ASSESSING FACTORS INFLUENCING WI-FI SECURITY IMPLEMENTATIONS IN NAIROBI’S CENTRAL BUSINESS DISTRICT

BY

JANET N. WACHIRA

UNITED STATES INTERNATIONAL UNIVERSITY

SUMMER 2017
ASSESSING FACTORS INFLUENCING WI-FI SECURITY IMPLEMENTATIONS IN NAIROBI’S CENTRAL BUSINESS DISTRICT

BY

JANET N. WACHIRA

A Project Report Submitted to the School of Science and Technology in Partial Fulfillment of the Requirement for the Degree of Master of Science in Information Systems and Technology

UNITED STATES INTERNATIONAL UNIVERSITY

SUMMER 2017
STUDENT’S DECLARATION

I, the undersigned, declare that this is my original work and has not been submitted to any other college, institution or university other than the United States International University in Nairobi for academic credit.

Signed: ________________  Date: ________________

Janet Njeri Wachira (ID No 631182)

This project has been presented for examination with my approval as the appointed supervisor.

Signed: ________________  Date: ________________

Paula Musuva-Kigen

Signed: ________________  Date: ________________

Dean, School of Science and Technology
Copyright

All rights reserved. No part of this project may be photocopied, recorded or otherwise reproduced, stored in retrieval system or transmitted in any electronic or mechanical means without prior permission of USIU-A or the author.
Janet Wachira © 2017
ABSTRACT

The technology scene in Kenya has seen tremendous growth in recent years. Many citizens own gadgets with internet and wireless access capabilities leading to a heavier online presence. By the end of March 2017, the Communications Authority of Kenya recorded 40.5 million registered internet users. Mobile data/internet subscriptions were 21.5 million contributing to 99% of the total internet subscriptions. Kenya’s internet bandwidth stood at 2,906.8Gbps (CAK, 2017).

Internet Service Providers (ISPs) such as Safaricom, Jamii Telecommunications (JTL) and Zuku have been successful in providing wireless network access to organizations, small-medium business owners and home users alike (CAK, 2017).

Wired networks require physical connection through cables to access the network. By contrast, Wi-Fi networks broadcast Radio Frequency (RF) signals into the air for any wireless device within reach to access. This opens Wi-Fi networks to vulnerabilities such as eavesdropping, Denial of Service (DoS) attacks, MAC spoofing and evil twin attacks (Zou, Wang, & Hanzo, 2015).

The purpose of this study was to assess the factors that influence the level of security implementations on Wi-Fi networks in Nairobi’s Central Business District (CBD). Using and extending the Protection Motivation Theory, the study tested the socio-cognitive factors influencing decisions to implement security measures on Wi-Fi networks. The study examined the influence of Perceived Vulnerability, Perceived Severity, Rewards, Response Efficacy, Self-efficacy, Response Cost, Vendor Support and Pressures on the Intent to secure Wi-Fi networks. Intent is then measured against the implemented Wi-Fi security measures observed.

The descriptive design approach was used to review the Wi-Fi security implementations in place. This involved conducting two wardrives within Nairobi’s CBD. The population for this study was the number of Wireless Access Points (WAPs) that were discovered. This was an average of 1816 WAPs.

Out of this, the sample size was determined by use of convenience sampling where 45 WAPs from Moi Avenue, Mama Ngina Street, Kimathi Street and Kaunda Street were tested. A limiting factor to the number of WAPs used in the sample size was the ability to identify specific business premises from the name given to Wi-Fi hotspots. Some of the
buildings hosted numerous businesses and it was not possible to access or get cooperation from every office.

Data from the wardrive was collected by use of Kismet and BlueNMEA. It was then mapped to Google Maps using GisKismet. A questionnaire was used to measure the various factors in the research model. The questionnaires were distributed to the 45 businesses from the sample size. The data was analyzed using PLS-SEM, because it is suited to studies with small sample sizes and for exploratory model building.

The structural model met the requirements for composite reliability, convergent and discriminant validity. The measurement model explained 78% of the variance in the dependent variable, Intention to implement Wi-Fi security. Three of the nine hypotheses put forward were supported by the data. This shows that rewards, response-efficacy and pressures significantly affect the intention of users to implement Wi-Fi security. Perceived Vulnerability, Perceived Severity, Self-efficacy, Response Cost and Vendor Support are statistically not significant in determining the intention of users to implement Wi-Fi security.

It is recommended that future research make use of online survey instruments so as to reach more respondents. Wardriving efforts with consent from participants can include penetration tests of Wi-Fi networks discovered, as this may have a stronger influence on recommending implementation of Wi-Fi security.

**Key Words:**

WLAN, Wi-Fi, WEP, WPA, WPA2, Nairobi, wardriving, Wi-Fi Security, Protection Motivation Theory, PMT.
ACKNOWLEDGMENT

This research project was a successful effort thanks to the help and support of many. I wish to express gratitude to the entire faculty team of the USIU School of Science and Technology who have unreservedly shared their time and wisdom and impacted a lot of knowledge throughout my Master’s Program.

Special thanks go to my project supervisor, Mrs. Paula Musuva-Kigen for her never-ending guidance, support and sheer willpower to see to the completion of this research project.
Table of Contents

Copyright................................................................................................................. iii
ABSTRACT............................................................................................................ iv
ACKNOWLEDGMENT................................................................................................... vi
List of Tables........................................................................................................... x
List of Figures........................................................................................................... xi
CHAPTER 1: INTRODUCTION.................................................................................... 1
  1.1. Background of the Problem ........................................................................... 1
  1.2. Statement of the Problem............................................................................. 6
  1.3. Purpose of the Study.................................................................................... 8
    1.3.1. Specific Objectives................................................................................ 8
  1.4. Significance of the Study............................................................................ 8
  1.5. Scope of the Study..................................................................................... 8
  1.6. Definition of Terms................................................................................... 9
  1.7. Chapter Summary..................................................................................... 9

CHAPTER 2: LITERATURE REVIEW SECTION...................................................... 10
  2.1. Introduction.................................................................................................. 10
  2.2. Assess Wi-Fi Security Risks, Vulnerabilities and Mitigations.................... 10
  2.3. Identify the Current State of Security Implementations on City-Wide Wi-Fi Networks.. 17
  2.4. Assessing Factors Influencing Wi-Fi Security Implementations Using the Protection Motivation Theory.................................................................22
  2.5. Research Approach................................................................................... 25
  2.6. Chapter Summary..................................................................................... 26

CHAPTER 3: METHODOLOGY................................................................................. 27
  3.1. Introduction.................................................................................................. 27
  3.2. Research Design......................................................................................... 27
  3.3. Population and Sampling Design................................................................ 28
    3.3.1. Population............................................................................................. 28
    3.3.2. Sampling Design.................................................................................. 28
  3.4. Data Collection Methods........................................................................... 29
  3.5. Research Procedures.................................................................................. 31
    3.5.1. Wardriving............................................................................................ 31
    3.5.2. Questionnaire Survey .......................................................................... 37
  3.6. Data Analysis Methods............................................................................... 37
  3.7. Ethical Considerations................................................................................ 38
3.8. Chapter Summary .......................................................................................................... 38

CHAPTER 4: MODEL ............................................................................................................ 39

4.1. Introduction .................................................................................................................. 39
4.2. Analysis ......................................................................................................................... 39
4.3. Modelling ...................................................................................................................... 41
4.3.1. Conceptual Model .................................................................................................... 45
4.3.2. Measurement Model ............................................................................................... 50
4.5. Proof-of-Concept ......................................................................................................... 52
4.6. Chapter Summary ....................................................................................................... 53

CHAPTER 5: RESULTS AND FINDINGS ...................................................................... 54

5.1. Introduction .................................................................................................................. 54
5.2. Wi-Fi Security Mitigations against Vulnerabilities and Risks ...................................... 54
5.3. Identifying Current State of Security Implementations in Nairobi’s CBD .................. 57
5.4. Assessing Factors Influencing Wi-Fi Security Implementations Using PMT ............. 62
5.4.1. Measurement Model Analysis ................................................................................. 64
5.4.2. Structural Model Analysis ...................................................................................... 68
5.5. Chapter Summary ....................................................................................................... 70

CHAPTER 6: DISCUSSION, CONCLUSIONS & RECOMMENDATIONS ...................... 71

6.1 Introduction .................................................................................................................. 71
6.2 Summary ....................................................................................................................... 71
6.3. Discussion .................................................................................................................... 73
6.3.1. Wi-Fi Security Mitigations against Vulnerabilities and Risks .................................. 73
6.3.2. Current State of Wi-Fi Security Implementations in Nairobi’s CBD ...................... 73
6.3.3. Assessing Factors Influencing Wi-Fi Security Implementations Using PMT .......... 74
6.3.3.1. Effect of Perceived Vulnerability on implementation of Wi-Fi security measures. .... 74
6.3.3.2. Effect of Perceived Severity on implementation of Wi-Fi security measures .......... 75
6.3.3.3. Effect of Rewards on implementation of Wi-Fi security measures ....................... 75
6.3.3.4. Effect of Response Efficacy on implementation of Wi-Fi security measures .......... 76
6.3.3.5. Effect of Self Efficacy on implementation of Wi-Fi security measures ................. 76
6.3.3.6. Effect of Response Cost on implementation of Wi-Fi security measures ............... 77
6.3.3.7. Effect of Vendor Support on implementation of Wi-Fi security measures ............. 77
6.3.3.8. Effect of Pressures on implementation of Wi-Fi security measures ..................... 78
6.3.3.9. Effect of Intent on actual implementation of Wi-Fi security measures ................... 78
6.4 Conclusion .................................................................................................................... 79
6.5 Recommendations & Future Work .............................................................................. 79
List of Tables

Table 3.4.1: Summary of various Wardriving Tools .................................................. 29
Table 4.3.2: Questionnaire Sources .......................................................................... 50
Table 5.3.1: Displays summary of the wardrive results breakdown .......................... 62
Table 5.4.1: Display of the demographics summary ................................................... 63
Table 5.4.2: Summary of Goodness-of-Fit statistics ................................................... 64
Table 5.4.1.1: Displays results of Cronbach’s alpha, composite reliability, convergent
reliability and multicollinearity VIF ......................................................................... 65
Table 5.4.1.2: Discriminant validity using Square roots of Average Variances Extracted
(AVEs) .................................................................................................................... 66
Table 5.4.1.3: Structure Matrix of Combined Loadings and Cross-Loadings .......... 67
Table 5.4.2.1: Effect size contributions ..................................................................... 69
Table 5.4.2.2: Summary of Tests of Hypotheses ....................................................... 70
Table 6.2.1: Displays a summary of hypotheses tested and their results ............... 72
List of Figures

Figure 1.1.1. How Wi-Fi transmits data .......................... 2
Figure 1.5.1: A map depicting Nairobi’s Central Business District .......................... 9
Figure 2.2.1.1: Summary of the WEP encryption process (Poddar, 2014) .................. 12
Figure 2.2.2.1: WPA Encryption Process (Poddar, 2014) .................................. 14
Figure 2.2.3.1: WPA2 Encryption Process (Vilius et al., 2015) ......................... 15
Figure 3.5.1: A display of the Kismet startup page ......................... 32
Figure 3.5.2: Capture of the Kismet Server Startup options .................. 33
Figure 3.5.3: Adding wireless interface capture source .................. 33
Figure 3.5.4: An external wireless card – ALFA AWUS036NHA .................. 34
Figure 3.5.5: Kismet running with no GPS data .......................... 34
Figure 3.5.6: adb Command Forwarding TCP 4352 .......................... 35
Figure 3.5.7: gpsd Command Enabling Transfer of GPS Location Data ............ 35
Figure 3.5.8: BlueNMEA running on my Android phone .................. 36
Figure 3.5.9: Terminal displaying successful read on gpsd .................. 36
Figure 4.3.1: Conceptual Model of the Protection Motivation Theory ............... 45
Figure 4.5.1: Kismet server displaying captured packets in the USIU area .......... 53
Figure 5.2.1: Illustrating Default SSID changed, WPA2 enabled & WPS disabled ...... 54
Figure 5.2.2: Setup of Guest Network .................................. 55
Figure 5.2.3: Firewall setup on the access point .......................... 55
Figure 5.2.4: MAC address Filtering and WPS disabled. ....................... 56
Figure 5.2.5: Enabling VPN protection on Android Device using F-Secure ........... 56
Figure 5.2.6: VPN Features ............................................. 57
Figure 5.3.1: Querying GisKismet database & specifying KML output ................ 58
Figure 5.3.2 SQLite database displaying WAPs from the first wardrive ............... 58
Figure 5.3.3: SQLite database displaying WAPs from the second wardrive ........... 59
Figure 5.3.4 Map of all the WAPs discovered in Nairobi’s CBD .................. 59
Figure 5.3.5: Map of all the WAPs using WPA+PSK & WPA+AES .................. 60
Figure 5.3.6: Map of all the WAPs using WPA+TKIP WPA+PSK & WPA+AES .... 60
Figure 5.3.7: Map of all the WAPs using no encryption protocol from wardrive 1 .... 61
Figure 5.3.8: Map of all the WAPs using WEP encryption from wardrive 1 .......... 61
Figure 5.4.2.1: Results of the Structural Model Testing ....................... 68
### Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AES</td>
<td>Advanced Encryption Standard</td>
</tr>
<tr>
<td>CRC</td>
<td>Cyclic Redundancy Check</td>
</tr>
<tr>
<td>DDoS</td>
<td>Distributed Denial of Service</td>
</tr>
<tr>
<td>GPS</td>
<td>Global Positioning System</td>
</tr>
<tr>
<td>GPSD</td>
<td>Global Positioning System Device</td>
</tr>
<tr>
<td>ICV</td>
<td>Integrity Check Value</td>
</tr>
<tr>
<td>IDS</td>
<td>Intrusion Detection System</td>
</tr>
<tr>
<td>IEEE</td>
<td>Institute of Electrical and Electronics Engineers</td>
</tr>
<tr>
<td>ISPs</td>
<td>Internet Service Providers</td>
</tr>
<tr>
<td>IV</td>
<td>Initialization Vector</td>
</tr>
<tr>
<td>JTL</td>
<td>Jamii Telecommunications</td>
</tr>
<tr>
<td>MIC</td>
<td>Message Integrity Check</td>
</tr>
<tr>
<td>NMEA</td>
<td>National Marine Electronics Association</td>
</tr>
<tr>
<td>OSI</td>
<td>Open Systems Interconnection</td>
</tr>
<tr>
<td>MIC</td>
<td>Message Integrity Check</td>
</tr>
<tr>
<td>MiTM</td>
<td>Man-in-the-Middle Attack</td>
</tr>
<tr>
<td>PRNG</td>
<td>Pseudo-Random Number Generator</td>
</tr>
<tr>
<td>RC4</td>
<td>Rivest Cipher 4</td>
</tr>
<tr>
<td>RFMON</td>
<td>Radio Frequency Monitor Mode</td>
</tr>
<tr>
<td>RSSI</td>
<td>Received Signal Strength Indicator</td>
</tr>
<tr>
<td>SSID</td>
<td>Service Set Identifier</td>
</tr>
<tr>
<td>SMEs</td>
<td>Small-to-Medium Enterprises</td>
</tr>
<tr>
<td>TKIP</td>
<td>Temporal Key Integrity Protocol</td>
</tr>
<tr>
<td>WAPs</td>
<td>Wireless Access Points</td>
</tr>
<tr>
<td>WEP</td>
<td>Wired Equivalent Privacy</td>
</tr>
<tr>
<td>WiGLE</td>
<td>Wireless Geographic Logging Engine</td>
</tr>
<tr>
<td>WPA2</td>
<td>Wi-Fi Protected Access, Version 2</td>
</tr>
<tr>
<td>WPS</td>
<td>Wi-Fi Protected Setup</td>
</tr>
<tr>
<td>Wi-Fi</td>
<td>Wireless Fidelity</td>
</tr>
<tr>
<td>WLANs</td>
<td>Wireless Local Area Networks</td>
</tr>
<tr>
<td>XOR</td>
<td>Exclusive OR</td>
</tr>
</tbody>
</table>
CHAPTER 1: INTRODUCTION

This chapter covers the adoption, implementation and use of Wi-Fi networks in the modern age of digital communication. It explores the benefits provided by Wireless Local Area Networks as well as the various ways its advantages can be exploited by malicious outsiders to gather information and/or exploit the network.

