, if they have checked if wireless coverage is available beyond their property.

Figure 21 presents the most common places the AP is positioned within the home by those respondents who have worked in the IT industry. Of these 84 respondents, 24 stated that their wireless product was located on the side or the rear of their home. The largest group of 48 respondents stated that their wireless product was located in the centre of their home and 12 individual's stated that the product was located at the street frontage.

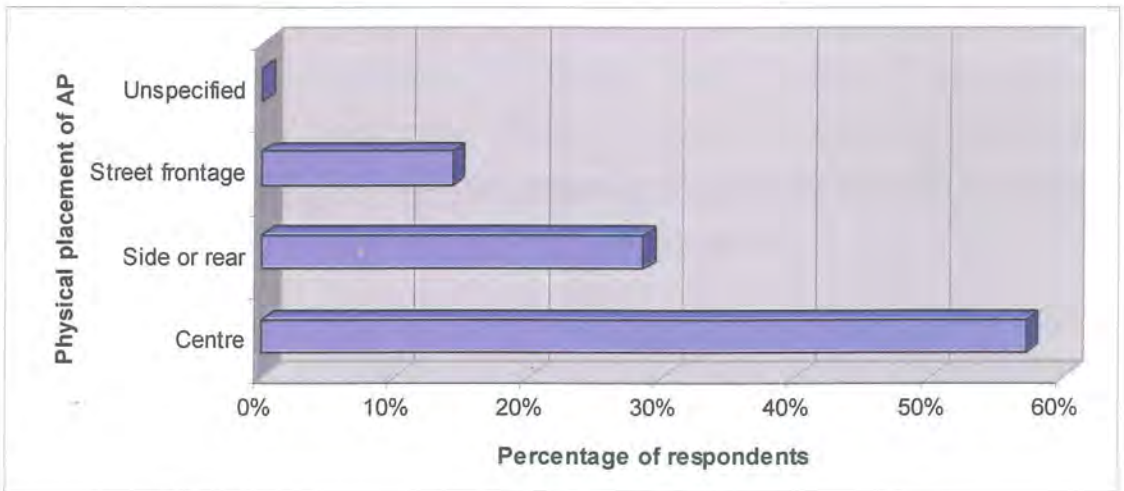


Figure 21 Wireless AP location amongst respondents working in IT

Figure 22 presents the places the AP is positioned within the home by those respondents who have not worked in the IT industry. Of the 79 respondents, 33 stated that their wireless product was located on the side or the rear of their home. 35 respondents stated that their wireless product was located in the centre of their home, 10 individual's stated that the product was located at the street front, and 1 respondent did not specify.

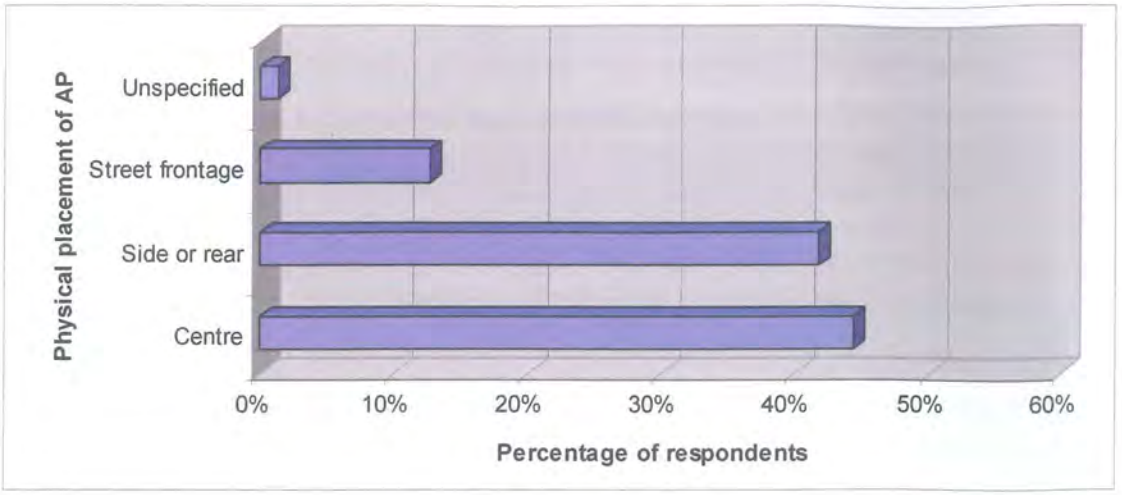


Figure 22 Wireless AP location amongst respondents not working in IT

The ideal location for an AP is at the centre of a home, this was clearly the dominant position (57 percent) for those who have currently or previously worked in IT. In contrast those who had not worked in IT had positioned their AP at the side or rear (42 percent), and centre (44 percent) of their home.

Figure 23 illustrates the percentage of respondents who have proactively checked if wireless coverage is present beyond their property. The proportion of respondents who have worked in the IT industry that checked if wireless coverage is available beyond their house is 50 of 83. In contrast the proportion of those who have not worked in IT and have checked wireless coverage is 33 of 77 respondents.

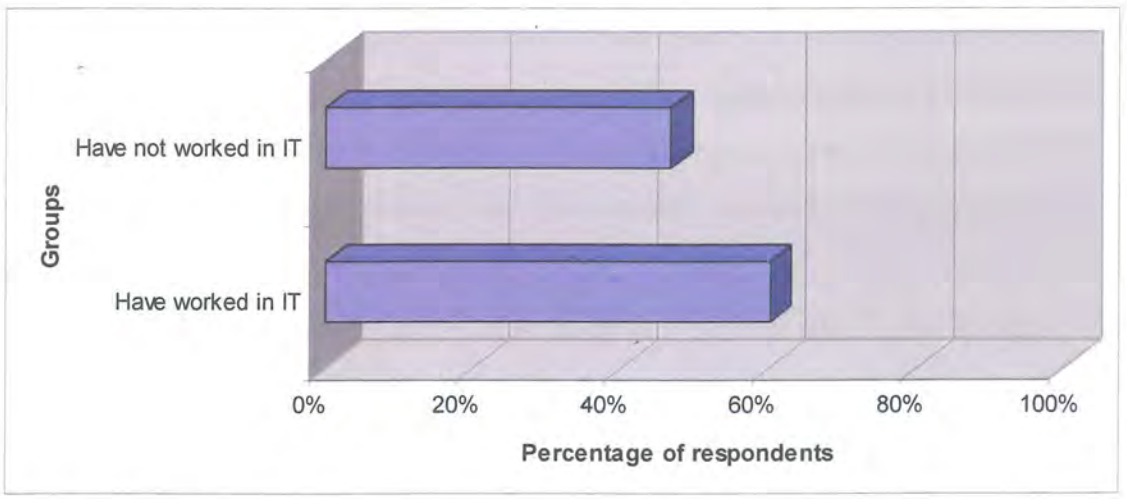


Figure 23 Respondents who checked if wireless coverage is propagating beyond their property

Overall those who have currently or previously worked in IT had positioned the AP in an ideal location. The majority (60 percent) who worked in IT were also proactive in checking if wireless coverage is available beyond their property. This is compared to 47 percent of those who do not work in IT.

4.2.8. Attitude of Wireless Usage and Configuration

As was presented in the Chapter 2 correlations have been identified between a positive attitude and an associated positive behaviour towards a specific subject or area. A positive experience towards wireless networking should result in individuals reacting in a positive proactive manner. As the concern amongst respondents is high, individuals should be implementing appropriate security methods to lower their concern. However, most individuals do not know, and few have specified valid security features, which may be the cause of poorly configured wireless devices. Hence, the following attitude scores amongst respondents should result in negative or unfavourable experiences towards using and configuring the wireless device.

Respondents were asked what their experience had been of utilising and configuring their wireless network using a Likert Scale analysis approach (Ary, Jacobs & Razavieh, 2002, p.225). Each item on the scale has been given a value ranging from 1 to 4 inclusive. Thus 'positive' has been given a value of 4, "slightly positive" a value of 3, "slightly negative" a value of 2 and 'negative' a value of 1. The two groups that have been formed are those who have worked in IT and those who have not worked in the IT industry. Each individual has been given a total score based on the two 4-point Likert Scale questions, thus a maximum score of 8 and a minimum score of 2 is possible. Two respondents had not answered both Likert Scale questions and have been omitted.

Figure 24 shows those who have worked in the IT industry and Figure 25 those who have not worked in the IT industry and the frequency of their attitude scores towards wireless usage and the configuration process. Both frequency histograms show that the majority of respondents' attitudes have a score of six or higher presenting a positive attitude towards their experience of using and configuring their 802.11 wireless products.