The chapter states the problem and the purpose of the study, the main objectives as well the significance of the study and its contribution to the body of knowledge. The scope of the study is also covered here.

1.1. Background of the Problem

1.1.1. Understanding Wi-Fi Networks

The term Wi-Fi is used alternatively to refer to Wireless Local Area Networks (WLANs). This is because IEEE defines Wi-Fi as any WLAN product that adheres to the 802.11 standard and most Wi-Fi networks conform to the 802.11 standard (Varma, 2012). All wireless networks connect back to a wired network at some point.

Wireless LANs constitute of Wireless Access Points (WAPs), wireless clients that have wireless adapters installed on them and wireless routers that help route the traffic. Wi-Fi uses radio frequency (RF) signals to connect to the network. The wireless adapter translates the data sent to it into a radio signal. An antenna is used to send the RF signals to the wireless router that then decodes the RF signals to data once again. The data is then forwarded to the internet through a wired Ethernet network. Wi-Fi networks emit frequencies between 2.4 GHz and 5 GHz. The amount of traffic passing through the Wi-Fi network determines the speeds the devices connected to it will be able to use (Brain, Wilson, & Johnson, 2001).

The various standards under the IEEE 802.11 have different bandwidth and data rate capabilities. 802.11a and 802.11g can transmit data at 6 - 54Mb/s using a bandwidth of 20MHz. 802.11b has data speeds of 1 - 11Mb/s and a bandwidth of 22MHz. 802.11n and 802.11a transmit at speeds between 7.2 – 433.3 Mb/s using bandwidth of 20 – 80 MHz (Babiker, Abdelrahman, Babiker, Mustafa, & Osman, 2015).

Fig 1.1.1 shows how devices may be interconnected on a network and transmit data through Wi-Fi.
Figure 1.1.1. How Wi-Fi transmits data (Eusso, 2007)

Wired networks are more secure than wireless networks (Varma, 2012). Wired networks require physical connection through cables to access the network unlike wireless networks whose RF signals are broadcast into the air for any wireless router within reach to access. This makes the information carried on Wi-Fi networks more vulnerable.

Nevertheless, Wi-Fi networks have grown in popularity due to their ease of setup and low costs incurred during installation (Gameli, 2016). Wired networks require pre-planning before installation especially in areas where the public is to use it. Network cables have to be fitted into walls before the complete construction of a building is done - which generally means that they are more labor and cost intensive in comparison to Wi-Fi networks. Even for buildings that have already incorporated wired networks, expanding the network layout through use of Wi-Fi networks usually proves cheaper and faster.

Wireless LANs have been implemented extensively in Kenya. Mobile devices, smartphones, tablets and laptops are now equipped with inbuilt wireless adapters thereby increasing Wi-Fi adoption. Hotspots are easily created by one mobile device providing internet connectivity to a number of other devices.

Rather than use the more expensive 3G or 4G connections from their ISPs, many residential users have implemented Wi-Fi networks in their homes. Restaurants, coffee houses, salons, public service vehicles (PSVs) and large organizations have also employed the use of Wi-Fi networks to capitalize on its various benefits. Small businesses use Wi-Fi networks to increase traffic flow of their clientele to their businesses.
1.1.2. Attacks on Wi-Fi Networks

As the popularity and accessibility of this more vulnerable network grows, so does the number of malicious network attackers and intruders (Vilius, Liu, Panneerselvam, & Stimpson, 2015). The lure to point out the glaring security vulnerabilities of a network seems unsurpassable to hackers. The 2016 Global Economic Report shows cybercrime to be the second most performed economic crime worldwide (PwC, 2016). Hackers use the most vulnerable device on the network to exploit systems. If a Wi-Fi network uses weak security, it stands a higher chance of being exploited by malicious attackers.

The architecture employed by Wi-Fi networks is mostly similar to that of wired networks. It incorporates the OSI model in the transmission of data packets over the different layers (Tamimi & Abdel-Karim, 2006). The OSI model consists of seven layers namely; the Physical, Medium Access Control (MAC), Network, Transport, Session, Presentation and Application layers. Wi-Fi networks however, do not implement the presentation and session layers.

According to Zou et al. (2015), users are susceptible to the following types of network layer attacks that can be meted out on poorly secured Wi-Fi networks.

Attacks on the Physical layer include:

i. Eavesdropping – where the attacker listens in on communications between two nodes to gather information.

ii. Denial of Service attacks by jamming – where the attacker denies legitimate users of the network access to it.

Attacks on the Medium Access Control layer include:

i. MAC spoofing – where an attacker will change the assigned MAC address of his network node in an attempt to spoof another network’s MAC for malicious purposes.

ii. MiTM attacks – where an attacker routes traffic between sender and receiver on a network to pass through him.

iii. Identity theft – where a MAC attacker will pretend to be another legitimate network node to gain access to confidential information on the victim’s network. This can be achieved through MAC spoofing.

iv. Network injection – the attacker will inject bogus network reconfiguration commands that paralyze intelligent network devices such as routers and switches.
The network devices may have to be rebooted or reprogrammed for the network get back up.

At the Network layer, Wi-Fi networks are susceptible to the following attacks:

i. IP Spoofing – where the attacker forges a false IP address with the aim of hiding their true identity or impersonating another network node for the purposes of carrying out illegitimate activities. The network node communicating with the falsified source IP address will send responses back to the forged IP address. This type of attack is capable of paralyzing the network by flooding it with forged IP packets.

ii. IP Hijacking – where attackers take over legitimate users IP addresses on a given network and use that connection to access confidential information. Where the attacker is successful, the legitimate network node is dropped from the network.

iii. Smurf attack – is a form of denial of service attack where the attacker broadcasts ICMP packets using a spoofed IP address to a group of legitimate users on the network. Once the destined network nodes receive the ICMP requests, they are required to send back responses. If too many nodes get the broadcast, the network becomes paralyzed from all the overwhelming traffic on it.

The Transport Layer is susceptible to the following attacks:

i. TCP / ping flooding – similar to a smurf attack in the network layer, ping flooding is a type of Denial of Service (DoS) attack where numerous pings in the form of ICMP echoes are sent to the targeted node. This results in ping replies which both floods the buffers of the victim node and end up delaying connection on that network.

ii. UDP flooding – Similar to TCP flooding, in this type of attack, numerous UDP packets are sent out to a targeted node which is forced to attempt to reply to all the packets. If the number of packets is sufficiently high, legitimate packets attempting to communicate with the targeted node will find it unreachable. The attacker is able to spoof their IP address making them undetectable from legitimate nodes.

iii. TCP sequence prediction attack – the attacker will attempt to predict the sequence number of the victim’s TCP packet and fabricate his own packets with the victim’s sequence number. If the attacker succeeds, he can take over a victim’s
communication session with the transmission node where subsequent communications will appear to be coming from the legitimate transmission node.

To understand the various ways exploitation of Wi-Fi networks has been made possible, it is necessary to understand the underlying Wi-Fi security protocols put in place over the years by the IEEE and how malicious attackers have worked to find vulnerabilities that they can exploit.

One user with access to the wired network could create a hotspot using his connection to give many users wireless internet connections. Wireless Access Points (WAPs) can be purchased and easily setup to connect to existing wired networks. The WAPs may come with manuals directing the user on how to setup their network. The problem with this method of network creation is majority of users, after having successfully setup the Wi-Fi network, are likely to disregard the security instructions on the manuals that come with the WAP. They are more likely to leave the default password that come with the WAP and leave the Wi-Fi network unprotected by any security protocol altogether (Vilius et al., 2015).

This is because majority of users - even the technologically savvy- seem to share the same thought process that leads them to believe they are too far removed from the likelihood of a Wi-Fi network attack (Harbach, Fahl, & Smith, 2014). They think that these sort of attacks only happen in first world countries or to big institutions who are the likelier targets of such attacks.

For users who get their WAPs from ISPs, security policies and protocols come pre-configured. However, despite the secure APs, the security nature of the wireless networks also depends on the hardware devices being connected to the network. Security policies are subjected to timely updates, and some of the legacy hardware may not be supported to be compatible with the newly developed security protocols. This scenario may result in weaker security policies for a given entire wireless network, and possibly compromising the security features of other capable devices belonging to the network. This type of scenario leaves all users of the Wi-Fi network vulnerable to a myriad of malicious attacks (Vilius et al., 2015).

The Serianu (2012) report cites numerous weaknesses associated with Kenyan ISPs. These include weaknesses such as spamming, phishing and poor reputation scores.
Internet connected computers in Kenya are infected with malicious programs that expose users to risks such as loss of personal data and increased susceptibility to online fraud. As a result, email and web traffic from Kenya was filtered and blocked.

It is primarily important for the customers to review the security protocols of their WAPs and they should also not ignore security updates. IT literates often ensure their data protection by the use of strong security protocols, while users without complete understanding of the security requirements might go with the default security settings of their WAPs in fear of losing or corrupting their network setup (Vilius et al., 2015).

Common practices within a home-based wireless networks, involve providing access and sharing of passwords with guest users, and at times this access might also be left open and users may not habitually reset their passwords. All these practices are categorized as weak security practices, which might leave the network vulnerable and susceptible to unauthorized access (Vilius et al., 2015).

Owing to the available open source platforms, such vulnerabilities can be exploited by the malicious players, on the insecure networks, for launching various types of network attacks. Also the quality of the security protocols is often challenged by the ever-emerging attacking techniques.

1.2. Statement of the Problem

Introduction of Wi-Fi networks in Kenya has seen many organizations and businesses adopt it as a strategy to cut costs. The allure of free or subsidized internet access has not escaped smart device owners. Anyone with knowledge of a convenient Wireless Access Point will put aside their internet-related activities until they can access the Wi-Fi network. This allows the user to cut on data network charges that are incurred from subscription-based services from their ISPs.

Majority of Wi-Fi users are not aware of the dangers underpinning an unsecured network. They will altogether ignore headlines on cybercrime believing themselves to be too far removed from the target of such an attack (Harbach et al., 2014). They will therefore, continue to access and connect to open Wi-Fi networks conducting a myriad of activities (that include providing usernames and passwords to access multiple sites, conducting
online banking transactions etc.) as long as they believe it to be free and are unaware of any risks on the corresponding network.

Small business and home owners find it easy enough to set up wireless routers after purchase by following instructions that come with the manual. What they are likely to leave out of their set up are the highly recommended security settings in fear of corrupting their current working configuration or complicating management of the Wi-Fi network any further (Vilius et al., 2015). As a result, a malicious attacker may find it easy getting through these weakly configured installations. Subsequently, they can access users’ work and personal information, their credit card and bank statements and even gain complete control of the users' devices.

Kenya recorded economic losses of up to Kshs.15 billion in 2015 attributed to cybercrime and cyber fraud (Serianu, 2015). The PWC Global Economic Survey reported a steady rise of cybercrime in Africa - 57% in 2016 compared to 50% in 2014. Malicious attackers exist at local and regional levels and have been getting away with numerous types of attacks that yield billions of shillings.

Majority of domestic and small business owners of Wi-Fi networks believe themselves to be below the target of a malicious attack. Such headlines are believed to only affect large organizations or government institutions(Harbach et al., 2014).

To be able to be able to understand the factors that influence a users’ intention to secure their Wi-Fi networks, the Protection Motivation Theory (PMT) was used. PMT is a predictive model that helps assess user’s intention to adopt protective measures. It has been borrowed from the health and social sciences due to its effectiveness in predicting an individual’s intention to engage in protective behavior (Rogers & Maddux, 1983). It has been successfully used in smoking cessation, safety-belt campaigns, self-breast examinations and natural disaster precautionary action. It has also been adopted in numerous other information security research papers (Chenoweth, Minch, & Gattiker, 2009; Crossler, 2010; Dupuis, Crossler, & Endicott-popovsky, 2016; Li & Qian, 2016; Woon, Tan, & Low, 2005).
1.3. Purpose of the Study
The purpose of this study is to assess the factors that influence the level of security implementations on Wi-Fi networks in Nairobi’s Central Business District.

1.3.1. Specific Objectives
Following are the main objectives of this research paper:

1. Assess Wi-Fi networks’ security risks, vulnerabilities and mitigations
2. Identify the current state of security implementations on city-wide Wi-Fi networks.
3. Assess factors that influence Wi-Fi security implementations using the Protection Motivation Theory.

1.4. Significance of the Study
Both Small-Medium Businesses (SMBs) and public Wi-Fi users who implement and make use of Wi-Fi networks will gain value from this research. This research presents Wi-Fi security findings that relate to the local Kenyan context. By incorporating the Protection Motivation Theory, the research objectively shows the dire need for security implementation while educating end users on the risks and threats they expose themselves to everyday by connecting to unsecured Wi-Fi networks.

1.5. Scope of the Study
Several reports on security of the Kenyan landscape have been released in recent years, detailing the cyber security threats facing the country. These reports however, concentrate mainly on threats facing organizations. This study will assess the factors that influence the level of security implemented on the publicly accessible Wi-Fi networks. This research seeks to cover publicly accessible Wi-Fi networks that have end users connecting to them in areas such as coffee shops, restaurants, hotels and even modes of transport such as public service vehicles.

The study will focus on Nairobi’s Central Business District particularly, Moi Avenue, Mama Ngina Street, Kimathi Street and Kaunda Street. These streets were chosen for their high number of coffee shops, restaurants and clubs which provide Wi-Fi services to their clientele. The level of security of a Wi-Fi network will be determined by the security protocols (either WEP, WPA, WPA2) that will have been implemented.
1.6. Definition of Terms

Security protocol – the cryptographic algorithm safeguarding the transit of data across wireless networks

Wardriving – locating and logging wireless access point locations using the broadcast signal they transmit.

1.7. Chapter Summary

The main objective of this research is to assess the factors that influence the level of security implemented on Wi-Fi networks in Nairobi’s Central Business District. This chapter has introduced the various threats and risks facing unsecured Wi-Fi networks. It has stated the objectives to be followed in this research study as well as the significance of the research to the body of knowledge.
CHAPTER 2: LITERATURE REVIEW SECTION

2.1. Introduction
This chapter reviews prior research and literature that has been conducted to determine the various security protocols used on Wi-Fi networks. It shows the known security vulnerabilities associated with some of the earlier security protocols and the measures that users can take to protect themselves against these vulnerabilities.

It also identifies wardriving techniques and displays how these have been valuable to other research studies trying to gather reliable data on the state of Wi-Fi security in their various cities. This is necessary in providing valid data on the number of networks vulnerable to potential cyber-attacks.

2.2. Assess Wi-Fi Security Risks, Vulnerabilities and Mitigations
To tackle the numerous risks facing Wi-Fi networks, IEEE has over the years developed a number of security protocols. Despite their efforts however, numerous Wi-Fi networks are implemented with no security at all or using outdated security protocols with easily exploitable vulnerabilities.

A study by Klasnja et al. (2009) showed that users are generally unaware of how Wi-Fi networks work and of the limitations of any security protocols that may be in use. Results from their study showed that users knew little of the broadcast nature of Wi-Fi and the role of SSL in encrypting their data. Only four of eleven participants understood that sending unencrypted information in an open network was visible to other devices on the same network.

The same study showed that, rather than choose a Wi-Fi network based on security measures implemented; users will more often consider the network signal and reliability before deciding which network to connect to. The more strength a signal gave off and the more reliable the Wi-Fi network, the higher its chances for a user to select it.

Both wired and wireless networks use the Open Systems Interconnection (OSI) structure to facilitate communication. This provides common threat and attack vulnerabilities that can be exploited by malicious attackers for the different layers. The physical and MAC layers are the only differences in protocol implementation between wired and wireless networks. The application, transport, and network layers are similar to wired networks,
thus similar security attacks that can be made on wired networks can also be made on wireless networks (Zou et al., 2015).

The physical layer is the lowest layer in the OSI model and is vulnerable to: (1) eavesdropping (2) jamming.

Eavesdropping is made possible due to the broadcast nature of wireless networks. A malicious attacker within range of the network can intercept and view communications in plaintext from the source node to the destination node. To counter this problem, communications on the network are encrypted using secret keys.

Jamming is a form of attack where a node on the wireless network intentionally disrupts communication by ensuring legitimate users cannot access wireless network resources. To counter this, spread spectrum techniques are used to spread the transmit signal over a wider bandwidth than its original frequency (Zou et al., 2015).

The MAC layer is susceptible to: (1) MAC spoofing and (2) identity theft attacks. All devices communicating in a network are equipped with Network Interface Cards (NIC) where the MAC address of the device is hard coded. However, it is possible for a malicious attacker to steal the MAC address of a legitimate node on the network and use it to access the network. This is what is referred to as an identity theft attack. Users should realize that MAC filtering isn’t a very secure means of protecting the network as spoofing a MAC address can be done very easily using open source tools that automate this process for attackers.

Over the years, the IEEE 802.11 standard has had three security protocols in place to help maintain security of Wi-Fi networks: WEP, WPA, and WPA2. This section will go through the various security protocols and attempt to establish what vulnerabilities in each protocol allow for Wi-Fi network exploitation.

2.2.1. Wired Equivalent Privacy (WEP)

WEP protocol was the first IEEE 802.11 security standard to be introduced in an attempt to secure wireless networks. It consists of two parts: the encryption and authentication. It achieves access control by preventing unauthorized access to users without an appropriate WEP key. Data privacy is achieved by encrypting data stream packets separately with a
Rivest Cipher 4 (RC4) algorithm which is derived from the 64-bit RC4 key (Vilius et al., 2015).

The RC4 encryption key is composed of a 40-bit WEP key and a 24-bit Initialization Vector (IV). The WEP key is shared between clients and WAPs on the network while the IV is generated afresh for each packet encryption. The RC4 algorithm enables self-synchronization of the packets in order to prevent them from being affected by packet losses and becoming indecipherable.

In the process of encrypting, the RC4 algorithm runs a Cyclic Redundancy Check (CRC) on each plaintext resulting in a value referred to as the Integrity Check Value (ICV). The ICV is then added to the corresponding text. The pre-shared 40-bit secret key is combined to the randomized 24-bit IV to produce a 64-bit seed referred to as the Pseudo-Random Number Generator (PRNG). The PRNG generates a random number, which is then developed into a keystream. The keystream and the ICV are processed with Exclusive OR (XOR) operation, to derive the ciphertext. Finally, the IV is combined to the resulted cypher text for transmission (Vilius et al., 2015).

Figure 2.2.1.1 displays the summary of the WEP encryption process.

![Diagram](image.png)

**Figure 2.2.1.1: Summary of the WEP encryption process (Poddar, 2014)**

WEP was designed to have similar security strengths as its wired counterpart, however the encryption part of the protocol proved to be relatively weak. Growth of wireless LAN adoption attracted malicious attackers who learned that obtaining the WEP key was easy.
Vulnerabilities that were identified in WEP include the fact that the Initialization Vector is unencrypted which can easily be captured in the air together with its keystream. Combining the two will reveal the 40-bit encryption key. Armed with this, malicious attackers are able to intercept traffic going through a WEP protected Wi-Fi network and retrieve all the data and information (Vilius et al., 2015).

WEP fails to protect the information against forgery and replay attacks, hence an attacker may be capable of intentionally either modifying or replaying the data packets without the legitimate users becoming aware that data falsification and/or replay has taken place. Additionally, it is easy for an attacker to forge an authentication message in WEP, which makes it straightforward for unauthorized users to pretend to be legitimate users and hence to steal confidential information (Zou et al., 2015). To remedy these vulnerabilities, WPA was introduced as an alternative in 2007.

2.2.2. WPA (Wi-Fi Protected Access)

Wi-Fi Protected Access (WPA) is a combination of Temporal Key Integrity Protocol (TKIP) and Advanced Encryption Standard (AES) encryption algorithm. Initially, WEP devices could not support AES encryption but with the development of WPA-TKIP, WEP vulnerabilities were patched by incorporating AES features in later manufactured WEP devices. WPA encryption was temporarily able to overcome the vulnerabilities of WEP, by introducing TKIP and Message Integrity Check (MIC) (Vilius et al., 2015).

The WPA standard has two main types:

1) Personal WPA, which is also known as WPA Pre-Shared Key (WPA-PSK). It is used is mainly in households where employment of an authentication server is impractical. The secret key is shared between the client device and WAP.

2) Enterprise WPA is used for enterprise networks, which require an 802.1x authentication server to carry out the security control that effectively guards against malicious attacks (Zou et al., 2015).

The main advantage of WPA over WEP is that WPA employs more powerful data encryption referred to as Temporal Key Integrity Protocol (TKIP), which is assisted by a
Message Integrity Check (MIC) invoked for the sake of protecting data integrity and confidentiality of Wi-Fi networks.

The TKIP protocol utilizes two separate keys to encrypt wireless traffic: first the 128-bit key used by the key mixing algorithm to produce an encryption key for each packet and a 64-bit MIC key used to verify the contents of the received packets for any modifications during their transportation. The advantage of this WPA-Mixed mode over WEP is that, it not only secures legacy devices with AES standard but also offers a higher-level security for newer devices with a combination of WPA-AES encryption.

Figure 2.2.2.1 displays the summary of the WPA encryption process.

![WPA Encryption Process Diagram](image)

**Figure 2.2.2.1: WPA Encryption Process (Poddar, 2014)**

With time, vulnerabilities were also discovered in this security protocol as well. The WPA-TKIP combination developed vulnerabilities against several types of network attacks such as Denial of Service (DoS) attack, which can compromise an organization’s entire network. A later modified version of the WPA-TKIP combination is WPA2, which is considered to be a more secure protocol for wireless network security (Vilius et al., 2015).

### 2.2.3. WPA Mixed Mode Encryption (WPA/WPA2)

WPA2 successfully mitigates the security weaknesses in WEP. It enforces a mixed key function composed of the secret root key along with IV, into the text before being fed to
the RC4 algorithm. This ensures the key is constantly changed, and thus reducing probabilities of IV based attacks. WPA-TKIP standard also introduced a sequence counter to secure the network against replay attacks, which ensured data integrity by dropping the packets that are not in the right sequence, and thus preventing data modification by Man-in-the Middle (MitM) attacks. By increasing the size of IV from 24 to 40, and setting up the TKIP keys with a finite lifetime, and by forcing keys to renew more frequently, the likelihood of key recovery was greatly reduced in WPA2, which significantly reduces the possibility of both capturing the IVs and revealing the encryption key (Vilius et al., 2015).

Figure 2.2.3.1 displays the summary of the WPA2 encryption process

![Figure 2.2.3.1: WPA2 Encryption Process (Vilius et al., 2015)](image)

However, Wi-Fi has been identified as a security concern when WPA-TKIP encryption is used. This is because it no longer provides adequate security for personal and enterprise networks. Though modified, relationships can still be identified between WPA-TKIP and WEP, making it susceptible to similar types of attacks. As an effect, the Wi-Fi alliance has started to prohibit manufacturers from implementing the use of "TKIP-Only" mode on primary interfaces, and strongly discouraged the use of WPA/WPA2 mixed mode encryption on wireless devices (Vilius et al., 2015).

The types of threats and attacks that WEP, WPA and WPA2 security protocols are susceptible to are as follows:
✓ Authentication attacks – WEP is vulnerable to authentication attacks where illegitimate users may steal legitimate users’ credentials by use of either a cracked version of the shared key or use of the default WEP key.

WPA PSK is also vulnerable to this type of attack using dictionary attacks that also gives the hacker the key used to encrypt the users’ data.

✓ Denial of Service attacks – attempt to inhibit or prevent legitimate use of the wireless communication services

✓ Masquerading attacks – an attacker impersonates an authorized user and gains certain unauthorized privileges.

✓ Man-in-the-Middle attacks – the attacker intercepts the path of communications between two legitimate parties, thereby obtaining authentication credentials and data.

✓ Traffic Analysis – the attacker passively monitors transmissions to identify communication patterns and the participants involved.

✓ Physical attacks – Attacker has physical access to the device and can replace firmware or steal credential information like static keys.

To reinforce security when in public spaces, users are advised to: (1) make use of device firewalls; (2) VPNs when connecting to the access point; (3) open DNS to guard against DNS poisoning and (4) to only access websites through Secure Hypertext Transfer Protocol (HTTPS) (Raju & Nair, 2015).

Research by Zou et al. (2015) shows that implementation of WEP, WPA and WPA2 security protocols alone isn’t sufficient to protect against malicious attacks. Implementation of VPNs and firewalls should also be considered when using Wi-Fi networks.
2.3. **Identify the Current State of Security Implementations on City-Wide Wi-Fi Networks.**

Popular public hangout places, where consumers spend their leisurely time, tend to avail free public Wi-Fi to their clients. Many coffee shops, restaurants, hotels, airports, schools, salons in Kenya are some of the spaces that have implemented Wi-Fi networks.

Consumers will use these networks to conduct various activities including: online shopping, sending emails, working, social networking, online dating, photo-sharing and instant messaging. Businesses readily implement Wi-Fi networks to pull in more clientele to their businesses but they fail to look into the security implications of public Wi-Fi networks.

To estimate and locate the number of Wi-Fi networks in Nairobi’s Central Business District, a number of wardrives will be necessary. Wardriving was coined by Peter Shipley at the turn of the second millennium (Sagers, Hosack, Rowley, Twitchell, & Nagaraj, 2015). It refers to locating and logging wireless access point (WAP) locations using the broadcast signal they transmit. Prior to Shipley coinage and automating the process, wardriving was conducted manually by use of pen and paper to locate and log WAPs.

Wardriving entails driving around a targeted location picking up the Wi-Fi networks in the area and recording their GPS locations. Wardriving using specialized software can help determine the security protocols implemented on WAPs as well as the signal strength, hardware used for the WAP and known vulnerabilities associated with certain WAP implementations.

By conducting a wardrive, an attacker can easily gain knowledge of the Wi-Fi networks in a given area and proceed to gaining their security key as majority of public Wi-Fi networks openly advertise the key. In some cases, no security key is even implemented. Once a malicious attacker has access to the network, they can proceed to sniffing the network and intercepting packets of data that are broadcast into the air.

If these packets are unencrypted, the attacker can easily decipher the contents of the packets. It would thus be best if users of Wi-Fi networks limited their connections to secured networks (Sagers et al., 2015).
Users of Wi-Fi networks are vulnerable to numerous risks when connected to poorly secured public Wi-Fi networks. These include: eavesdropping, jamming, man-in-the-middle attacks, MAC spoofing, phishing attacks, network injection and identity theft. It is worth noting that users may not be aware of the security risks they are faced with and even if they are, they do not believe themselves vulnerable or the likely targets of such attacks (Harbach et al., 2014).

Numerous studies have been conducted in various cities all over the world using wardrives to allow for comparisons in the levels of Wi-Fi encryption adopted over the years.

To hack a Wi-Fi network, an intruder would require relatively cheap hardware and a couple of different readily available software tools and techniques. Some of the more popular techniques include use of: sniffers which intercept, monitor and log traffic on networks; brute force and dictionary attacks; and war driving which involves driving around in a motor vehicle searching for a Wi-Fi network using a mobile smart phone, laptop or tablet.

Various wardrive studies have been conducted using popular software tools in the open source platform. The results they display show that a determined malicious attacker could easily obtain damaging information about an individual no matter their social or financial ranking.

One such city is Auckland where the first wardrive study was carried out in the city’s Central Business District in 2003 (Sathu & Sarrafzadeh, 2015). Similar efforts were conducted in 2015 to study changes in securing Wi-Fi networks as well as user awareness levels to security challenges of Wi-Fi networks. The study compared results from 2003 to assess the increase in the number of public wireless access points, encryption type used and whether or not SSIDs were broadcast.