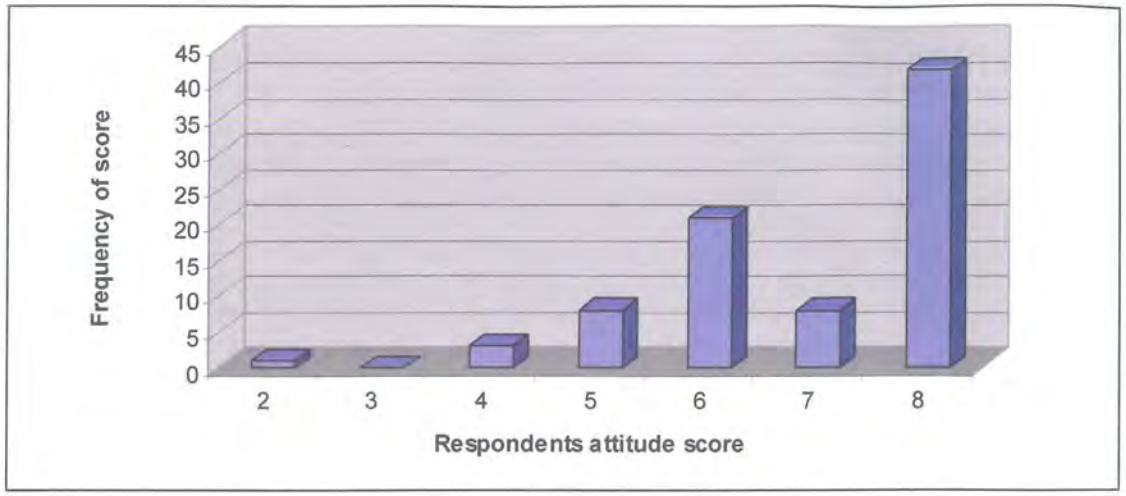


Figure 24 Frequency histogram attitude score distribution of those who worked in IT

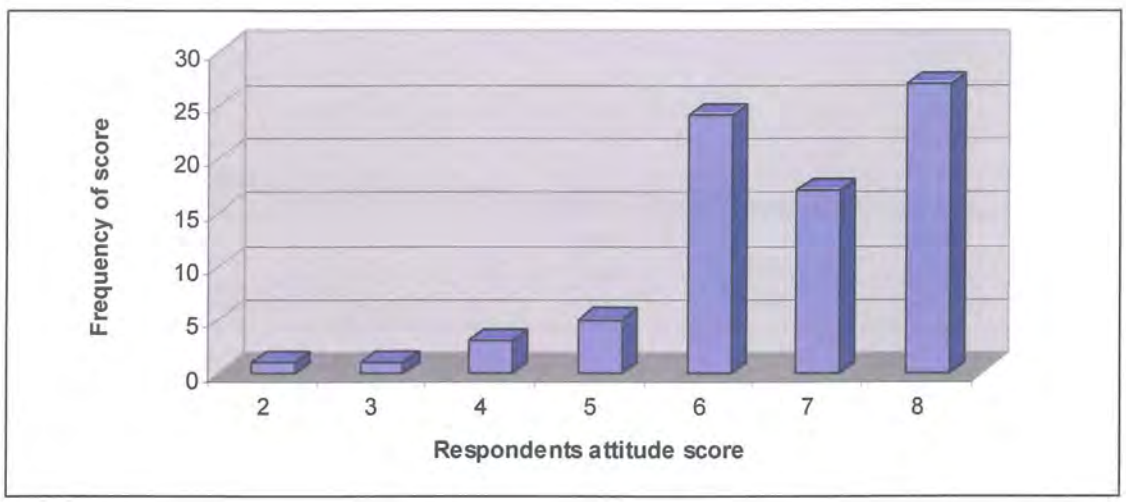


Figure 25 Frequency histogram attitude score distribution of those work have not worked in IT

As the frequency histograms (Figures 24 and 25) attitude scores towards wireless usage and the configuration process closely resemble one another descriptive statistics were calculated (Table 18). Both those who have worked in IT, and those who have not worked in IT have high mean scores, 6.89 and 6.68 respectively (out of a possible score of 8). The mean scores represent a highly positive attitude score even though manuals and hardware lack standardisation for the consumer. The scores also identify insignificant discrepancy between those who have worked in the IT industry and hence may have more experience configuring hardware and those with little or no knowledge of IT.

Table 18 Descriptive statistics of attitude towards usage and configuration experience

Descriptive Statistics	Worked in IT results	Not worked in IT results
Mean	6.89	6.68
Standard Deviation	1.33	1.30
Variance	1.78	1.70
Standard Error	0.15	0.15

4.2.9. *Information Sources for Wireless Network Configuration*

The results indicate that those who sought out specific security features on their wireless product are also predominantly concerned with the risks involved in utilising an 802.11 wireless network. The dominant features requested from respondents upon time of purchase were WPA and WEP encryption. This section - the sources of information used for wireless network users, is intended to determine what respondents are relying upon in order to configure and secure their wireless network. Although the identified flaws in the design of manuals, the information required for wireless security is present in the manual in terms of security features.

The 163 respondents, 140 individuals (including those who have and have not worked in IT) claimed to have configured the wireless network themselves (see Figure 26). Two respondents did not specify the person who configured the device, 12 individuals who had not worked in IT used a household friend, and 5 individuals who had not worked in IT used a friend not living with them. The remainder 4 individuals who had not worked in IT used a technician to setup and configure the wireless devices. Only one respondent who had worked in IT did not configure the wireless device themselves and hence relied on a technician.

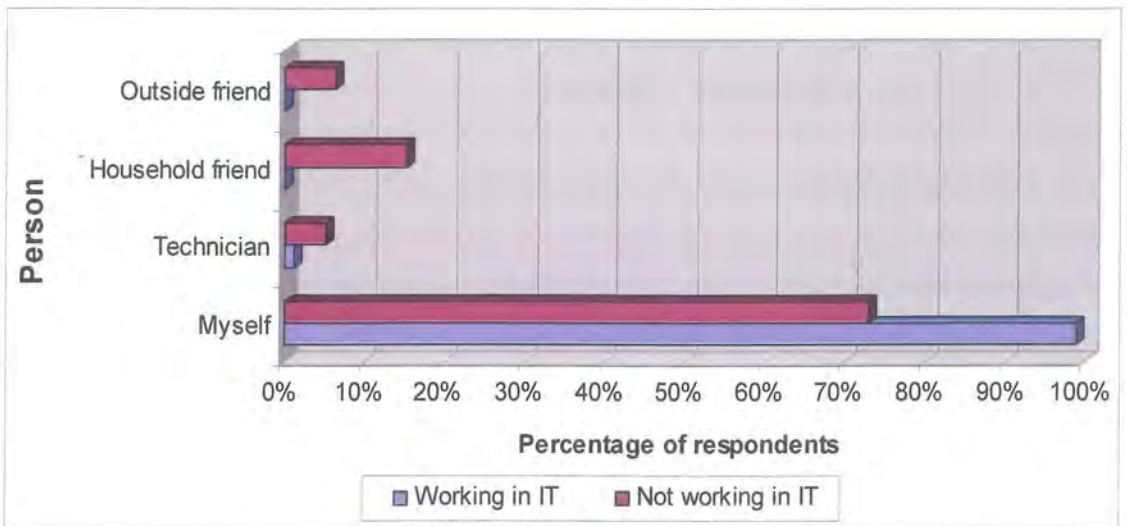


Figure 26 Percentage of respondents using other person to configure wireless network

The Respondents were given the opportunity to choose the sources of information they used when configuring their wireless network. Respondents had the option of choosing any applicable sources and where able to provide their own response.

Figure 27 shows the percentage of each information source that was used among those working in the IT industry. Respondents may have used one or more of the started sources. From the 84 respondents who had worked in IT two respondents had not specified their sources of information. Prior wireless networking knowledge was used 72 times. The quick start guide had been used 30 times and the Internet 15 times. A friend for support was utilised 5 times, and ISP support was used once, and knowledge from working in the field or undertaking a computing course was used once (referred to as other).

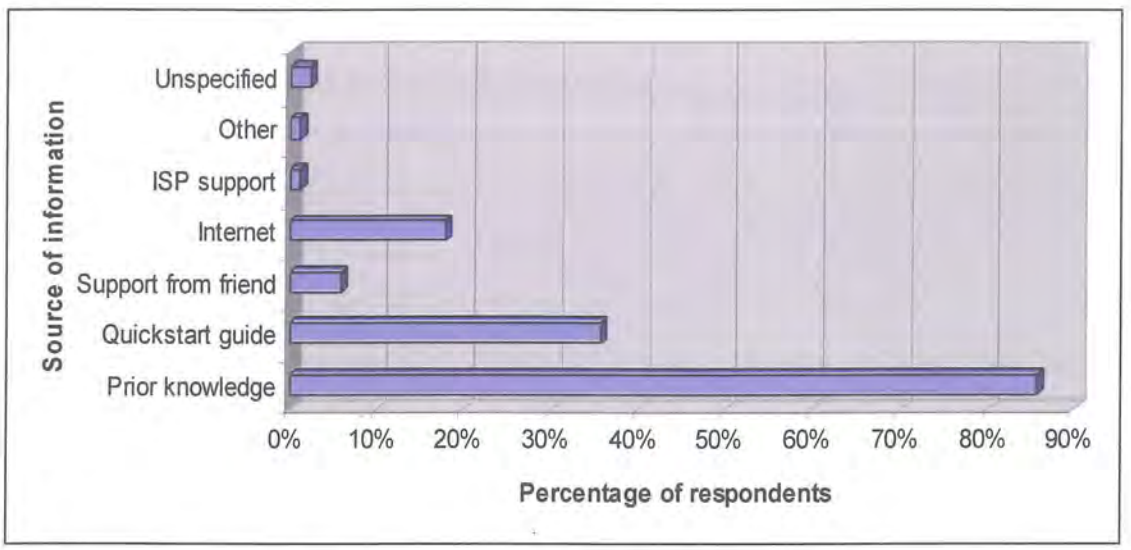


Figure 27 Information used to configure wireless network by those working in IT industry

Figure 28 shows the percentage of each information source that was used among those who have not worked in the IT industry, totalling 79 respondents, with 2 of the respondents not specifying a source of information. Prior knowledge had been used as a source of information 50 times, and the quick start guide 37 times. In contrast to those working in IT slightly more individuals referred to a friend for help which occurred 16 times, and trial and error was utilised 3 times. The Windows XP networking wizard (categorised as other) was used once, and knowledge from having undertaken a computing course was used twice (also categorised as other).

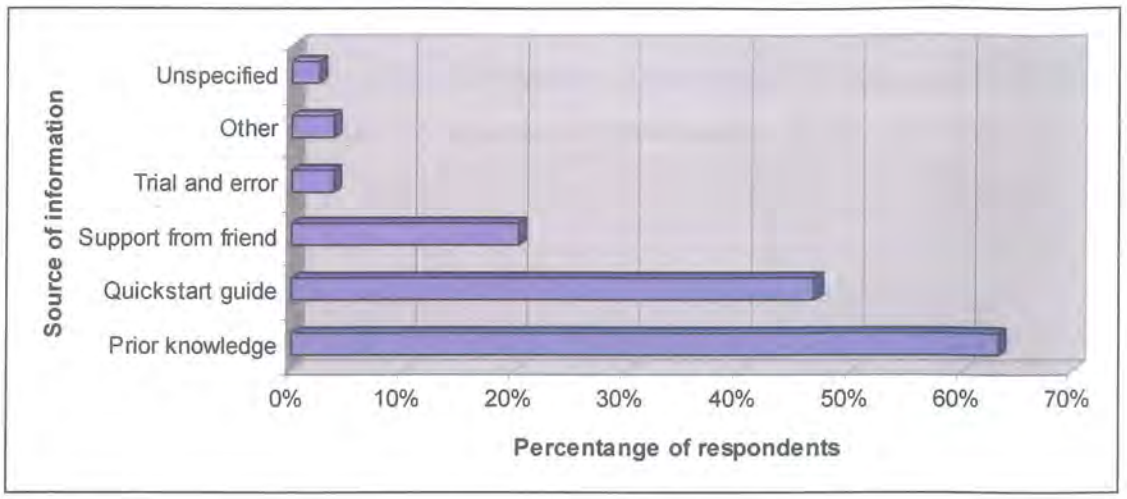


Figure 28 Information used to configure wireless network by those not working in IT industry

4.2.10. Sources of Information and Awareness of Security Methods

Of the total 163 respondents, 140 respondents stated that they configured their wireless network themselves. This section will look at the total number of information sources that were used by the 140 respondents, the number of sources used ranged from 4 to 1. The total number of sources will be compared to the perceptions the respondents have of their wireless security features (namely the authentication and encryption security features outlined in section 4.2.3). From the perceptions respondents had of their security features on their wireless products three groups have been formed, namely "some knowledge", "false response" and "don't know, unspecified".

- "Some knowledge" refers to the group of respondents who stated a valid authentication and/or encryption method.
- "False response" refers to the group of respondents who did not state a valid authentication and/or encryption method.
- "Don't know, unspecified" refers to the respondents who did not state an authentication and encryption method.

Figure 29 shows the comparison of the number of information sources used to configure the wireless network, compared to their perceptive awareness of their wireless security. As the results indicate utilising a larger number of sources to configure a wireless network is not necessarily a beneficial approach. Those who used only one source of information (75 respondents) stated either using one of the following; prior knowledge,

a vendor provided quick start guide, the Internet, or a trial and error approach. Of the 75 respondents using one source of information 41 had stated a valid perceived utilised security method, 29 respondents had made a false response and 5 did not know or did not specify a response.

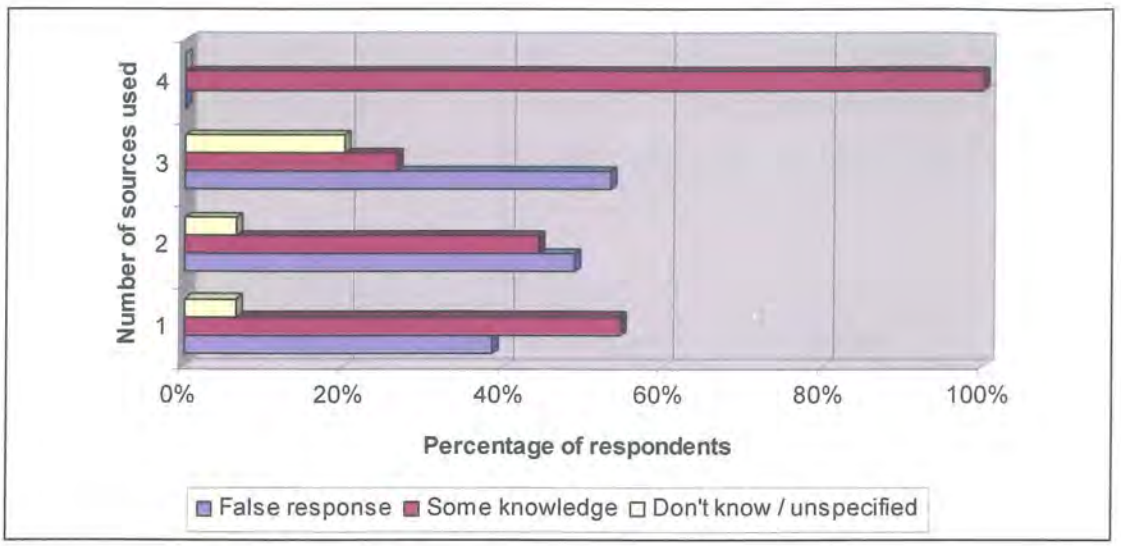


Figure 29 Number of sources used to configure wireless network and awareness of security methods

A total of 45 respondents had claimed to have used two sources of information to configure their wireless network. Of those using two sources of information 22 had stated a false response, and another 20 had some knowledge of the security methods implemented on their wireless network. A remaining 3 respondents did not specify a response or stated that they did not know what security methods were present. From the 15 respondents who used three sources of information to configure their wireless network, 8 individuals provided a false response, 4 provided a valid response and 3 did not know or specify the perceived security methods present. The one respondent who claimed to have used 4 sources of information had perceived a valid security method (some knowledge) on their wireless product.

CHAPTER 5. DISCUSSION

The study was aimed at answering one main research question and three sub questions, namely to determine if there are identifiable behaviours and perceptions of respondents utilising wireless networks in a home environment. The research results have successfully discovered some of the identified behaviours and perceptions. This section will discuss the results in conjunction with previously discussed literature, evident trends and ideas.

5.1. Wireless Background Information

The survey instrument results identified that the top two chosen ISP's were the least publicised on television and radio. Westnet and iinet formed 42 percent of the total responses in contrast to Bigpond, Optus, Iprimus and Dodo which formed just over 20 percent of the total sample. The literature review highlighted that through clever marketing individuals may have their perception of wireless products altered. This may lead consumers to believe that certain products are advantageous, and hence presented in a superior manner in contrast to competitors. The evidence in this research shows that in terms of wireless networking, respondents do attempt to investigate companies trying to sell products. Hence, the evidence suggests that respondents' perceptions may not be altered to believe an ISP is advantageous over others who do advertise on television or radio.