The researchers ensured that they followed the same routes as the initial wardrive conducted in 2003 so as to have results they could reliably draw comparisons from. The tools used include Acrylic Pro and WiGLE Wi-Fi. Acrylic Pro was chosen for use on a laptop as it allowed the researchers to find various access points and the corresponding devices connected to them. It also provided information on security mechanisms, SSID, signal level, passwords, channel in use and its compatibility to various Wi-Fi network standards.
Sathu & Sarrafzadeh (2015) categorized their findings according to the vendors of the WAPs discovered, the network types implemented (either ad-hoc or infrastructure), encryption type used and the SSID setting on WAPs. New vendors, Huawei and Ubiquiti, were found to have taken over large portions of the market that were held before by D-Link and Lucent.

Use of ad-hoc mode of Wi-Fi networks was found to have greatly reduced by 2015. Only 3% of the networks population implemented ad-hoc networks as compared to 97% of the ad-hoc market usage in 2003. Ad-hoc networks are more susceptible to compromise by malicious attackers as compared to infrastructure setups. The significant reduction was interpreted to mean that users of Wi-Fi networks in Auckland’s CBD had an increase in the level of security awareness when compared to 2003.

In terms of Wi-Fi encryption, Auckland’s entire CBD population was found to be implementing Wi-Fi security protocols in one form or another. Less than 3% implemented WPA, whereas at least 26% percent of the population used WEP encryption. This left the greater population of seventy percent using the more preferable and reliable form of Wi-Fi security – WPA2.

In the UAE, wireless security implementations were assessed in 2010 and 2008 in the cities of Abu Dhabi, Dubai and Sharjah. The 2008 study found a total of 15,000 access points compared to 12,000 in 2010. There was a recorded 5% increase in the use of WPA and WEP as well as a 10% decrease in the number of unencrypted access points (Aloul, 2010). The continued use of weak encryption standards was interpreted by the researchers as a lack of wireless security awareness amongst users.

Two studies conducted in the UK in 2007 used NetStumbler, a wireless security software package that can be used to identify access points and a Toshiba laptop with an inbuilt wireless adapter for their wardriving purposes. Two research groups CAIR and ISRNG carried out separate independent studies around the areas of the University of Plymouth and the North Eastern part of the University of Wales respectively (Cunningham & Grout, 2009).

The CAIR conducted their first study in a sixteen-kilometer square radius with a population of sixty thousand residents. The second study was conducted eight months after the first covering a four-kilometer square radius with a population of 15,600 residents. The first study recorded 1,153 access points while the second study recorded
1,113 APs. The difference in size of the areas covered and the WAPs discovered indicated an increase in the uptake of wireless networking in the community. The researchers also assumed an increase in the level of users’ awareness on Wi-Fi security as many WAPs had WEP implemented on them.

The NetStumbler software used to discover WAPs could only discover WEP as the security protocol implemented thus the study could not give results for other security implementations. To correct this, the researchers issued a questionnaire to some of the residents in the sampled area and discovered approximately 70% used Wi-Fi for personal reasons and 30% for both personal and work purposes. Approximately 70% had changed their default SSID, 20% had not and 10% of users did not know.

Responses regarding the Wi-Fi encryption protocols used showed that users implemented WEP, WPA, implemented access control filtering using either MAC filtering or IP addresses and even hid the SSID of the WAP as well as changing default passwords. The ISRN group conducted four different surveys over a four-year period that showed similar results. The evolution of security features on wireless networks had taken an upward trend. However, the 2006 survey showed a worrying trend where 26 WAPs used the house number and street address as the SSID. This would provide potential attackers additional information when eavesdropping allowing for better associations with personal information intercepted.

Another study in the city of Derby in the UK was conducted to reveal the security trends implemented on Wi-Fi networks and compare their efficiencies against current vulnerabilities. A similar study had been conducted in 2006 thus a comparative analysis of Wi-Fi security trends is done (Vilius et al., 2015).

The study used an open source Raspberry Pi platform and Kismet for its software. It also paired an external ALFA AWUS036NHA Wi-Fi antenna to collect Wi-Fi broadcast signals since Raspberry Pis do not have an inbuilt wireless card. To validate the accuracy of the data collected, three separate wardrives are conducted at different times and under different weather conditions.

Significant differences are recorded among the wardrives with a 59% difference recorded for the number of WAPs discovered between wardrive one and two. This is however chalked down to signal attenuation since wardrive one is conducted on a rainy Sunday afternoon. Signal attenuation leads to an increase in packet loss and decreased Received
Signal Strength Indicator (RSSI) on the 802.11 2.4 GHz wireless network (Anastasi, Falchi, Passarella, Conti, & Gregori, 2004). During heavy rainfall, 90% of the packets can be received at 5 meters and only 20% of the packets are received at a distance of 20 meters.

The second wardrive recorded lesser WAPs than the third due to the travel speeds the researchers had to use. The wardrive encountered busy traffic thus limiting the time necessary for the wardriver to connect to the AP. Research by Tsui, Lin, Chen, Huang, & Chu (2010) found that warwalking to be a more accurate means of logging WAPs as it provides more accurate results when compared to wardriving.

An analysis by Vilius et al. (2015), of the encryption standards used for the area surveyed in Derby, showed that majority of APs used WPA-Mixed Mode while WEP was the least used standard. Comparisons with studies from the year 2006 show that WEP implementation had experienced a steady decline with the rise of WPA/WPA2 implementations. In New Zealand, a study is conducted by Nisbet (2012) in the four major cities’ Central Business Districts in 2011. These include Auckland, Wellington, Dunedin and Christchurch. A prior study had been conducted for the cities of Auckland and Wellington in 2004 hence those results were used to compare the growth in wireless networks. The purpose of the study was to find out the number of Wi-Fi networks and the security settings implemented on the WAPs.

The above studies show that the researcher needs to be aware of the speeds they use when conducting a wardrive. High speeds could result in lesser WAPs being logged.

Several studies have attempted to explain why some users implement Wi-Fi security measures while others do not. Sagers et al. (2015) proposed to show that socio-economic factors determine whether wireless security is used in Wi-Fi networks. The study involved collecting data on WAPs by conducting wardrives and using results from the last census to extract variables of interest to the study. These included the income, age, education level, race and workforce type from the census and ESSID, BSSID, MAC address of the WAP, channel on which the WAP was operating, encryption type used and GPS location for the wardrive data.

GPS location of WAPs was correlated to information from the last census using ArcGIS. Results point out that some socio-economic factors do in fact inform us on the adoption of wireless security. Census block groups with higher levels of education used encryption on WAPs however, influence was not that significant. This was in line with other research which showed groups with higher levels of education accessing computers and internet services more often than others.

Census blocks with a higher white population – which were more likely to have higher mean income, elevated levels of education and age groups – also implemented security encryption on their WAPs. Age and income were found to not be reliable statistical predictors of security usage in the population.

A study by Harbach et al. (2014) involved an online survey by use of a questionnaire aimed at testing WLAN risk and consequence awareness of users. The questionnaire was structured to ask users of what risks they were aware of in certain scenarios while using the internet. The scenarios included using the Internet in general, users logging in to their social network accounts, shopping online, online banking, and finding a shared ride using online services.

After stating risks identified for different scenarios, participants of the study were asked to rate the risks on a scale of 0 – 100 as well as common sources they last heard reference of these risks from. They were also asked to state perceived potential consequences for each scenario in order of severity. The questionnaire concludes with a block set of 22 common risks users are frequently warned about. The users’ task was to show which risks
they had knowledge of and show their relevance on a scale of “not relevant at all” to “very relevant”.

Results of the study showed that users were aware of risks but gave incorrect consequences for the risks identified. This led to the hypothesis that participants did not evaluate which risks had tangible consequences leading to them underestimating the impact of the risks on themselves (Harbach et al., 2014). Many of the consequences identified involved losing money, causing damage to health and inconveniences arising from risks.

Ratings of low likelihood indicated that users viewed the risks and consequences named as never applying to them. This may lead to a carefree attitude while using the internet despite users of the network being aware of the risks and consequences posed to them. Open ended questions were analyzed through coding. Results showed that many non-financial consequences were phrased in an impersonal. This led to researchers hypothesizing that impersonal consequences caused some risks to be ignores as they were not perceived as applying to them. It would also be a waste of resources for users to bother protecting themselves against these risks as no benefits could be perceived from engaging in this action.

Interestingly, the survey conducted showed very few users viewed risks and consequences as arising from their own mistakes or negligence. Leaving their accounts logged into and use of weak passwords are some of the ways users propagate risks by being negligent. The hypothesis drawn from this was that users are unaware of the risks arising from their own mistakes, or that they were not considered important enough to be relevant. It may also be that users were simply just not aware that they were doing these and other security relevant activities wrong.

Research by Howe, Ray, Roberts, & Urbanska (2012), showed participants of their study believed that only wealthy and “important” people could be attacked. One participant stated they did not make over $40,000 in a year thus could not possibly be the target of any attack. Others stated they had nothing important enough stored on their computers to warrant an attack on their machines.

Harbach et al. (2014) study shows that users will not acknowledge the existence of risks when they believe themselves capable of dealing with the threat. Some users who were
aware of risks also cited budget constraints as reasons for not implementing security measures.

Age may also play a significant role in perception of risks to the user. In a study that included both college aged and older adults, the researchers found that older adults tended to perceive a lower risk from a threat involving loss of data confidentiality than college aged adults (Howe et al., 2012).

The logical assumption to help curb against Wi-Fi insecurity would be that users who were aware of the risks posed to them would be more likely to take security measures to protect against them. However, research shows that despite users being aware of the risks of WLANs, they take little action in the way of protecting themselves.

Other studies have adopted theoretical frameworks to explain user behavior in the adoption of security measures.

One such framework is the Protection Motivation Theory (PMT). It has been widely used to examine adoption of security measures in Information Security (IS) literature. It can explain security behavior outside of a corporate setting providing a theoretical explanation as to why people perform certain countermeasures to detect and prevent threats, which ultimately result in deterring continued attacks (Crossler, 2010).

The theory posits that individuals go through two cognitive processes: threat appraisal and coping appraisal. Threat appraisal is the process where individuals gauge the probability of a threat occurring and the likelihood to experience those threats. Coping appraisal is the process where individuals assess the effectiveness of the proposed coping mechanism in dealing with the threat (Rogers & Maddux, 1983).

A study by Woon et al. (2005) used the Protection Motivation Theory to assess the factors influencing home wireless network users’ decision to adopt security. Their findings support the use of PMT in explaining users’ intention to adopt protective measures like numerous other studies in the field of IS.

This research project will conduct a survey to help determine the factors that contribute to implementation of Wi-Fi security in Nairobi’s CBD.
2.5 Research Approach

To determine the level of security implemented on Wi-Fi networks, various studies have conducted city wide wardrives. This has resulted in the discovery of the types of security protocols in place as well as the overall number of existing Wi-Fi networks. Studies have also shown conducting more than one wardrive helps to validate the number of APs recorded.

There are three security protocols used to secure Wi-Fi networks released by the IEEE. These include WEP, WPA and WPA2. Vulnerabilities exploiting existing loopholes have been found for both WEP and WPA protocols. As a consequence, the most secure protocol is WPA2. Users are also advised to incorporate extra layers of security such as use of VPNs, https and firewalls to mitigate security risks.

In Nairobi, wardrive research by Gameli (2016) was conducted around the numerous industrial and residential areas. It however did not include the Central Business District. As a result, this study’s scope concentrates on Nairobi’s CBD to extend the study conducted by Gameli in 2016.

To assess users’ security behavior the Protection Motivation Theory has been successfully used in several information security studies. Data collected from users is analyzed using the PLS-SEM algorithm which has been found to be appropriate for exploratory model building studies.

A Wi-Fi security comparative study in Europe by Osorio (2008) found France to be the most secure country in the employment security mechanisms. This was determined to be as a result of the stringent rules employed by their ISPs when issuing Wi-Fi services. Vendor support and pressure are factors that will also be examined in this study to determine the influence they have over Wi-Fi security implementations.

Ethical considerations taken into account in the various research studies include the criminal nature of accessing people’s data without their consent. Wardrives are conducted rather than hacking demonstrations to show the vulnerabilities in Wi-Fi networks.

This study will follow the above research approaches to guide how this project will be conducted. A number of wardrives in Nairobi’s CBD will be carried out to determine the number of Wi-Fi networks in place as well as the security protocols used. Following this,
the PMT will be used to determine the motivation for employing the chosen security mechanism on different access points.

2.6. Chapter Summary

This chapter discusses the various threats and vulnerabilities likely to be exploited on wireless networks by wireless hackers or attackers in an attempt to gain private information or penetrate a network.

It also covered various wardriving efforts conducted in different countries to determine the uptake of Wi-Fi network security and the measures implemented to protect against cyber-security threats. Local research done by Gameli (2016), covered residential estates on the outskirts of Nairobi’s CBD. This research will bridge the gap by conducting wardrives in Nairobi’s Central Business District to determine the security implemented on Wi-Fi networks.
CHAPTER 3: METHODOLOGY

3.1. Introduction
This chapter describes the descriptive and survey research design methods used in this study. The population and sample size are defined from the wardrive tests conducted to determine the number of Wi-Fi networks in Nairobi’s CBD. The various tools and methods used to collect data in the wardrives are defined, as well as the research and analysis procedures followed.

3.2. Research Design
The research design is defined as the scheme, outline or plan that is used to generate answers to research problems (Kombo & Tromp, 2006).

The research design used in this research study followed the descriptive design. The descriptive design defines the state of affairs as they exist. It enables the researcher to report findings which may result in formulation of important principles of knowledge and solutions to significant problems (Kombo & Tromp, 2006).

For this study, two wardrives were conducted in an attempt to capture the Wi-Fi networks in use in Nairobi’s Central Business District. This was important as it enabled the mapping out of how Wi-Fi networks have been secured. An average total of 1,816 wireless access points were mapped out from the two wardrives conducted in November 2016 on two separate days.

Next, the researcher distributed questionnaires to the owners of the discovered WAPs. By following a convenience sampling design a total of sixty questionnaires were successfully distributed however, only forty-five remained viable for analysis giving a 75% response rate. Before engaging in the survey, the researcher sought consent from users of the Wi-Fi network then distributed questionnaires alongside a letter that assured the participants of their anonymity.
3.3. Population and Sampling Design

3.3.1. Population

The population targeted for this research was obtained from the results of the wardrives conducted in Nairobi’s Central Business District. Targeted locations included the numerous popular eating, drinking joints and businesses offering free public Wi-Fi to its customers.

The average population result from the two wardrives conducted was 1816 Wireless Access Points (WAPs).

3.3.2. Sampling Design

The sampling technique used for this research was convenience sampling. This method allowed for the selection of Wi-Fi networks whose SSIDs correlated to the names of the business or one that the researcher immediately identified. This helped ensure that the researcher did not waste too much time trying to identify the precise location of Wi-Fi networks. From this design, the resulting sample size that was measured was 45 identifiable and accessible wireless access points.