As previously discussed in Chapter 4 (section 4.1.1) 50 percent of the sample, had or were working within the IT industry and 90 percent of the sample had successfully configured a computer network. A study on behalf of CISCO (2003) identified that from 200 end-users, respondents rated mobility as the greatest benefit for choosing to use wireless. In contrast, the CISCO study found that ease of installation was a major concern and hence a negative aspect of implementing wireless. The results from this study identified that mobility was the greatest selected benefit among the sample, while an easy setup process was one of the least selected options. Those who had worked in the IT industry had similarly chosen mobility as the greatest benefit, and the lack of speed was a minority selection among the group. In contrast those who had not worked

in the IT industry had predominantly selected convenience and mobility as reasons. The least selected options were speed and ease of installation. These results show an almost identical response to the CISCO study and identified that respondents perceive the true benefits of utilising a wireless network incorrectly.

Evidence derived from background information suggests that the sample had a good understanding of the fundamentals of wireless networking. The results conform to similar previous studies, and indicate that respondents are willing to put in the effort to choose products. This is possibly based on knowledge and intuition rather than being persuaded by talented marketing.

5.2. Knowledge and Associated Behaviour

Consumers who purchase wireless or computing products may often rely upon the salesperson to discuss the benefits, downfalls and alternatives of products, dependant on the consumer's situation. The salesperson may determine the consumer's requirements and attempt to sell a product based on these needs. From the sample, respondents were asked if a salesperson had discussed any security issues when they had purchased the wireless product. From the sample of 163 respondents, only 36 respondents (22 percent) had security issues discussed with them. Evidence from the results indicates that those respondents who experienced a salesperson discuss security issues, were predominantly concerned with the issues surrounding the wireless technology. The evidence predicts that the less commercialised ISP's are predominantly utilised amongst the sample. Although beyond the scope of this research, there could be a link between the less commercialised ISP wanting to gain a larger market share by not deterring consumers from choosing their products. Hence, not bringing up security issues may prevent an aspect of fear and not deter customers from purchasing bandwidth.

When respondents were asked if they had purposely enquired about specific security features a large portion had questioned the salesperson (40 percent). The results indicate that those who were spoken to, or had enquired about security features were concerned. The evidence suggests that those who did enquire about security questioned both weak and strong security features. WEP encryption was questioned 41 times from the sample, even though it is the default standard encryption on most wireless products. WPA

encryption was chosen 51 times and MAC address filtering was selected 39 times. The results showed that respondents chose the less commercialised ISP's, and had to undertake a degree of research whether it be for price or quality of the service. However, in terms of specific security features, few appear to have researched what hardware or security is provided by an ISP and hence the standard features on each product.

The sample was provided with the opportunity to select their perceived security methods (authentication and encryption) in place on their wireless access point. The purpose was to discover if respondents were utilising weak security methods such as Open System or WEP, or safer methods such as Shared Key or WPA/WPA-PSK. However, a conclusion on weak or strong security methods could not be drawn from the results. This is because results showed that the majority (80 percent) did not know, or provided an incorrect response for their authentication method. For the encryption method used, almost 60 percent of the sample did not know, or provided an incorrect response. An incorrect response was indicative of respondents believing that they were using both WEP and WPA/WPA-PSK or Open System and Shared Key which is not technically possible.

The evidence shows that those who had worked in the IT industry were identified as having a slightly better perception of security compared to those not working in IT, by stating additional valid authentication and encryption methods. The analysis showed that those respondents who had not worked in the IT industry, and had not configured a network successfully, had a higher percentage that did not know or stated incorrect security methods. A similar study by Hu and Dinev (2005, p.62) identified that those who had experience in the IT industry had failed to be proactive in computer security, even after having sound knowledge of security issues. The results from the previous study complement the results of this study, and portray that working in the IT industry does not guarantee that an individual will be an expert in all areas of computing and in particular security.

Placement of the AP within a house is not always the choice of the consumer, but rather restricted to the placement of the RJ12 phone line connection in the house, as many AP's are built in to the ADSL router/modem. In spite of this limitation, the evidence

suggests that those who are in the IT industry are slightly more proactive in security than those who are not. The respondents in the IT industry showed that almost 60 percent positioned the AP in the centre of the house with few positioning it at the street frontage or, the side or rear. In contrast, an almost equal amount of respondents who had not worked in the IT industry, had positioned the AP in the centre or, the side or rear with 44 and 41 percent respectively. The results indicate that those working in the IT industry have a marginally better awareness of how a radio wave may leak and hence be stolen by a third party. Restricting the propagation of the wave by placing the AP in the centre of a house with interfering walls may prevent bandwidth theft.

From the sample, 86 percent had configured the network themselves and utilised either prior knowledge or a vendor provided quick start guide. Chapter 2 revealed the lack of standardisation among six separate vendor wireless router manuals. However, only the Netgear manual followed some of the best practise design methods. The majority of respondents had configured the wireless network themselves with only a few using a friend or a technician. The evidence suggests that those who have worked within the IT industry believe that they should have the knowledge to configure a wireless network appropriately. This is identified in the results of almost 100 percent of respondents who have worked in IT configuring the network themselves. In contrast, those who have not worked in the IT industry saw just over 70 percent of respondents configuring the network themselves, with friends and technicians being relied upon also.

Although respondents working in IT had configured the wireless network themselves, they were not significantly more aware of the security methods in place on their wireless router. The majority of respondents from both groups used some form of prior knowledge as the source of information to configure their wireless network. Among those working in the IT industry prior knowledge was relied upon predominantly and the vendor quick start guide and Internet were also used marginally. In contrast, those who had not worked in the IT industry had again used prior knowledge to a degree as well as the quick start guide, and support from a friend. The heavy reliance upon prior knowledge would suggest that respondents would be skilled and knowledgeable in the area of wireless networking. This was clearly not the case as the majority did not know (or specified invalid responses) on their security methods they had in place. Further research would need to be conducted in determining what the prior knowledge

respondents have towards wireless networking and where this information had been gathered from.

5.3. Perceptions and Attitudes

The sample as a whole are concerned with issues surrounding the wireless technology that specifically impact them in the present rather than what may impact them in the future. Ensuring integrity and confidentiality of personal data are things which impact the respondent directly, as is the availability of a stable wireless connection. In contrast, it appears that the respondents are not as concerned or aware of bandwidth theft or money loss due to fraud. This may be because these matters are not highly publicised in the media, or the effects are not immediately felt. Theft of bandwidth and money loss due to wireless fraud did not concern 22 and 30 percent of the sample respectively. This could mean as well that these respondents have superior wireless security or are not aware of the simplicity of such an attack being initiated. A study in 2001 conducted by NOP World Technology on behalf of CISCO (CISCO, 2003) found that those who had worked in the IT industry were significantly more aware and hence concerned with the issues surrounding the wireless technology. Using the five 4-point Likert Scale questions outlined in the results, each respondent's concern score had been tallied. Overall respondents from both groups are both significantly concerned with the issues surrounding the technology. Both groups had an average score of 14.67 and 14.26 respectively out of a possible 20, representing a 'moderate' (i.e. second highest) concern towards the issues.

A large case study research experiment examined the behaviour of respondents on various types of manual design methods (Schriver, 1997). The outcome of the research saw that when individuals were presented with poorly written instructions and could not complete the task they would blame themselves, and hence rate the experience as negative. The review of vendor manuals and guides (section 2.4) identified them as poorly designed and did not follow specific standards. However, respondents noted that experiences configuring and utilising their wireless product were in general positive with almost 90 percent of respondents in both cases stating to have a 'slightly positive' or 'positive' experience. As Chapter 2 showed those respondents who have a positive experience in configuring and utilising their wireless network, should, in turn, behave in

a similar positive proactive manner. However, evidence from this study identified that respondents are somewhat proactive in security matters (i.e. checking wireless coverage). The knowledge of security features is one area in which attention to detail is lacking. Numerous respondents stated invalid perceived security methods, or implemented encryption such as WEP rather than the more secure alternative WPA/WPA-PSK. Thus, it appears that a solely positive attitude towards an area will not necessarily ensure the individual will behave in a continuing positive proactive manner.

This study of wireless networking identified that respondents were aware of the basics in relation to wireless such as ISP and connection type. Frisk and Drocic (2004) saw respondents being well aware of the basics in relation to computing. They (Frisk & Drocic, 2004) uncovered that when it came to specific security matters such as questions on administrator mode or password use, respondents were not aware, or did not state valid arguments for justifying their use. The results from this study show a similar knowledge among respondents since they did not know the specifics of security in wireless networking. Hence, the results indicate that more attention should be placed on educating users on the specifics of security and explaining how certain functions operate so that users are well aware of advanced security features on products.

5.4. Discussion Summary

In summary the behaviours and perceptions identified by the study show that respondents are aware and concerned of the risks involved in utilising a wireless network. However, this was not shown through their behavioural attitudes. For example, their behaviour when purchasing wireless products saw at most only 51 percent of any discussed group enquire on security matters. When positioning or checking AP coverage, again only a handful applied security testing behavioural techniques. The experiences of respondents are shown to be positive among configuring and utilising a wireless network. The sources used included quick start guides and predominantly prior knowledge, although neither of these have proven to be ideal due to the lack of perceived implemented security.

Respondents, both those who have and have not worked in the IT industry, appear to be trying to secure themselves from becoming a victim to wireless fraud. Respondents are

aware and hence concerned, and also feel that their AP is vulnerable to an attack. Presumably, if an individual is concerned and does feel vulnerable there would be an expectation that the individual would want to stop that concern from reoccurring. However, if respondents are not informed of security matters during time of purchase, or by media publications not discussing the flawed techniques, then this concern can not be catered for. It appears that in order to ensure respondents are concerned, more proactive further education and media releases could be made available and publicised to get the message and information across.

CHAPTER 6. CONCLUSION

This thesis presented research that identified behaviours and perceptions among individuals who utilise 802.11 wireless networks at home. The research was significant as this is one of few discourses which focused specifically on the home user instead of the business counterpart. The home user was chosen because unlike a business or large corporation, an individual may find it especially difficult to recover from an attack such as an excessive use charge acquired from bandwidth theft. Accordingly the research was important in formulating a foundation for further research to stem from, to avoid the home user from becoming a victim to a crime they cannot see, touch or hear.

6.1. Summary of Chapters

Chapter 1 introduced the fundamental background of this research and identified in brief some of the problems evident in utilising an 802.11 wireless connection. The chapter then discussed the significance of the research in that it was unique and would lay down the foundation from which hopefully further research may grow. A set of research questions were developed based on the reviewed literature, to determine if there are any identifiable behaviours and perceptions apparent by the selected sample group.

Chapter 2 reviewed current literature relevant to this study discussing the 802.11 wireless standards and the key features of the transition from wired to wireless networking. The countermeasures and threats were presented, and although there were numerous threats, it was discovered that the associated countermeasures were weak or flawed. Many of the 802.11 wireless network threats may be exploited unskilled individuals utilising easily accessible freeware utilities. Current manuals provided by vendors of wireless networking products were tested against recommended manual design standards. The manuals were identified as not conforming to any standards, and appear to not have been developed to inform and advise individual of 802.11 wireless network risks and security methods. Finally, computer security literature was presented which showed that individuals were not aware and did not have adequate knowledge to implement security at home on their computer. Studies on implemented 802.11 wireless networks discovered that businesses and critical infrastructure are being left unsecured

and hence vulnerable to exploitation due to insufficient or inappropriate wireless network security.

Chapter 3 discussed the chosen research methodology and presented philosophical beliefs which were followed as part of this research. Limitations of the research were identified and addressed to ensure these would not negatively impact on the research. The online survey instrument was presented and a clear explanation of each of the 29 questions provided. Chapters 5 and 6 presented the results which were collected from the study in conjunction with a discussion component answering the research questions and presenting arguments and beliefs based on those results. The discussion chapter compared results from this study to previous studies and identified similarities and differences between results.

6.2. Summary of Research Questions

The study encompassed one main research question, and three sub questions which formulated the basis for this research. Each question in turn will briefly be summarised in terms of the results and discussion formulated.

What are the identifiable behaviours and perceptions of individuals who use wireless networks and wireless security at home?

Respondents were well aware and informed of the broad and basic issues and benefits surrounding the wireless technology. Results indicated that respondents could clearly distinguish between the benefits and disadvantages of using wireless networks, or choose an ISP with greater benefits, which is usually less commercialised. However when distinguishing amongst specific 802.11 wireless security methods, few individual's have a valid perception of their exact security methods on their AP. An identifiable behaviour is that respondents are trying to implement the security methods they believe are ideal for their situations, although it seems as though they do not have accurately detailed information available. As Chapter 2 identified if a respondent is not aware of the security methods in place, then they can not be proactive in researching safer security methods (e.g. WPA-PSK instead of WEP). Further research is needed to determine the most effective way in which to educate individuals of the specifics of

wireless networking, and hence allow them to be proactive in implementing, safer and strong security methods.

The study did not identify significant discrepancies between those respondents who have worked in the IT industry and those who have not. Both groups appear to be equally concerned and aware of the issues surrounding the wireless technology. Although those who have worked in the IT industry should be well aware of the risks and hence have implemented strong security methods, this was not the case. In terms of implemented security, those who had worked in the IT industry saw only marginally more respondents stating valid security methods than would be expected. The perception that those who have worked in the IT industry are deemed experts in all fields of computing is not supported by this study.

This study did identify that those respondents who had worked within the IT industry relied predominantly on their own knowledge in contrast to the group who had not worked in the IT industry and hence used a wide variety of sources. The evidence suggested that respondents who have worked in the IT industry believed that the knowledge they have would be adequate to configure a wireless network. Although respondents may successfully configure a computer network, this does not necessarily mean it is operating in a secure state.

Are individuals who use wireless networks at home concerned with the risks, and is this justified by their behavioural attitudes?

The evidence from this research, as expected showed that a high portion of the sample did not feel that their wireless networking products were vulnerable. However, they were concerned with the issues surrounding the wireless technology. The study has identified that only a portion of the respondents were concerned with the risks associated with the wireless technology. Of the entire sample approximately 50 percent believe that their wireless products are vulnerable to exploitation. In contrast a significantly more respondents were concerned with the issues surrounding the wireless technology. Further research could determine why respondents believe their wireless products are vulnerable, and hence the reason for concern for the broad issues.

Both groups were equally concerned with the issues surrounding the wireless technology. However, the evidence identified that those who were slightly more concerned also worked in the IT industry and were also predominantly proactive in security. When investigating who had checked if wireless coverage was available beyond their premises only 53 percent of the sample had done this test. However, those who had worked in the IT industry had conducted this test significantly more so, in contrast to those who had not worked in the IT industry.

An analysis of the respondents purchasing behaviour identified that those respondents who were predominantly concerned with the issues surrounding the wireless technology also queried specific security features during the time of purchase. Evidence from the research suggests that in order for an individual to have a proactive behaviour in terms of wireless security they must understand the problems and be aware of the issues. As respondents were overall less concerned with the wireless issues this saw fewer individuals checking wireless coverage or enquiring about specific features when purchasing their product. Hence, it appears that additional information must be made publicly available to consumers to stimulate concern which should in turn see individuals attempt to be proactive in security to a higher degree.

Has configuring and using the wireless network been a positive or negative experience for the home user?

Even though the vendor manuals are flawed, the majority of respondents still claimed to have had a positive experience when configuring and utilising their wireless network. Even though it was assumed that the flaws would impact negatively on experience attitudes, this was clearly not the case. The majority of respondents claimed to have had a positive experience configuring and utilising their wireless network. For the most part, this positive attitude has been carried forward through respondents' proactive behaviour of basic wireless security measures such as checking wireless coverage and AP positioning.

Overall, respondents did appear to have a positive experience configuring and utilising their wireless network. However, with a majority of vendors now releasing 'out of the

box' configurations, little physical configuration is required to setup the wireless products. Hence, further research would be required to determine what exactly was done by the individual to setup their network and hence determine the attitude level from this information. The theory that a positive attitude experience will in turn produce a positive proactive experience is not support by this study as security implementations were poorly implemented.

What sources are being used by home users to setup and secure their wireless network?

It was presumed at the start of this research that the vendor literature would be utilised by a significant majority of the respondents. As the previous research question identified, the majority of respondents did had a positive experience configuring their wireless network. As the vendor literature was presented as flawed, it was assumed that respondents would encounter negative experiences configuring their wireless network. In turn respondents would therefore have a lack of sufficient implemented security. This was not the case in terms of the research as respondents did have a positive experience, the vendor literature was not predominantly utilised, and chosen security features were invalid or not known.

Evidence from this research showed that home users are relying upon prior knowledge as the main source of information when configuring their wireless network. Where this information is being obtained from was beyond the scope of this study, but should be followed up in future research. This would determine if it has credentials or if it is up to date with latest security information. Although respondents are using various means of information to configure their wireless network, utilising more than one source did not show any improvement in terms of perceived security on their wireless product.

Whilst prior knowledge and the vendor quick start were the top two sources of information used, other sources include support from a friend or the Internet. The evidence suggests that those respondents who have worked in the IT industry rely predominantly on prior knowledge there is also a reliance to use the Internet as a source. In contrast, those who had not worked in the IT industry relied on prior knowledge and the quick start guide but also support from a friend to configure their wireless network.