These were located on the following streets: Moi Avenue, Mama Ngina Street, Kimathi Street and Kaunda Street.

The best sampling method for the large data set would have been simple random sampling however, once in the field, convenience sampling was discovered to be more suitable. This was because a large number of the WAPs had SSIDs that made it difficult to locate and identify them precisely. It required the WAPs’ exact location so as to hand out the questionnaires to the owner or managers of the Wi-Fi network.

It should however be noted that a hacker only needs the WAP’s signal to intercept the network and not its specific location. With the aid of external Wi-Fi antennas that gain the attacker more signal strength proximity to the WAP becomes unnecessary. The only chance users of that network stand is ensuring the Wi-Fi network is properly secured.
### 3.4. Data Collection Methods

The methods used in this research study were structured observation for the wardrive and survey questionnaires which allowed for the testing of research hypotheses.

With reference to wardriving, Shankdhar (2015) annotates the following tools that are used to sniff and exploit wireless network vulnerabilities:

**Table 3.4.1: Summary of various Wardriving Tools**

<table>
<thead>
<tr>
<th>Name</th>
<th>Features</th>
<th>Platform</th>
<th>Selected for this research</th>
</tr>
</thead>
</table>
| Kismet      | A sniffer & Intrusion Detection System (IDS) that:  
- Passively collects packets to identify & detect hidden networks.  
- Logs wireless access points’ location, BSSID, SSID, channel it operates on, number of clients connected to the WAPs and the Wi-Fi security encryption type used on the WAP. | Linux, OSX, Windows BSD | Yes. Among the sniffer tools listed below Kismet provided the most relevant data to this research. |
| Reaver      | - Designed to attack Wi-Fi networks that have WPS implementations.  
- Can be used to regain WPA/WPA2 passphrases in a matter of hours.                                                                                                                                      | Kali Linux | No. This research did not engage in active attacks.                                         |
| NetStumbler | Used for:  
- wardriving,  
- verifying network configurations,  
- finding locations with poor network,  
- detecting unauthorized access points &  
- detecting other networks causing interference                                                                                                                                                    | Windows  | No. This tool is easily detected by most wireless intrusion detection systems available and does not work properly with the latest 64 bit Windows OS. |
| Network Miner | A network forensic analysis tool that can be used to analyze packets transmitted on the network to detect:  
- operating system in use,  
- active sessions  
- host device’s name & - number of open ports on the network. It extracts:  
- files transmitted on the network.  
- user credentials such as usernames and passwords (Hjelmvik, 2017)                                                                                                         | Windows, Linux, OSX, Free BSD | No. This tool collects data about hosts on the network rather than collecting data regarding traffic on the network |
| Wellenreiter | A wireless network discovery and auditing tool that can:  
- Scan & detect WAPs, ad-hoc cards  
- determine SSID broadcasting, the manufacturer and use of WEP on the network  
- decode and display DHCP & ARP traffic                                                                                                           | Linux     | No. This tool limits audit to Wi-Fi 802.11b channels.                                        |
<table>
<thead>
<tr>
<th>Tool</th>
<th>Description</th>
<th>Platform(s)</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>CommView</td>
<td>-A monitor and packet analyzer tool that captures every packet and displays access points, stations, signal strength, network connections and protocol distribution. Captured packets can be decrypted by user-defined WEP or WPA keys.</td>
<td>Windows</td>
<td>No. Majority of the tools the researcher worked with were only compatible in the Linux environment.</td>
</tr>
<tr>
<td>OmniPeek</td>
<td>A packet sniffer and network analyzer tool used to capture and analyze wireless traffic.</td>
<td>Windows</td>
<td>No. The tool is commercial and can only be used in an Windows environment.</td>
</tr>
<tr>
<td>inSSIDer</td>
<td>Can find open Wi-Fi access points, track signal strength, and save logs with GPS records.</td>
<td>Windows OS X</td>
<td>No. The tool is commercial, retailing at $19.99.</td>
</tr>
<tr>
<td>Cain &amp; Abel</td>
<td>A password recovery tool that can: -recover passwords by sniffing the network, -crack encrypted passwords using Dictionary, Brute-Force and Cryptanalysis attacks; -record VoIP conversations; -decode scrambled passwords; -recover wireless network keys; -reveal password boxes; -uncover cached passwords &amp; -analyze routing protocols (Fahmy, Nasir, &amp; Shamsuddin, 2012)</td>
<td>Windows</td>
<td>No. Despite the numerous useful features on Cain &amp; Abel, the research was limited to passive discovery of Wi-Fi networks.</td>
</tr>
<tr>
<td>Wireshark</td>
<td>A network protocol analyzer that captures and interactively browses the traffic running on a computer network. Features: -deep inspection of hundreds of protocols; -live capture and offline analysis &amp; -decryption support for IPsec, ISAKMP, Kerberos, SNMPv3, SSL/TLS, WEP, and WPA, WPA2</td>
<td>Windows Linux MacOS Solaris FreeBSD NetBSD</td>
<td>No. Wireshark would not serve the purpose of a wardrive</td>
</tr>
</tbody>
</table>

In this research, Kali Linux was used as the host device’s primary operating system. The tool that accumulates the most relevant data to the research in Kali Linux is Kismet. Kismet enables the researcher to gain the wireless access points’ location, BSSID, SSID, channel it operates on, number of clients connected to the WAPs and the Wi-Fi security encryption type used on the WAP.

Kismet requires the use of a GPS device to map WAP locations. By using, BlueNMEA – an android application – a mobile device reads as a GPS device in Kismet enabling the transfer of GPS coordinates via Bluetooth.
GisKismet is also used to extract the required data from Kismet to help create wireless reconnaissance maps that can be viewed on Google Maps.

Survey questionnaires are also distributed to locations where the WAPs discovered on the wardrive were accessible.

The data collected shows the extent to which Wi-Fi networks have been deployed, which security measures have been included on them and analyze the relationship between user awareness and the measures taken to secure these networks using the Protection motivation Theory (PMT).

3.5. Research Procedures

3.5.1. Wardriving

The hardware and software tools that were used to setup and run this research were:

✓ Laptop
✓ GPS capable Android device.
✓ An External Wireless Card Antenna
✓ Kali Linux Environment
✓ Kismet
✓ GisKismet
✓ BlueNMEA
✓ Google Maps

To get started, a small laptop was setup with the Kali Linux environment. Kali was the operating system of choice because it was specifically created for penetration testing, ethical hacking and network security assessments.

The laptop of choice was a Samsung Notebook N100SP. The laptop was chosen due to its lightweight and easily concealable nature.

With the Linux environment in place, the tools specifically to be used for the wardrives were setup next. Kismet was the tool of choice for this task. It runs from the command line but has several advantages over other wireless network assessment tools. These include: collecting information on the devices attached to the WAP at the time of the scan, the devices’ IP addresses and IP range, it can identify cloaked networks i.e. those not broadcasting their SSID and can collect manufacturer’s information on the wireless access point’s router by resolving the IP address associated with it.
The above features are invaluable for a hacker as they provide numerous ways for breaching access and collecting information on the network. A hacker can gain access to networks that filter devices using MAC address by spoofing an IP address of one of the client devices associated with the network. The encryption type associated with the network lets the hacker know which tools they may require to capture and decrypt data packets as they are sent across the network. The manufacturer information collected on the various Wi-Fi access points could lead a hacker to find out the known vulnerabilities associated with those WAPs that they could exploit.

![Image of Kismet startup page](image.png)

**Figure 3.5.1: A display of the Kismet startup page**

For this study the most relevant information required from kismet is the location, encryption type and SSID of the WAPs in Nairobi’s CBD.

To run kismet, one has to open terminal and type in kismet. The Kismet console window will pop up alerting you that it is running as root as shown in figure 3.5.1. In Linux, running any program as root is a task that should be taken on cautiously as it is possible to easily corrupt your system by mishandling or misinterpreting code working at the command line. However, we need kismet to run as root as this is the only way to set up the wireless card in monitor mode for it to capture packets.
Monitor mode (rfmon) essentially means that we are dissociating the network interface from normal use and setting it up to only monitor and capture packets on the 802.11 layer. It is generally impossible to remain associated to a wireless network while running Kismet on that same interface.

Therefore, the next steps will be to start up the Kismet server, define the wireless interface that will be capturing packet sources and set up the GPS device that will tie the WAP location to the data Kismet captures as shown in figure 3.5.2 and figure 3.5.3.

![Capture of the Kismet Server Startup options](image)

**Figure 3.5.2: Capture of the Kismet Server Startup options**

![Adding wireless interface capture source](image)

**Figure 3.5.3: Adding wireless interface capture source**
To aid in the capturing of packets, an external wireless card with a directional antenna was added. The ALFA AWUS036NHA is one of the most reliable, highly recommended wardriving tools and costs slightly more than $30. Kismet automatically detects the device type and channels supported by the wireless card. The Alfa card is displayed in figure 3.5.4.

![ALFA AWUS036NHA](image)

**Figure 3.5.4: An external wireless card – ALFA AWUS036NHA**

At this point, Kismet is running and collecting wireless packets but it is not recording any GPS data as no GPS receiver is connected yet as shown in figure 3.5.5.

![Kismet running with no GPS data](image)

**Figure 3.5.5: Kismet running with no GPS data**

Rather than purchase a GPS receiver, an alternative an android application known as BlueNMEA was chosen instead. BlueNMEA sends the phones’ location data via
Bluetooth (RFCOMM) or TCP in the National Marine Electronics Association (NMEA) format to the device it is connected to. This is displayed in figure 3.5.8.

To set it up to communicate with the laptop, Android SDK tools had to be installed on the host machine. Enabling USB debugging on the phone under developer options allowed for the phone and computer to communicate. Next, issuing an adb command to forward TCP port 4352 from the phone to the computer, figure 3.5.6 and another command to get gpsd listening on the forwarded port ‘4352’ as shown in 3.5.7 ensures the GPS location of the phone is sent to the laptop.

![Figure 3.5.6: adb Command Forwarding TCP 4352](image)

![Figure 3.5.7: gpsd Command Enabling Transfer of GPS Location Data](image)

The gpsd command is run on a separate terminal window from the one kismet is running from to allow the two processes to continue running separately as shown in figure 3.5.9.
With the success of the previous steps, wardriving then began. Log files were stored in the directory where kismet was started from. Since Kismet was started from root (Kali Linux default login settings is root), log files will be located at the root directory.

Kismet saves the following types of log files: gpsxml, .pcapdump, .nettxt, .netxml, .alert.
3.5.2. Questionnaire Survey

The second research procedure of this research aimed at distributing questionnaires to the various owners of the discovered Wi-Fi networks. This section of the research attempted to find out users’ Wi-Fi security awareness levels as well as the cognitive processes that led to their choice of Wi-Fi security (where one was in use).

This data was then analyzed to determine whether the hypotheses in this research are supported or not.

3.6. Data Analysis Methods

This research targeted businesses in Nairobi’s Central Business District that offered Wi-Fi services to its clients. The main focus was on determining the level of Wi-Fi security put in place, if any, and the motivating factors for securing the network.

Data acquired from the wardrive was exported to an SQLite database where the number of Wireless Access Points (WAPs) and security protocol used were determined. This study used the Partial Least Squares based Structural Equation Modelling (PLS-SEM) algorithm to analyze questionnaire data. More specifically, the WarpPLS v5.0 software was used. PLS-SEM was determined appropriate for this study because it is preferred for studies with small sample sizes and for predictive testing.

Analysis of data was done via two components in the SEM namely the outer/measurement model and the inner/structural model (Hair, Ringle, & Sarstedt, 2011). Data reliability and validity was examined by assessing composite reliability, inter-item loading, convergent validity as well as discriminant validity.
3.7. Ethical Considerations
Before administering questionnaires, respondents were first presented with a letter identifying the researcher and the research project. The researcher also presented her school ID to further identify herself when respondents sought further authentication.

Consent was also sought before providing the questionnaire while the accompanying letter assured respondents of their anonymity. The data provided was only to be used in collective terms during analysis. No self-identifying data has been used in the project.

3.8. Chapter Summary
This chapter presented this research study as following the descriptive design. The population for the study was determined by conducting a wardrive that determined the number of wireless access points available in Nairobi’s Central Business District as well as the level of security implemented.

The sample size was determined by means of convenience sampling which allowed administration of survey questionnaires assessing the cognitive factors that motivated the choice in Wi-Fi security measures implemented.

Data was then analyzed by use of WarpPLS which implements the partial least squares structural equation modelling algorithm. PLS-SEM is preferred for studies whose aim is exploratory model building rather than theory testing and is also implemented on studies with small sample sizes.
CHAPTER 4: MODEL

4.1. Introduction

The previous chapters have discussed literature on prior wardrive studies that have been conducted in other countries.

Local research done by Gameli (2016), covered residential estates on the outskirts of Nairobi’s CBD. This research will bridge the gap by conducting wardrives in Nairobi’s Central Business District to determine the security implemented on Wi-Fi networks. It also incorporates the Protection Motivation Theory which allows for better understanding of the cognitive factors that come into play when deciding whether to implement Wi-Fi security measures.

4.2. Analysis

This research targeted businesses in Nairobi’s Central Business District that offered Wi-Fi services to its clients. The main focus was on determining the level of Wi-Fi security put in place, if any, and the motivating factors for securing the network. The unit of analysis therefore, was the person responsible for managing the network.

The model constituted 37 items describing nine latent constructs: Perceived Vulnerability, Perceived Severity, Rewards, Response Efficacy, Self-Efficacy, Response Cost, Vendor Support, Pressures and Behavioral Intention. The seven independent variables and dependent variable behavioral intention measure values from a person’s response about themselves whilst the dependent variable observed security is a report on the actual behavior as recorded by the researcher.

The Partial Least Squares based Structural Equation Modelling (PLS-SEM) algorithm was favorably selected for analysis in this study because it is better suited for exploratory model building as well as studies with smaller sample sizes. Several studies (Crossler, 2010; Johnston & Warkentin, 2010; Lee & Larsen, 2009; Matt & Peckelsen, 2016; Salleh, Hussein, Mohamed, & Aditiawarman, 2013; Tu & Yuan, 2011) implementing the Protection Motion Theory model analyzed their data using PLS-SEM.

The quality and fit of the model are measured using ten global indices (Kock, 2015b):

i) Average Path Co-efficient (APC)

ii) Average R-Squared (ARS),
iii) Average Variance Inflation Factor (AVIF),
iv) Average Adjusted R-Squared(AARS),
v) Average Full Collinearity VIF (AFVIF),
vi) Tenenhaus GoF (GoF),
vii) Sympson’s Paradox Ratio (SPR),
viii) R-Squared Contribution Ratio (RSCR),
ix) Statistical Suppression Ratio (SSR), and
x) Non-Linear Bivariate Causality Direction Ratio (NLBCDR).