From those who had worked in the IT industry, no one used the Internet possibly due to not knowing areas to find relevant information or understanding the technical material.

6.3. Future Research

The time limitations of this study restricted the possible resultant sample size. Further future research could permit the online survey instrument to be accessible for a greater length of time. The current study conducted online surveys which were only accessible to an academic population. More detailed analysis could include a more representative population using a random selection process also including non academics.

The research was limited to a quantitative analysis identifying attitudes and perceptions of wireless network usage in home environments. Further research could address this limitation and undertake a qualitative analysis that would compare the respondent's perceptions against reality. This would require interviews and physical access to the respondent's hardware.

In spite of the presented limitations the research in this thesis has set the groundwork for future research in the area of 802.11 wireless security literatures for the home user. Developing improved manual design standards may address the insufficient knowledge that respondents perceive to have on specific wireless security methods. This further research would help individuals understand the specifics of wireless networking, and enable them to be highly proactive in wireless security matters. By enforcing education on respondents by quality literature respondents may therefore implement stronger security methods, reducing their likelihood of becoming a victim to a wireless crime.

CHAPTER 7. REFERENCES

ABS. (2005). *Australian Social Trends Education and Training Higher Education Graduates in the Labour Market.* Retrieved October 14, 2005, from http://www.abs.gov.au/Ausstats/abs@.nsf/94713ad445ff1425ca25682000192af2/e1a27d207c960e79ca256e9e00286295!OpenDocument

AirJack. (2006). *AirJack.* Retrieved April 25, 2006, from http://sourceforge.net/projects/airjack/

AirSnort. (2006). *AirSnort.* Retrieved April 10, 2006, from http://airsnort.shmoo.com/

Airview. (2006). *Airview 1.0.* Retrieved April 27, 2006, from http://sourceforge.net/projects/airview

Alreck, P. L., & Settle, R. B. (1995). *The Survey Research Handbook.* Burr Ridge, IL: Irwin Professional Publishing.

Arbaugh, W. A. (2003). *Wireless Security is Different.* Retrieved 20 August, 2005, from http://ieeexplore.ieee.org/iel5/2/27423/01220591.pdf?arnumber=1220591

Ary, D., Jacobs, L. C., & Razavieh, A. (2002). *Introduction to Research in Education.* Belmont, CA: Wadsworth.

AusCERT. (2005). *Computer Crime & Security Survey.* Retrieved August 30, 2005, from http://www.auscert.org.au/images/ACCSS2005.pdf

Babbie, E. (1990). *Survey Research Methods.* Belmont, CA: Wadsworth.

Babbie, E. (2002). *The basics of social research.* Belmont, CA: Wadsworth/Thomson Learning.

Babbie, E. (2005). *The Basics of Social Research.* Toronto, Ontario: Wadsworth.

Bahli, B., & Benslimane, Y. (2004). An exploration of wireless computing risks: Development of a risk taxonomy. *Information Management & Computer Security, 12*(3), 245.

Barnes, C., Bautts, T., Lloyd, D., Ouellet, E., Posluns, J., & Zendzian, D. M. (2002). *Hack Proofing Your Wireless Network.* Rockland, USA: Syngress Publishing.

Berghel, H., & Uecker, J. (2005). WiFi attack vectors. *Association for Computing Machinery. Communications of the ACM, 48*(8), 21.

Blaikie, N. (1993). *Approaches to social enquiry.* Cambridge, England: Polity Press.

Blank, A. G. (2004). *TCP/IP Foundations.* Alameda, CA: Sybex.

Billion. (2005). *BiPAC 7202 / 7202G (802.11g) ADSL2+ Router User's Manual.* Retrieved August 10, 2005, from http://www.billion.uk.com/support/download/usermanual/usermanual.htm

Bolan, C., & Yek, S. (2004a). *The growth of 802.11b and 802.11g networks in the Perth CBD, Western Australia.*

Bolan, C., & Yek, S. (2004b). *An analysis of security in 802.11b and 802.11g wireless networks in Perth, W.A.* Paper presented at the 2nd Australian Computer, Network and Information Conference in 2004, Esplanade Hotel in Fremantle, Western Australia.

Bowmanm, B. (2002). *802.11a Wireless Networking with Windows XP.* Retrieved April 2, 2006, from http://www.microsoft.com/windowsxp/using/networking/expert/bowman_02july29.mspx

Burness, L., Higgins, D., Sago, A., & Thorpe, P. (2003). Wireless LANs - present and future. *BT Technology Journal, 21*(3), 32.

Cam-Winget, N., Housley, R., Wagner, D., & Walker, J. (2003). Security flaws in 802.11 data link protocols. *Association for Computing Machinery. Communications of the ACM, 46*(5), 35.

Ciampa, M. (2006). *CWNA guide to wireless LANs.* Boston, Mass: Thomson Course Technology.

Cisco. (2003). *2003 Wireless LAN Benefits Study.* Retrieved 22 August, 2005, from http://www.cisco.com/application/pdf/en/us/guest/products/ps4570/c1031/cdccont_0900aecd800cf91f.pdf

Clyde, L. A. (2003). Wi-fi and warchalking. *Teacher Librarian, 31*(1), 44.

Czaja, R., & Blair, J. (2005). *Designing Surveys.* Thousand Oaks, CA: Pine Forge Press.

D-Link. (2004). *D-Link DSL-G604T Wireless ADSL Router User's Guide.* Retrieved August 10, 2005, from http://www.dlink.com.au/default.aspx?ArticleID=740

Eagly, A. H., & Chaiken, S. (1993). *The Psychology of Attitudes.* Orlando, FL: Harcourt Brace Jovanovich.

Ethereal. (2006). *Ethereal: A Network Protocol Analyser.* Retrieved April 25, 2006, from http://www.ethereal.com/

Fenech, S. (2006). Voila, opening the box of tricks. *The Sunday Times,* pp. 4-5.

Frisk, U., & Drocic, S. (2004). *The State of Home Computer Security.* Linkopings University, Linkoping, Sweden.

Furnell, S. (2005). Why users cannot use security. *Computers & Security, 24*(4), 274-279.

Fritze, J. (2005). *Wireless Web for housing sought.* Retrieved October 12, 2005, from http://www.baltimoresun.com/business/realestate/bal-md.wireless10oct10,1,1068437.story?ctrack=1&cset=true

Gittlen, S. (2005). Open source, tried and true. *Network World, 22*(8), 66-68.

Golmie, N., Dyck, R. E. V., Soltanian, A., Tonnerre, A., & Rebala, O. (2003). Interference Evaluation of Bluetooth and IEEE 802.11b Systems. *Wireless Networks, 9*(3), 201.

Guarnieri, S., Noonan, W., Pacifico, D., & Taitelbaum, B. (2005). *WEP Encryption and the Cavalier Wireless Network.* Retrieved May 14, 2006, from http://www.cs.virginia.edu/sammyg/CS551/paper.pdf

Hanna, G. (2005). Securing Wireless Networks Against Intruders. *The CPA Journal, 75*(4), 68-70.

Hänninen, T. (2003). *Wi-Fi Security.* Retrieved 23 August, 2005, from http://www.cs.helsinki.fi/u/lamsal/teaching/autumn2003/student_final/tomi_hanninen.pdf

Henderson, T. (2005). Bountiful Router offers plentiful wireless range. *Network World, 22*(43), 50-52.

Hinchey, P. H. (1998). *Finding Freedom in the Classroom a Practical Introduction to Critical Theory.* New York, USA: Peter Lang Publishing.

Hu, Q., & Dinev, T. (2005). Is spyware an Internet nuisance or public menace? *Association for Computing Machinery. Communications of the ACM, 48*(8), 61.

Jensen, B. K. (2005). An Interview with Jason Romo, CISSP. *Journal of Information Technology Case and Application Research, 7*(2), 49-53.

Kagan, A. (2003). *How Things Work: WLAN Technologies and Security Mechanisms.* Retrieved March 11, 2006, from http://www.sans.org/rr/whitepapers/wireless/1301.php

Karygiannis, T., & Owens, L. (2002). *Wireless Network Security 802.11, Bluetooth and Handheld Devices*, from http://csrc.nist.gov/publications/nistpubs/800-48/NIST_SP_800-48.pdf

Kim, S. H., Mims, C., & Holmes, K. P. (2006). An introduction to current trends and benefits of mobile wireless technology use in higher education. *AACE Journal, 14*(1), 77-100.

Lally, L. (2005). Information Technology as a Target and Shield in the Post 9/11 Environment. *Information Resources Management Journal, 18*(1), 14-15.

Lawson, S. (2005). *The case of the stolen Wi-Fi: what you need to know.* Retrieved April 5, 2006, from http://www.computerworld.com.au/index.php/id;359557196;fp;4;fpid;18

Lim, K. H. (2003). *Security Guidelines for Wireless LAN Implementation.* Retrieved 9 August, 2005, from http://www.sans.org/rr/whitepapers/wireless/1233.php

Lough, D. L. (2001). *A Taxonomy of Computer Attacks with Applications to Wireless Networks.* State University of Virginia.

Maufer, T. A. (2004). *A field guide to wireless LANs for administrators and power users* Upper Saddle River, NJ: Prentice Hall.

Maxim, M., & Pollino, D. (2002). *Wireless Security.* Berkeley, USA: McGraw-Hill.

May, T. (1993). *Social Research Issues, Methods and Process.* Bristol, PA: Open University Press.

McCue, A. (2001). *City firms risk drive-by hacks.* Retrieved August 18, 2005, from http://www.vnunet.com/computing/news/2069189/city-firms-risk-drive-hacks

Motorola. (2003). *User Guide SBG900 Wireless Cable Modem Gateway.* Retrieved August 11, 2005, from http://broadband.motorola.com/consumers/support/default.asp?SupportSection=CableModems

Mussulman, J. (2002). *Scouts Out! - Protecting the Army's Wireless Networks and its impact on Corporate Wireless Computing.* Retrieved July 5, 2006, from http://www.sans.org/reading_room/whitepapers/wireless/173.php

NetComm. (2005). *NetComm Broadband Solutions User Guide.* Retrieved August 10, 2005, from http://www.netcomm.com.au/Support/downloads.php?Category=ADSL&Products=NB5PLUS4W

Netgear. (2005). *Reference Manual for the Model Wireless ADSL Firewall Router DG834G.* Retrieved August 11, 2005, from http://kbserver.netgear.com/inquira/default.asp?question_box=DG834G&collections=kb_file%2Cdatasheets&ui_mode=question&collection_restriction=docs&x=95&y=29

Noble, I. (2001). *Wireless networks wide open.* Retrieved September 21, 2005, from http://news.bbc.co.uk/1/hi/sci/tech/1638920.stm

Oppenheim, R. (2002). Connecting your home office. *Infotech Update, 11*(3), 7-11.

Perelman, L. C., Paradis, J., & Barrett, E. (1998). *The Mayfield Handbook of Technical & Scientific Writing.* Mountain View, CA: Mayfield Publishing Company.

Perrig, A., Stankovic, J., & Wagner, D. (2004). Security in Wireless Sensor Networks. *Association for Computing Machinery. Communications of the ACM, 47*(6), 53-57.

Peterson, B. H., Heninger, W. G., Lindstrom, C. J., & Romney, M. B. (2004). Install Your Own Wireless Network. *Journal of Accountancy, 198*(5), 51-57.

Pollard, M. (2003). *Wireless LAN Security Brisbane CBD Wireless Survey*. Retrieved May 20, 2006, from http://www.bridgepoint.com.au/Default.aspx?tabid=76

Risley, A., & Roberts, J. (2003). *Electronic Security Risks Associated with use of Wireless, Point-to-Point Communications in the Electric Power Industry*. Retrieved August 23, 2005, from http://www.selmsd.com/techpprs/6144.pdf

Rubin, A. D. (2003). Wireless networking security. *Association for Computing Machinery. Communications of the ACM, 46*(5), 28.

Schriver, K. A. (1997). *Dynamics in Document Design*. New York, USA: John Wiley & Sons.

Schultz, E. (2005). Study shows home computer users are ignorant about security. *Computers & Security, 24*(1), 5.

Shay, W. A. (2004). *Understanding Data Communications and Networks*. Belmont, CA: Thomson.

Sheu, S.-T., Tsai, Y., & Chen, J. (2003). MR2RP: The Multi-Rate and Multi-Range Routing Protocol for IEEE 802.11 Ad Hoc Wireless Networks. *Wireless Networks, 9*(2), 165.

Shipley, P. (2001). *Open WLANs the early results of WarDriving*. Retrieved August 25, 2005, from http://www.vjolt.net/vol9/issue3/v9i3_a07-Ryan.pdf

Siemens. (2004). *SpeedStream® 6500 Series Residential Gateway User's Guide*. Retrieved August 10, 2005, from http://www.siemens.com/page/1,3771,1272700-1-999_0_0-9,01.html

Spiga, J. (2004, August). Worry-free wireless. *Australian Personal Computing Magazine*.

Sportack, M. A. (2005). *TCP/IP First-Step*. Indianapolis, IN: CiscoPress.

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2004). Analysis of end user security behaviors. *Computers & Security, 24*(2), 124-133.

Swanson, R. A., & Holton, E. F. (1999). *Results - How to Assess Performance, Learning, and Perceptions in Organisations*. San Francisco, CA: Berrett-Koehler Publishers.

Swartz, N. (2005). War on Terror Targets ISPs in Europe. *Information Management Journal, 39*(5), 10.

Sybex. (2001). *Networking Complete*. Alameda, CA: Sybex.

Tagg, G. (2003). *Wireless LANs – The threats to the Network and how to address them*, from http://www.tagg-consulting.co.uk/Cyprus-Infosec-paper.pdf

Trochim, W. M. K. (2001). *Research Methods Knowledge Base*. Cincinnati, OH: Atomic Dog Publishing.

Turner, R. (2003). *Wireless Security and Monitoring for the Home Network*. Retrieved March 14, 2006, from http://www.sans.org/rr/whitepapers/wireless/1217.php

Ward, M. (2002). *Hacking with a Pringles tube*. Retrieved September 19, 2005, from http://news.bbc.co.uk/1/hi/sci/tech/1860241.stm

Webb, S. (2002). *Wireless InSecurity - Current Issues with Securing WLAN's utilising 802.11b technology*. 3rd Australian Information Warfare and Security Conference, Edith Cowan University.

Webb, S. (2003a). *Identifying Trends in the Deployment and Security of 802.11b Wireless Technology, in Perth, W.A.* Paper presented at the 1st Australian Computer, Information and Network Forensics Conference, Scarborough, Western Australia.

Webb, S. (2003b). *Wireless local area network security: an investigation into security tool usage in wireless networks.* Edith Cowan University, Perth, Western Australia.

Westen, D. (2002). *Psychology - Brain, Behaviour, & Culture*. USA: John Wiley & Sons.

Wieringa, D., Moore, C., & Barnes, V. (1993). *Procedure Writing*. Piscataway, NJ: IEEE Press.

Wirelessdefence. (2006). *Void11*. Retrieved April 26, 2006, from http://www.wirelessdefence.org/Contents/Void11Main.htm

Woodward, A. (2004a). *The risks, costs and possible solutions involved in setting up and running wireless local area networks.* Paper presented at the 2nd Australian Computer Network & Information Forensics Conference, Esplanade Hotel, Fremantle, Western Australia.

Woodward, A. (2004b). *Wireless Jacks - An Analysis of 802.11 Wireless Denial of Service Attacks and Hijacks.* Paper presented at the 3rd European Conference in Information Warfare, Royal Holloway, University of London, UK.

Woodward, A. (2005). *WPA / WPA2: Placebo or panacea?* Paper presented at the 6th Australian Information Warfare & Security conference, Deakin University, Geelong.

Yek, S. (2005). *How to build a faraday cage on the cheap for wireless security testing.* Paper presented at the 3rd Australian Computer, Network & Information Forensics Conference, Edith Cowan University, Perth, Western Australia.

CHAPTER 8. APPENDICES

8.1. Appendix A Letter of Consent to Participants

An attitude and perception study of wireless network usage in home environments.

Dear Respondent

My name is Patryk Szewczyk and I am conducting research on the attitudes and usage of wireless networks at home or in a small office as part of my Honours thesis in Computer Science at Edith Cowan University. If you have any questions or require any further information about the research project please contact Patryk Szewczyk or Dr Craig Valli. Furthermore if you have any concerns or complaints and would like to talk to an independent person, you may contact the Research Ethics Office whose details are provided below.

As you may be aware numerous companies are offering high speed Internet access, and several adverts are emphasising the use of wireless and thus mobile computing. For you this means you are accessing the Internet from a computer which is not directly connected to a network device via a cable but rather through wireless transmissions. I invite you to complete a questionnaire requiring approximately 10 minutes, about your experiences and thoughts on wireless networking in the home.

The purpose of the research is to determine if users are utilising the technology securely and understand the concepts and properties of wireless networks. The research will provide useful information about how secure or insecure individuals are when using their wireless devices and the information sources used by home users when setting up a wireless network at home.