Analysis of data is done via two components in the SEM namely the outer/ measurement model and the inner/ structural model (Joe F. Hair et al., 2011).

4.2.1. Measurement Model Analysis

The reliability of reflective instruments is assessed by measuring individual item reliability and composite reliability, whereas the validity is measured using convergent validity as well as discriminant validity.

Construct reliability assessment characteristically focuses on composite reliability as an estimate of a construct’s internal consistency. It is recommended that values be 0.70 or greater to be acceptable (Latan & Ramli, 2013). Each indicator’s reliability is also taken into account and should be above 0.70. However, removal of indicators can affect the construct validity therefore, only indicator lower than 0.40 should be removed (Joe F. Hair et al., 2011).

Convergent validity is examined using the Average Variance Extracted. An AVE of 0.5 or higher is expected as it shows that a latent variable explains more than half of its indicator’s variance. The combined loadings and cross-loadings table is also used to analyze convergent validity. Indicators should exhibit high loadings on their own constructs, and no items should load higher on constructs they were not intended to measure (Lee & Larsen, 2009).

Discriminant validity examines the amount of variance a latent variable shares with its assigned indicators compared to other latent variables in the structural model. The AVE of each latent construct should be greater than the latent construct’s highest squared correlation with any other latent construct (Joe F. Hair et al., 2011).
Tests for multicollinearity are also performed where Variance Inflation Factors (VIFs) lower than 3.3 suggest no multicollinearity (Hair et al., 2010). Multicollinearity tests for common method bias.

4.2.2. Structural Model Analysis

With the reliability and validity of the measurement model confirmed, analysis of the structural model then follows.

Testing of the structural model involves estimation of the path coefficients and their respective P values, $R^2$ and $Q^2$. Path coefficients can be interpreted as standardized betas which calculate the strength between the dependent and independent variables. $R^2$ examines the amount of variance explained in the dependent variable by the independent variables. $Q^2$ reports the predictive relevance of a latent variable to the independent variable. Predictive relevance is accepted when the Q-squared value is greater than zero.

Effect sizes are also analyzed to establish whether the effects indicated by path coefficients (P-value) are small, medium or large (Kock, 2015b). It is generally accepted that 0.02 constitutes a small effect size, 0.15 moderate effect size and 0.35 a large effect size. Similarly, 0.02 represents weak predictive relevance in $Q^2$, 0.15 moderate predictive relevance and 0.35 strong predictive relevance (Latan & Ramli, 2013).

4.3. Modelling

There are various models that have been used to explain behavior and attitudes toward Information Security (IS) among individuals.

The Rational Choice Theory (RCT) offers a theoretical explanation as to how individuals make choices when faced with choices. It argues that individuals weigh costs and benefits of their options before making a decision (Bulgureu, Cavusoglu, & Benbasat, 2010). This theory was not chosen for this research due to the criticism researchers have given. The main criticism against it is that individuals have personal preferences thus; choices made after weighing benefits and costs cannot be applied to the general population as every individual will make decisions based on their own preferences (McCarthy, 2002).

The Theory of Reason Action (TRA) examines the importance of attitude and subjective norm in predicting behavioral intention. Attitude stems from individual perceptions.
whereas subjective norm stems from an individual’s perception of important people around them (Gundu & Flowerday, 2012).

The Theory of Planned Behavior (TPB) extends the Theory of Reasoned Action and states that the intention to perform certain behavior can be predicted by examining attitudes. Behavior is measured against behavioral beliefs, normative beliefs and self-efficacy (Bulgurcu et al., 2010).

The General Deterrence Theory (GDT) borrowed from the criminal justice domain measures individuals’ adoption of Information Security (IS) by increasing the certainty and severity of punishment where IS is not implemented (Crossler, 2010).

GDT, TRA, and TPB were not chosen for this research for various reasons. GDT is limited for use in corporate settings whereas TRA and TPB assume prior knowledge of the subject matter being examined. RCT did not include enough measurement variables for the researcher to examine in the current study. The Protection Motivation Theory (PMT) includes measurement constructs relevant to this study.

Protection Motivation Theory is a predictive model that helps assess user’s intention to adopt protective measures after a fear appeal has been expressed to the user. It was formulated in 1975 by Ronald W. Rogers and later enhanced in (Rogers & Maddux, 1983). It postulates that the use of fear appeals can directly affect behavioral change to a recommended adaptive behavior.

To motivate users to consider security implementations, one has to consider that negative consequences are the only kind of punishment a user has to fear outside a corporate setting where policies are otherwise enforced on users (Harbach et al., 2014).

A fear appeal can simply be described as a “persuasive message designed to scare people by describing the terrible things that will happen to them if they do not do what the message recommends (Witte, 1992). A well formulated fear appeal will contain statements designed to communicate the severity of the threat and its probability of occurrence. It will also recommend an appropriate coping response to avert the threat specifically highlighting the value of the recommended coping response (Johnston & Warkentin, 2010).
As such, the two main components framing the protection motivation theory are threat appraisal and coping appraisal. When individuals are exposed to a fear appeal, they will engage in the threat appraisal process followed up with the coping appraisal process.

Threat appraisal is the process of assessing the amount of a danger a threat poses to an individual. It consists of:

I. *Perceived vulnerability* which refers to “an individual’s perception of the likelihood to experience a harmful situation when engaging in risky behavior” (Salleh et al., 2013). If the individual’s perceived vulnerability is high they are more likely to engage in the coping appraisal process.

II. *Perceived severity* which refers to an individual’s perception of how huge the impact of a threat will have on them after the threat has occurred. If the threat is significant enough to the individual, they are likelier to engage in the coping appraisal process.

III. *Rewards* refer to the extrinsic or intrinsic rewards that could motivate the individual to engage in adaptive behavior.

The PMT framework was chosen for this study as it has been applied to other researches seeking to understand and predict a wide array of protective actions. It has been used in numerous information security research papers to identify factors affecting mobile users’ antivirus software adoption (Al-ghaith, 2016); intent to adopt anti-spyware software (Chenoweth, Minch, & Gattiker, 2009); Matt & Peckelsen (2016) used it to explain individual’s intention to use privacy-enhancing technologies; Crossler (2010) to understand the determinants to backing up personal data; Lee & Larsen (2009) in adoption of anti-malware; Johnston & Warkentin (2010) to investigate the influence of fear appeals on the compliance of information security policies by end users; Salleh et al. (2013) used it to determine the factors influencing information disclosure on social networking sites; Tu & Yuan (2011) used it to understand the behavior in coping with security threat of mobile device theft and loss while Woon et al. (2005) used it to understand the decision variables influencing home wireless network users to implement security.
In this research, the recommended behavior is to have Wi-Fi networks with enabled security protocols of WPA2 at the very minimum. Having no security protocol or WEP enabled are considered maladaptive behavior.

The coping appraisal is the process where an individual determines their ability to cope with and avoid the potential loss or damage resulting from a threat at a perceived cost that is not too high (Crossler, 2010). It consists of:

I. *Response Efficacy* where an individual assesses the recommended behavior as being adequate to protect against the threat appraised. If the individual determines the recommended behavior as being appropriate, they are likelier to adopt the recommended behavior. In this study, that would be enabling security on their Wi-Fi network.

II. *Self-Efficacy* where an individual assesses their skills to be able to perform the recommended behavior by themselves.

III. *Response Cost* – the costs perceived by an individual in performing a recommended coping behavior and may include monetary expense, inconvenience, difficulty, and the side effects of performing the coping behavior (Woon et al., 2005).

A study by Klasnja et al. (2009) showed that users are generally unaware of how Wi-Fi networks work and of the limitations of any security protocols that may be in use. Results from their study showed that users knew little of the broadcast nature of Wi-Fi and the role of SSL in encrypting their data. Only four of eleven participants understood that sending unencrypted information in an open network was visible to other devices on the same network.

The same study showed rather than choose a Wi-Fi network based on security measures implemented, users will more often consider the network signal and propagation before deciding which network to connect to. The more strength a signal gave off and the more reliable the Wi-Fi network, the higher its chances for a user to select it.
4.3.1. Conceptual Model
Fig 4.3.1 depicts the structural and measurement model used in this study. Hypotheses 1-8 are the constructs used to measure the intention of users to implement Wi-Fi security. Hypothesis 9 measures the intention to secure Wi-Fi security against the security observed by the researcher in the wardrives conducted.

Figure 4.3.1: Conceptual Model of the Protection Motivation Theory
Harbach et al. (2014) conducted a study that showed very few users viewed risks and consequences as arising from their own mistakes or negligence. Leaving their accounts logged into and use of weak passwords are some of the ways users propagate risks by being negligent. The hypothesis drawn from this was that users are unaware of the risks arising from their own mistakes, or that they were not considered important enough to be relevant. It may also be that users were simply just not aware that they were doing these and other security relevant activities wrong. To the user, the risks are too abstract in nature and there is no benefit to be derived from taking measures to protect themselves from these risks.

From the above researches, it is clear to see that majority of Wi-Fi users are not aware of the risks they are open to. Therefore, this research hypothesizes that:

**H1: Perceived vulnerability positively influences the intention to enable Wi-Fi security measures.**

A study by Harbach et al. (2014) involved an online survey by use of a questionnaire aimed at testing Wi-Fi risk and consequence awareness of users. The questionnaire was structured to ask users of what risks they were aware of in certain scenarios while using the internet. The scenarios included using the Internet in general, users logging in to their social network accounts, shopping online, online banking, and finding a shared ride using online services.

After stating risks identified for different scenarios, participants of the study were asked to rate the risks on a scale of 0 – 100 as well as common sources they last heard reference of these risks from. They were also asked to state perceived potential consequences for each scenario in order of severity. The questionnaire concludes with a block set of 22 common risks users are frequently warned about. The users’ task was to show which risks they had knowledge of and show their relevance on a scale of “not relevant at all” to “very relevant”.

Results of the study showed that users were aware of risks but gave incorrect consequences for the risks identified. This led to the hypothesis that participants did not evaluate which risks had tangible consequences leading to them underestimating the impact of the risks on themselves (Harbach et al., 2014). Many of the consequences identified involved losing money, causing damage to health and inconveniences arising from risks.
Ratings of low likelihood of occurrence indicated that users viewed the risks and consequences named as never applying to them. This may lead to a carefree attitude while using the internet despite users of the network being aware of the risks and consequences posed to them. Open ended questions were analyzed through coding and showed that many non-financial consequences were phrased in an impersonal manner. This led to researchers hypothesizing that impersonal consequences caused some risks to be ignored as they were not perceived as being relevant to the user.

The above studies show that users may have a vague idea of security risks posed to them when they access the internet but may not implement any security measures to protect against them as they do not believe themselves the likely target of such attacks.

Research by Howe et al. (2012) showed participants of their study believed that only wealthy and “important” people could be attacked. One participant stated they did not make over $40,000 in a year thus could not possibly be the target of any attack. Others stated they had nothing important enough stored on their computers to warrant an attack on their machines.

Therefore, this research hypothesizes that:

H2: Perceived severity positively influences the intention to enable Wi-Fi security measures.

Rewards are defined as tangible or intangible compensations that an individual gains in return for engaging in a desired behavior (Boss, Kirsch, Angermeyer, Shingler, & Boss, 2009). Studies by Boss et al. (2009), Bulgurcu et al. (2010), Siponen, Paaknila, & Mahmood (2006) show that both monetary and non-monetary can act as incentives in encouraging desirable behavior in the information security context.

H3: Rewards positively influences the intention to enable Wi-Fi security measures.

Self-efficacy is defined as “the conviction that one can successfully execute the behavior required to produce outcomes” (Bandura, 1977, p. 215).

The study by Harbach et al. (2014) showed that users would not acknowledge the existence of risks when they believe themselves capable of dealing with the threat. Therefore, this research hypothesizes that:
H5: Self Efficacy positively influences the intention to enable Wi-Fi security measures.

In Harbach et al. (2014) study users who were aware of risks posed to them cited budget constraints as reasons for not implementing security measures. The same study also went on to show that some users believe they can influence their security on the internet. Users may believe themselves capable of dealing with known risks therefore may not perceive any consequences arising from these risks.

As a result, users are less likely to invest time and money attempting to mitigate risks by complying with security measures they do not consider themselves likely targets of. Users would go so far as rationalizing failure to implement and comply with security measures as causing more inconveniences than was necessary (Howe et al., 2012).

Therefore, this research hypothesizes that:

H4: Response efficacy positively influences the intention to enable Wi-Fi security measures.

H6: Response Cost positively influences the intention to enable Wi-Fi security measures.

Lee & Larsen (2009) study extends the protection motivation theory by incorporating situation-specific behavioral control variables i.e. social influence, vendor support, IT budget and firm size. They apply Orlikowski’s theoretical framework known as Structurational Theory of Technology, which shows how IT interacts with organizational forces. This research is based on external organizational settings, however one aspect of this study is shared with the small-and medium-sized businesses (SMBs) in Lee & Larsen, (2009) research – vendor support.

Having a limited number of IT experts to maintain systems has seen IT adoption studies encourage SMBs to outsource the much needed human resource. The individuals targeted in this research source their wireless services and access points from different vendors. This outside sourcing of equipment and services may come tied with the vendor firm’s policies on usage and security. It therefore becomes vital to incorporate vendor support as one of the instruments to measure.
H7: Vendor Support positively influences the intention to enable Wi-Fi security measures.

PMT is a social cognitive account of protective behavior however, prior researches have only concentrated on the cognitive account. The study by Lee & Larsen (2009) found that SMB executives were more likely to adopt anti-malware software if they found their business referents adopted the software. Tu & Yuan (2011) also take into account that individual’s behavior is unavoidably influenced by other people. When users lack information on threat avoidance tactics, the gap in knowledge is filled by their social environment which allows them to engage in safeguarding measures. This research expects that if Wi-Fi owners’ motivation to secure their network does not stem from their immediate environment or vendor support, it may come from competitors or network users. Therefore, this research hypothesizes that:

H8: Pressures positively influences the intention to enable Wi-Fi security measures.

The above constructs measure users’ intention to secure their Wi-Fi networks. This study will also assess users’ intentions against actual implementations observed from the wardrives conducted. This will enable the researcher to find out whether intent is a significant predictor of actual behavior. Therefore, this research hypothesizes that:

H9: Intention to secure a Wi-Fi network significantly influences the security observed
### 4.3.2. Measurement Model

The table below displays the survey questions used to measure the hypotheses in this study.

**Table 4.3.2: Questionnaire Sources**

<table>
<thead>
<tr>
<th>Construct</th>
<th>Items</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Our network could be subjected to a malicious hacking attempt.</td>
<td>(Woon et al., 2005)</td>
</tr>
<tr>
<td></td>
<td>We at risk of becoming victims of an unsecured Wi-Fi network.</td>
<td>(Matt &amp; Peckelsen, 2016)</td>
</tr>
<tr>
<td>Perceived Vulnerability</td>
<td>It is likely that we will experience Wi-Fi hacking incidents</td>
<td></td>
</tr>
<tr>
<td></td>
<td>It is possible that we will experience Wi-Fi hacking incidents.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Having an unsecured Wi-Fi network poses a severe security risk to our network and its users</td>
<td>(Al-ghaith, 2016; Lee &amp; Larsen, 2009; Matt &amp; Peckelsen, 2016; Woon et al., 2005)</td>
</tr>
<tr>
<td></td>
<td>Having an unsecured Wi-Fi network can enable remote access of sensitive data by third parties</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Having an unsecured Wi-Fi network can allow remote access to our mobile devices and computers</td>
<td></td>
</tr>
<tr>
<td>Perceived Severity</td>
<td>I believe that the consequences of using an unsecured Wi-Fi network are severe.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>I believe that the consequences of using an unsecured Wi-Fi network can be serious.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>I believe that the consequences of using an unsecured Wi-Fi network can be significant.</td>
<td></td>
</tr>
<tr>
<td>Rewards</td>
<td>Securing our Wi-Fi network would be worthwhile to its users</td>
<td>(Boss, Galletta, Lowry, Moody, &amp; Polak, 2015; Bulgureu et al., 2010; LaRose, Rifon, &amp; Enbody, 2008)</td>
</tr>
<tr>
<td></td>
<td>Enabling security on our Wi-Fi network would provide gains to its users</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Enabling security measures on our Wi-Fi network would be beneficial to its users</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Securing our Wi-Fi network would be favorable to its users</td>
<td></td>
</tr>
<tr>
<td>Response Efficacy</td>
<td>Enabling security measures on our Wi-Fi network will prevent hackers from stealing network bandwidth</td>
<td>(Matt &amp; Peckelsen, 2016; Woon et al., 2005)</td>
</tr>
<tr>
<td></td>
<td>Enabling the security measures on our Wi-Fi network is an effective way of deterring hacker attacks</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Enabling security measures on our Wi-Fi network will prevent hackers from gaining important personal/financial information</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Enabling security measures on our Wi-Fi network will prevent hackers from stealing my identity</td>
<td></td>
</tr>
</tbody>
</table>
| **Self-Efficacy** | It would be easy for us to enable security features on the Wi-Fi network  
We could enable Wi-Fi security measures if there was no-one around to tell us what to do  
We could enable Wi-Fi security measures if we only had manuals for reference  
We are able to set up Wi-Fi security features without much effort | (Anderson & Agarwal, 2010; Matt & Peckelsen, 2016; Woon et al., 2005) |
| **Response Cost** | The cost of enabling security measures on our Wi-Fi network would decrease its convenience  
There are too many overheads associated with trying to enable security measures on our Wi-Fi network  
Enabling security features on our Wi-Fi network would require considerable effort  
Enabling security features on our Wi-Fi network would be time consuming | (Woon et al., 2005) |
| **Vendor Support** | Our vendors provide support to help with the difficulties of setting up Wi-Fi security  
Our vendors offer training on how to setup Wi-Fi security  
Our vendors provide us with technical support for the Wi-Fi network | (Lee & Larsen, 2009) |
| **Pressures** | Our network users/customers believe we should have a secure Wi-Fi network  
Our network users require us to setup strong Wi-Fi security  
My colleagues think we should set up a secure Wi-Fi network  
My managers/supervisors require us to setup strong Wi-Fi security | (Lee & Larsen, 2009) |
| **Behavioral Intention** | It has been our intention to setup a secure Wi-Fi network  
It has been our intention to operate a secure Wi-Fi network  
It has been our intention to protect the users of our Wi-Fi network from hacking attempts  
We have always thought our Wi-Fi network was secure | (Al-ghaith, 2016; Anderson & Agarwal, 2010; Matt & Peckelsen, 2016) |
4.5. Proof-of-Concept

The target area for my wardrive was Nairobi’s Central Business District. However, before commencing on the targeted area, I did some initial tests around the USIU environment to ensure my setup was working and I was indeed capturing wireless packets from various Wi-Fi access points.

During the initial tests, I discovered that while attempting to conceal the laptop and other gadgets in a bag not draw too much attention to myself, I ended up collecting no data at all. This may have been due to a number of reasons.

i. Despite changing sleep and hibernate settings on the laptop in use to “never, after walking around selected areas (warwalking), I would find the laptop in a sleep state or shutdown. Again, there’s a number of possible reasons that could explain this behavior. It could be that the processes running were too resource hungry and the laptop fan needed more air to cool the system. Being in enclosed in a bag though, the laptop would have to shutdown or sleep to avoid overheating – depending on the manufacturer’s safety settings.

ii. It may have been that the external wireless card wasn’t receiving signals because it was enclosed in a bag.

iii. It may also have been that the laptop was running out of battery but there was no way of knowing as it was enclosed in a bag.

What these initial warwalks helped determine was that conducting a warwalk in the actual targeted area was no longer an option. I had considered this as driving in CBD can be insecure and / or frustrating due to the endless commotion of traffic caused by public service vehicles.

Therefore, to ensure that I could collect information on the WAPs around the USIU area, I walked around the campus with the laptop and accompanying hardware gadgets without enclosing them in a carrier. Being a learning institution, the test was conducted safely without the fear of loss from theft from malicious idlers.

Results proved that the setup was working well and the laptop had enough battery to last about an hour and fifteen minutes while capturing wireless packets from different WAPs.
Figure 4.5.1: Kismet server displaying captured packets in the USIU area

Before distribution of survey questionnaires, an information systems expert was given the survey to ensure face validity. The measures used were all sourced from previous studies and had therefore been previously validated.

4.6. Chapter Summary

This chapter has discussed the theoretical model used in this research study, the Protection Motivation Theory. The analysis procedures used – PLS-SEM – are also discussed here. It also presents the measurement constructs used in hypotheses testing for the Wireless Access points (WAPs) discovered in the wardrive conducted by the researcher.
CHAPTER 5: RESULTS AND FINDINGS

5.1. Introduction
This section shows the results of the various mitigation strategies that may be used to secure against Wi-Fi vulnerabilities as well as the results of the wardrives conducted in Nairobi’s Central Business District.

It also shows the method used to analyze data collected from the wardrive using the Partial Least Squares based Structural Equation Modelling (PLS-SEM) algorithm. More specifically, the WarpPLS v5.0 software was used. PLS-SEM is preferred in research studies where the main aim is exploratory model building rather than theory testing (Hair, Celsi, Money, Samouel, & Page, 2016). PLS-SEM algorithms in general also tend to be better at analyzing data with small sample sizes (Kock, 2015a).

Section 5.4 shows the findings for the analyzed measurement and structural models giving results for the reliability, validation and variance explained by the model.

5.2. Wi-Fi Security Mitigations against Vulnerabilities and Risks
This research successfully set up a wireless access point with WPA2 security as well as firewall as shown in figure 5.2.3. The SSID is changed to an unidentifiable name that cannot be associated with the access points’ manufacturer or the owner of the WAP as shown in figure 5.2.1. Login username and passwords are also changed from the defaults ‘admin’ and ‘password’.

![Wireless Configuration](image)

Figure 5.2.1: Illustrating Default SSID changed, WPA2 enabled & WPS disabled

54
Automatic security configuration (WPS) is disabled due to inherent exploitable vulnerabilities of the feature. A guest network can also be setup for non-regular users (figure 5.2.2) where security keys do not have to be shared with the main network.

Figure 5.2.2: Setup of Guest Network

MAC address filtering can also be setup to ensure that only the specified devices can access the network as shown in figure 5.2.4. By default this disables the WPS feature. This setting alone does not ensure security as MAC addresses can be spoofed in an identity attack.

Figure 5.2.3: Firewall setup on the access point
Figure 5.2.4: MAC address Filtering and WPS disabled.

A VPN was also successfully setup on an Android phone as shown in figure 5.2.5. The VPN enables secure connection to the internet by encrypting and anonymizing all data sent from and to a device. It also hides the location of the user so an attacker is unaware of the traffic’s source and destination (figure 5.2.6).

Figure 5.2.5: Enabling VPN protection on Android Device using F-Secure
5.3. Identifying Current State of Security Implementations in Nairobi’s CBD.

Two wardrives were conducted within Nairobi’s Central Business District. The first wardrive discovered a total of 2,333 WAPs while the second wardrive discovered 1,299 WAPs.

To translate this data onto a geographical map, I used GisKismet. GisKismet is a wireless reconnaissance tool that represents data captured in Kismet in a SQLite database. By querying the database it creates, one can specify to change the output format to a KML file, a Google Maps or Google Earth compatible file format as shown in figure 5.3.1.
Figure 5.3.1: Querying GisKismet database & specifying KML output

Figure 5.3.2 from wardrive1 and figure 5.3.3 of wardrive2 show the converted XML data from Kismet displayed in the SQLite database.

Figure 5.3.2 SQLite database displaying WAPs from the first wardrive
Figure 5.3.3: SQLite database displaying WAPs from the second wardrive

The following are geographical mappings of the wireless access points captured using Kismet. Figure 5.3.4 is an aerial view of the total number of access points discovered in the wardrive. Figure 5.3.5 displays access points using WPA2 protocol while figure 5.3.6 shows access points using WPA/WPA2 protocol.

Figure 5.3.4 Map of all the WAPs discovered in Nairobi’s CBD
Figure 5.3.5: Map of all the WAPs using WPA+PSK & WPA+AES

Figure 5.3.6: Map of all the WAPs using WPA+TKIP WPA+PSK & WPA+AES

Figure 5.3.7 shows the mapping of access points using no security (open) while figure 5.3.8 shows access points using the WEP security protocol.
Figure 5.3.7: Map of all the WAPs using no encryption protocol from wardrive 1

Figure 5.3.8: Map of all the WAPs using WEP encryption from wardrive 1

Table 5.3.1 shows the summary of the results from wardrive 1 and wardrive 2 categorizing access points based on the security protocol in place.
Table 5.3.1: Displays summary of the wardrive results breakdown

<table>
<thead>
<tr>
<th>Wardrive No.</th>
<th>Date Conducted</th>
<th>Encryption</th>
<th>No. of Access Points</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>None</td>
<td>WEP</td>
</tr>
<tr>
<td>1</td>
<td>7/11/16</td>
<td>353</td>
<td>45</td>
</tr>
<tr>
<td>2</td>
<td>9/11/16</td>
<td>239</td>
<td>24</td>
</tr>
<tr>
<td>Average</td>
<td></td>
<td>296</td>
<td>34</td>
</tr>
</tbody>
</table>

5.4. Assessing Factors Influencing Wi-Fi Security Implementations Using PMT.

Sixty questionnaires were distributed however, only 49 were returned by the respondents. Four questionnaires were eliminated because only the demographics section had been filled out. This left a total of 45 valid responses for data analysis. All data constructs were measured on a five-item scale (1=strongly disagree 2=Disagree 3=Neutral 4=Agree 5=strongly agree).

Data was cleaned and checked for missing values. Two missing data items were found for Participant Number 05 construct item SE2 and Participant Number 31 construct item SE3.

Cells with missing values were imputed with the mean of the variable items for that participant.

Five outliers were identified for the construct item PS2. The affected case numbers included 2, 14, 16, 20 and 22. I chose to retain the outliers identified because they provided beneficial information on the population that would have otherwise not been discovered in the normal course of analysis as suggested by (Hair et al., 2010).

Sixty-seven percent of the survey participants were male. The participants were mainly from the 26-35-year age group (51%). Majority of the participants were non-IT
professionals (62%) yet they rated themselves as mainly having intermediate (33%) and advanced (31%) computer skills. The businesses offering Wireless Network services were mainly retail stores (47%) and in the food and beverage industry (27%). The survey participants reported that mostly 1-20 people (49%) used their wireless networks each day and they used the connectivity mainly for email (69%) and social media (89%) interaction.

**Table 5.4.1: Display of the demographics summary.**

<table>
<thead>
<tr>
<th>Item</th>
<th>Frequency</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gender</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Male</td>
<td>30</td>
<td>66.7</td>
</tr>
<tr>
<td>Female</td>
<td>15</td>
<td>33.3</td>
</tr>
<tr>
<td>Age</td>
<td></td>
<td></td>
</tr>
<tr>
<td>18-25</td>
<td>11</td>
<td>24.4</td>
</tr>
<tr>
<td>26-35</td>
<td>23</td>
<td>51.1</td>
</tr>
<tr>
<td>36-45</td>
<td>11</td>
<td>24.4</td>
</tr>
<tr>
<td>Computer Skills</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Low</td>
<td>1</td>
<td>2.2</td>
</tr>
<tr>
<td>Basic</td>
<td>6</td>
<td>13.3</td>
</tr>
<tr>
<td>Intermediate</td>
<td>15</td>
<td>33.3</td>
</tr>
<tr>
<td>Advanced</td>
<td>14</td>
<td>31.1</td>
</tr>
<tr>
<td>Expert</td>
<td>9</td>
<td>20.0</td>
</tr>
<tr>
<td>Business Category</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Food &amp; Beverages</td>
<td>12</td>
<td>26.7</td>
</tr>
<tr>
<td>Retail Store</td>
<td>21</td>
<td>46.7</td>
</tr>
<tr>
<td>Beauty</td>
<td>3</td>
<td>6.7</td>
</tr>
<tr>
<td>Transportation</td>
<td>1</td>
<td>2.2</td>
</tr>
<tr>
<td>Other</td>
<td>8</td>
<td>17.8</td>
</tr>
<tr>
<td>Job Role</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IT Profession</td>
<td>17</td>
<td>37.8</td>
</tr>
<tr>
<td>Non-IT Profession</td>
<td>28</td>
<td>62.2</td>
</tr>
<tr>
<td>Wi-Fi users @ day</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1-20</td>
<td>22</td>
<td>48.9</td>
</tr>
<tr>
<td>21-50</td>
<td>8</td>
<td>17.8</td>
</tr>
<tr>
<td>51-100</td>
<td>5</td>
<td>11.1</td>
</tr>
<tr>
<td>100-200</td>
<td>4</td>
<td>8.9</td>
</tr>
<tr>
<td>200-300</td>
<td>4</td>
<td>8.9</td>
</tr>
<tr>
<td>&gt; 300</td>
<td>2</td>
<td>4.4</td>
</tr>
<tr>
<td>Online Service Usage</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Email</td>
<td>31</td>
<td>68.9</td>
</tr>
<tr>
<td>Social Media</td>
<td>40</td>
<td>88.9</td>
</tr>
<tr>
<td>Online Shopping</td>
<td>13</td>
<td>28.8</td>
</tr>
<tr>
<td>Online Banking</td>
<td>6</td>
<td>13.3</td>
</tr>
</tbody>
</table>

The measurement model test resulted in statistically accepted Goodness-of-Fit between the data and the proposed model as proposed by (Kock, 2015b). The following table displays the various goodness-of-fit statistics.
Table 5.4.2: Summary of Goodness-of-Fit statistics.