The research will be conducted anonymously and securely via an online, web based questionnaire, and we ask that you do not place your name or anything which may identify you on the survey. Please provide your honest opinion or recollections, as there are no wrong or right answers. You are free to withdraw or not participate from the questionnaire and this will not disadvantage you in any manner. Questions may be skipped, and the survey may be stopped at any point.

All data from the survey will be stored securely on an internal server located within the School of Computer and Information Science. Access to the data will be restricted solely to the researcher and supervisor, Dr Craig Valli. All data will remain encrypted during the gathering and analysis process and properly erased and disposed of on completion of the research.

I would like to thankyou in advanced for your contribution to this vital research.

Yours Sincerely

Patryk Szewczyk
School of Computer and Information Science
Edith Cowan University, Perth Western Australia
Email: pszewczy@student.ecu.edu.au

Dr. Craig Valli
Edith Cowan Unversity
Senior Lecturer – Computer and Network Security
c.valli@ecu.edu.au
Phone +61-8-9370-6162
Fax +61-8-9370-6100

Research Ethics Office
Edith Cowan University
100 Joondalup Drive
JOONDALUP WA 6027
research.ethics@ecu.edu.au
Phone +61-8-6304-2170

8.2. Appendix B Survey Instrument

This questionnaire is designed to question your attitude, understanding and beliefs towards wireless computing in your home or office. The questionnaire is a component of a thesis and is being conducted by Patryk Szewczyk an honours student in Computer Science. All responses are voluntary, anonymous and confidential. Select your answer by placing a tick in the appropriate box, unless otherwise specified.

1. I have a wireless connection for my home or small office computer

Yes	☐	No	☐

2. I use the following connection type to connect to the Internet at home.

Dialup	☐	Broadband	☐
Unsure	☐		
Other *(please specify)*			
_____			

3. I use the following company when connecting to the Internet

Telstra/Bigpond	☐	iinet	☐
Optus	☐	I-Primus	☐
Westnet	☐	Dodo	☐
Other *(please specify)*			
_____			

4. I am currently working, or have worked previously in the **IT industry**

Yes	☐	No	☐

5. I have **successfully** configured a computer network

Yes	☐	No	☐

6 I chose wireless rather than using a network cable to access the Internet because *(choose all that apply)*

a. Convenience	☐	d. Increased speed	☐
b. No messy cables	☐	e. Easy to set up	☐
c. Mobility	☐		

11 Was **any** security discussed with you purchased the wireless computer product?

Yes	☐	No	☐

12 When you purchased your wireless computer product, did you enquire about **any** security?

Yes	☐ (go to question 13)	No	☐ (go to question 14)

13 If you chose 'yes' for question 12 which specific security features were important to you?

WEP (Wired Equivalent Privacy)	☐
Key Length	☐
WPA (Wi-Fi Protected Access)	☐
MAC Control List (Restrict Client Access)	☐
Firewall or Virus Protection	☐
Other *(please specify)*	
_____	

14 Who setup your wireless computer product?

Myself	☐
Household Friend/Family	☐
Outside Friend/Family	☐
Computer Technician	☐
Other *(please specify)*	
_____	

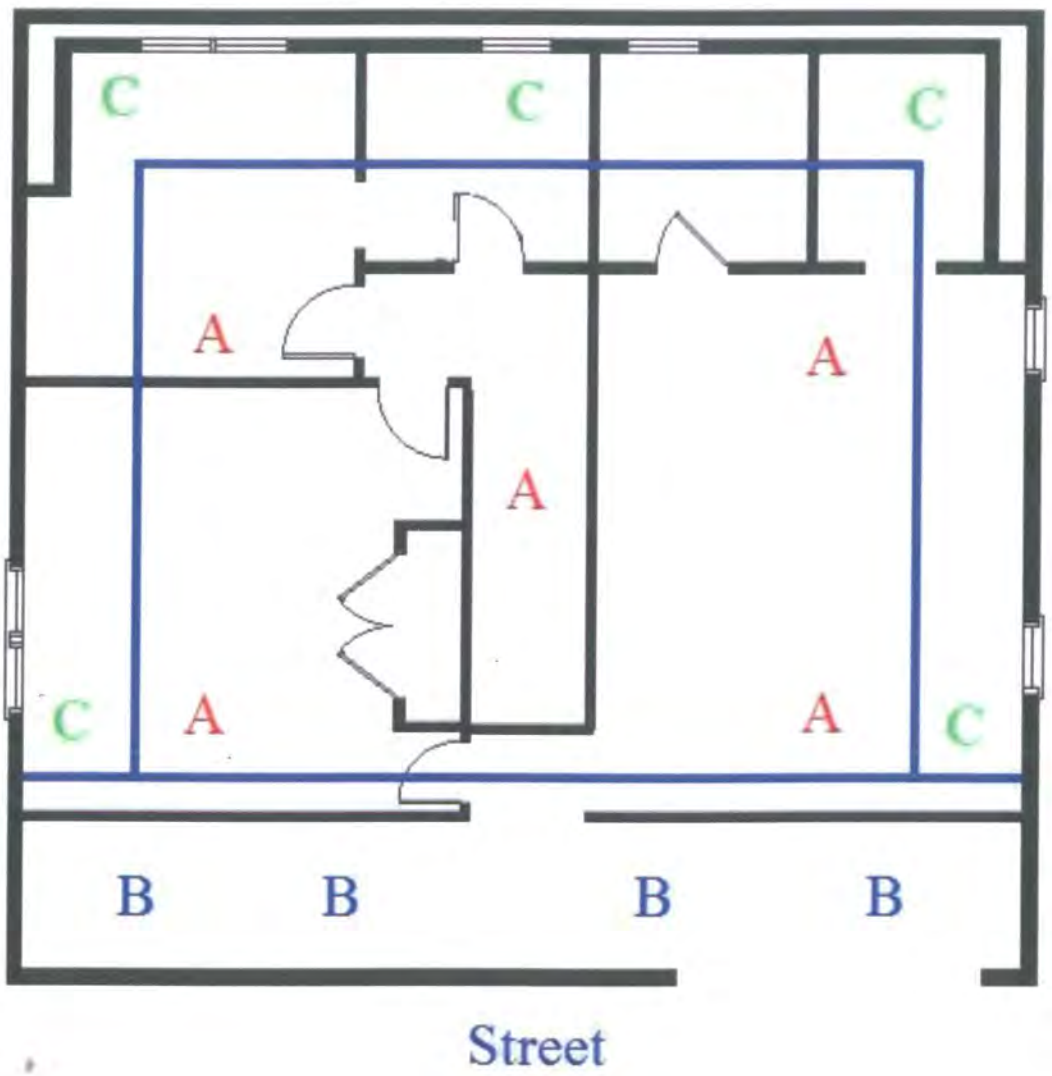
15 Where was information obtained from to setup the wireless product?

Prior Knowledge	☐
Quick Start Guide	☐
Internet	☐
Don't Know	☐
Other *(please specify)*	
_____	

16 Are you using any of the following security features on your wireless computer product?

Open System	☐
Shared Key	☐
WEP (Wired Equivalent Privacy)	☐
WPA (Wi-Fi Protected Access)	☐
WPA-PSK (Wi-Fi Protect Access - Pre Shared Key)	☐
Don't know	☐

17 The physical placement of the wireless box/access point in my home or office is (*choose most appropriate*)?



A: Centre of house	☐
B: Street side perimeter	☐
C: Side or rear perimeter	☐

18 Have you checked if wireless coverage is available beyond the perimeter of your house?

Yes	☐	No	☐

How concerned are you with the following when using your wireless Internet?

	Not Concerned			Extremely Concerned
19. Money loss due to wireless fraud	☐	☐	☐	☐
20. Ensuring personal data is not exposed	☐	☐	☐	☐
21. Ensuring wireless is always available	☐	☐	☐	☐
22. Ensuring personal data has not been altered	☐	☐	☐	☐

23 How **vulnerable** is your wireless product?

Not vulnerable	Moderately	Extremely	Don't know
☐	☐	☐	☐

24 Do you believe you are at risk by using wireless to access the Internet?

Yes	☐	No	☐

25 What has been your experience of **configuring** your wireless product?

Very Positive	Positive	Negative	Very Negative
☐	☐	☐	☐

26 What has been your experience of **using** your wireless product?

Very Positive	Positive	Negative	Very Negative
☐	☐	☐	☐

27 Please specify your age group.

18 - 24	☐	25 - 34	☐
35 - 44	☐	45 - 54	☐

55+	☐

28 Gender

Male	☐	Female	☐

29 Location:

Postcode	☐

Thank you for taking the time to complete this questionnaire.

All data is confidential and participants remain anonymous.