<table>
<thead>
<tr>
<th>Measure</th>
<th>Value</th>
<th>P Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Average path coefficient (APC) (&lt;0.05)</td>
<td>0.214</td>
<td>0.031</td>
</tr>
<tr>
<td>Average R-squared (ARS) (&lt;0.05)</td>
<td>0.416</td>
<td>P&lt;0.001</td>
</tr>
<tr>
<td>Average adjusted R-squared (AARS)</td>
<td>0.381</td>
<td>P&lt;0.001</td>
</tr>
<tr>
<td>Average block VIF (AVIF)</td>
<td>2.363</td>
<td>Good if &lt;= 5, ideally &lt;= 3.3</td>
</tr>
<tr>
<td>Average full collinearity VIF (AFVIF)</td>
<td>1.878</td>
<td>Acceptable if &lt;= 5, ideally &lt;= 3.3</td>
</tr>
<tr>
<td>Tenenhaus GoF (GoF)</td>
<td>0.533</td>
<td>Small &gt;= 0.1, medium &gt;= 0.25, large &gt;= 0.36</td>
</tr>
<tr>
<td>Sympson’s paradox ratio (SPR)</td>
<td>0.778</td>
<td>Acceptable if &gt;= 0.7, ideally = 1</td>
</tr>
<tr>
<td>R-squared contribution ratio (RSCR)</td>
<td>0.857</td>
<td>Acceptable if &gt;= 0.9, ideally = 1</td>
</tr>
<tr>
<td>Statistical suppression ratio (SSR)</td>
<td>1.000</td>
<td>Acceptable if &gt;= 0.7</td>
</tr>
<tr>
<td>Nonlinear bivariate causality direction ratio (NLBCDR)</td>
<td>0.889</td>
<td>Acceptable if &gt;= 0.7</td>
</tr>
</tbody>
</table>

Reporting of PLS results follows the structure and recommendations outlined in (Latan & Ramli, 2013).

5.4.1. Measurement Model Analysis

This study’s results show that all constructs composite reliability are above 0.70. Majority of the indicator loadings are above 0.70 except for PS1=0.624, PS4=0.649, RE1=0.541, RE2=0.647, SE3=0.512 and B14=0.543, which are retained to maintain construct validity as none fall below 0.40.

The research displays adequate convergent and discriminant validity and a non-existence of multicollinearity as shown in table 5.4.1.1 below.
<table>
<thead>
<tr>
<th>Construct</th>
<th>Item</th>
<th>Loading</th>
<th>Cronbach’s $\alpha$</th>
<th>Composite Reliability</th>
<th>Convergent Reliability AVE</th>
<th>Multicollinearity VIF</th>
</tr>
</thead>
<tbody>
<tr>
<td>Perceived Vulnerability</td>
<td>PV1</td>
<td>0.766</td>
<td>0.898</td>
<td>0.93</td>
<td>0.77</td>
<td>1.367</td>
</tr>
<tr>
<td></td>
<td>PV2</td>
<td>0.92</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>PV3</td>
<td>0.898</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>PV4</td>
<td>0.916</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Perceived Severity</td>
<td>PS1</td>
<td>0.624</td>
<td>0.807</td>
<td>0.862</td>
<td>0.512</td>
<td>2.333</td>
</tr>
<tr>
<td></td>
<td>PS2</td>
<td>0.782</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>PS3</td>
<td>0.799</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>PS4</td>
<td>0.649</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>PS5</td>
<td>0.71</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>PS6</td>
<td>0.714</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rewards</td>
<td>R1</td>
<td>0.826</td>
<td>0.911</td>
<td>0.938</td>
<td>0.792</td>
<td>2.615</td>
</tr>
<tr>
<td></td>
<td>R2</td>
<td>0.934</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>R3</td>
<td>0.938</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>R4</td>
<td>0.855</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Response Efficacy</td>
<td>RE1</td>
<td>0.541</td>
<td>0.759</td>
<td>0.852</td>
<td>0.602</td>
<td>2.479</td>
</tr>
<tr>
<td></td>
<td>RE2</td>
<td>0.647</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>RE3</td>
<td>0.916</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>RE4</td>
<td>0.926</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Self Efficacy</td>
<td>SE1</td>
<td>0.706</td>
<td>0.583</td>
<td>0.762</td>
<td>0.556</td>
<td>1.524</td>
</tr>
<tr>
<td></td>
<td>SE2</td>
<td>0.723</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SE3</td>
<td>0.512</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SE4</td>
<td>0.715</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Response Cost</td>
<td>RC1</td>
<td>0.765</td>
<td>0.849</td>
<td>0.843</td>
<td>0.573</td>
<td>2.216</td>
</tr>
<tr>
<td></td>
<td>RC2</td>
<td>0.815</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>RC3</td>
<td>0.689</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>RC4</td>
<td>0.754</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vendor Support</td>
<td>VS1</td>
<td>0.816</td>
<td>0.75</td>
<td>0.884</td>
<td>0.719</td>
<td>1.244</td>
</tr>
<tr>
<td></td>
<td>VS2</td>
<td>0.857</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>VS3</td>
<td>0.869</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pressures</td>
<td>P1</td>
<td>0.806</td>
<td>0.804</td>
<td>0.899</td>
<td>0.689</td>
<td>1.285</td>
</tr>
<tr>
<td></td>
<td>P2</td>
<td>0.798</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>P3</td>
<td>0.851</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>P4</td>
<td>0.864</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Behavioral Intention</td>
<td>BI1</td>
<td>0.937</td>
<td>0.855</td>
<td>0.907</td>
<td>0.718</td>
<td>2.582</td>
</tr>
<tr>
<td></td>
<td>BI2</td>
<td>0.933</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>BI3</td>
<td>0.909</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>BI4</td>
<td>0.543</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The square root of the Average Variance Extracted (AVE) displayed along the diagonal, demonstrate discriminant validity for the measurement instruments used in this study. This is displayed in table 5.4.1.2 below.

Table 5.4.1.2: Discriminant validity using Square roots of Average Variances Extracted (AVEs).

<table>
<thead>
<tr>
<th></th>
<th>PV</th>
<th>PS</th>
<th>Rewards</th>
<th>RE</th>
<th>SE</th>
<th>RC</th>
<th>VS</th>
<th>Pressures</th>
<th>BI</th>
</tr>
</thead>
<tbody>
<tr>
<td>PV</td>
<td>0.877</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PS</td>
<td>0.349</td>
<td>0.716</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rewards</td>
<td>0.414</td>
<td>0.617</td>
<td>0.89</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RE</td>
<td>0.308</td>
<td>0.605</td>
<td>0.613</td>
<td>0.776</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SE</td>
<td>0.128</td>
<td>0.111</td>
<td>0.427</td>
<td>0.408</td>
<td>0.67</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RC</td>
<td>0.132</td>
<td>-0.283</td>
<td>-0.156</td>
<td>-0.162</td>
<td>0.021</td>
<td>0.757</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VS</td>
<td>0.164</td>
<td>0.186</td>
<td>0.13</td>
<td>0.171</td>
<td>0.141</td>
<td>-0.132</td>
<td>0.848</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pressures</td>
<td>0.176</td>
<td>0.235</td>
<td>0.506</td>
<td>0.369</td>
<td>0.425</td>
<td>-0.131</td>
<td>0.214</td>
<td>0.83</td>
<td></td>
</tr>
<tr>
<td>BI</td>
<td>0.097</td>
<td>0.249</td>
<td>0.426</td>
<td>0.498</td>
<td>0.342</td>
<td>-0.262</td>
<td>0.384</td>
<td>0.672</td>
<td>0.847</td>
</tr>
</tbody>
</table>

Table 5.4.1.3 displays the loadings and cross loadings of the data that was analyzed.
<table>
<thead>
<tr>
<th></th>
<th>PV</th>
<th>PS</th>
<th>Rewards</th>
<th>RespEff</th>
<th>SelfEff</th>
<th>Pressur</th>
<th>RC</th>
<th>VS</th>
<th>BI</th>
</tr>
</thead>
<tbody>
<tr>
<td>PV1</td>
<td>0.766</td>
<td>-0.027</td>
<td>-0.125</td>
<td>-0.015</td>
<td>-0.049</td>
<td>0.146</td>
<td>-0.16</td>
<td>0.313</td>
<td>-0.208</td>
</tr>
<tr>
<td>PV2</td>
<td>0.92</td>
<td>0.046</td>
<td>0.006</td>
<td>0.05</td>
<td>-0.051</td>
<td>0.128</td>
<td>0.081</td>
<td>-0.11</td>
<td>-0.154</td>
</tr>
<tr>
<td>PV3</td>
<td>0.898</td>
<td>-0.023</td>
<td>0.051</td>
<td>-0.019</td>
<td>0.075</td>
<td>-0.11</td>
<td>0.018</td>
<td>-0.133</td>
<td>0.118</td>
</tr>
<tr>
<td>PV4</td>
<td>0.916</td>
<td>-0.001</td>
<td>0.048</td>
<td>-0.019</td>
<td>0.019</td>
<td>-0.143</td>
<td>0.034</td>
<td>-0.021</td>
<td>0.213</td>
</tr>
<tr>
<td>PS1</td>
<td>-0.076</td>
<td>0.624</td>
<td>-0.283</td>
<td>0.693</td>
<td>-0.154</td>
<td>0.194</td>
<td>0.341</td>
<td>-0.071</td>
<td>0.045</td>
</tr>
<tr>
<td>PS2</td>
<td>0.107</td>
<td>0.782</td>
<td>-0.087</td>
<td>0.222</td>
<td>-0.044</td>
<td>-0.131</td>
<td>-0.024</td>
<td>0.2</td>
<td>0.108</td>
</tr>
<tr>
<td>PS3</td>
<td>0.054</td>
<td>0.799</td>
<td>-0.16</td>
<td>0.239</td>
<td>0.081</td>
<td>-0.1</td>
<td>0.024</td>
<td>0.286</td>
<td>0.072</td>
</tr>
<tr>
<td>PS4</td>
<td>-0.043</td>
<td>0.649</td>
<td>0.338</td>
<td>-0.334</td>
<td>-0.089</td>
<td>0.04</td>
<td>-0.208</td>
<td>-0.224</td>
<td>-0.007</td>
</tr>
<tr>
<td>PS5</td>
<td>0.016</td>
<td>0.71</td>
<td>0.289</td>
<td>-0.414</td>
<td>0.039</td>
<td>0.103</td>
<td>-0.362</td>
<td>-0.121</td>
<td>-0.258</td>
</tr>
<tr>
<td>PS6</td>
<td>-0.089</td>
<td>0.714</td>
<td>-0.074</td>
<td>-0.4</td>
<td>0.135</td>
<td>-0.054</td>
<td>0.251</td>
<td>-0.152</td>
<td>0.025</td>
</tr>
<tr>
<td>R1</td>
<td>-0.149</td>
<td>-0.077</td>
<td>0.826</td>
<td>-0.068</td>
<td>-0.195</td>
<td>0.183</td>
<td>-0.006</td>
<td>0.047</td>
<td>0.073</td>
</tr>
<tr>
<td>R2</td>
<td>0.002</td>
<td>-0.038</td>
<td>0.934</td>
<td>-0.129</td>
<td>0.111</td>
<td>-0.066</td>
<td>-0.129</td>
<td>-0.001</td>
<td>-0.093</td>
</tr>
<tr>
<td>R3</td>
<td>-0.033</td>
<td>0.08</td>
<td>0.938</td>
<td>-0.191</td>
<td>0.053</td>
<td>-0.134</td>
<td>0.044</td>
<td>-0.067</td>
<td>0.123</td>
</tr>
<tr>
<td>R4</td>
<td>0.177</td>
<td>0.028</td>
<td>0.855</td>
<td>0.415</td>
<td>0.009</td>
<td>0.043</td>
<td>0.1</td>
<td>0.03</td>
<td>-0.104</td>
</tr>
<tr>
<td>RE1</td>
<td>-0.016</td>
<td>-0.401</td>
<td>-0.009</td>
<td>0.541</td>
<td>-0.368</td>
<td>0.519</td>
<td>0.085</td>
<td>-0.067</td>
<td>-0.64</td>
</tr>
<tr>
<td>RE2</td>
<td>-0.125</td>
<td>0.023</td>
<td>0.726</td>
<td>0.647</td>
<td>-0.205</td>
<td>-0.18</td>
<td>-0.075</td>
<td>-0.018</td>
<td>0.464</td>
</tr>
<tr>
<td>RE3</td>
<td>0.08</td>
<td>0.176</td>
<td>-0.182</td>
<td>0.916</td>
<td>0.22</td>
<td>-0.186</td>
<td>0.004</td>
<td>-0.006</td>
<td>0.051</td>
</tr>
<tr>
<td>RE4</td>
<td>0.017</td>
<td>0.045</td>
<td>-0.322</td>
<td>0.926</td>
<td>0.14</td>
<td>0.006</td>
<td>-0.001</td>
<td>0.058</td>
<td>-0.001</td>
</tr>
<tr>
<td>SE1</td>
<td>-0.119</td>
<td>-0.365</td>
<td>0.575</td>
<td>-0.033</td>
<td>0.706</td>
<td>-0.352</td>
<td>-0.324</td>
<td>0.054</td>
<td>0.168</td>
</tr>
<tr>
<td>SE2</td>
<td>0.241</td>
<td>-0.171</td>
<td>-0.089</td>
<td>0.304</td>
<td>0.723</td>
<td>0.198</td>
<td>0.135</td>
<td>-0.102</td>
<td>-0.388</td>
</tr>
<tr>
<td>SE3</td>
<td>0.179</td>
<td>0.52</td>
<td>-0.39</td>
<td>-0.36</td>
<td>0.512</td>
<td>0.078</td>
<td>0.357</td>
<td>-0.296</td>
<td>0.582</td>
</tr>
<tr>
<td>SE4</td>
<td>-0.255</td>
<td>0.16</td>
<td>-0.198</td>
<td>-0.016</td>
<td>0.715</td>
<td>0.092</td>
<td>-0.073</td>
<td>0.262</td>
<td>-0.19</td>
</tr>
<tr>
<td>P1</td>
<td>0.082</td>
<td>0.048</td>
<td>-0.226</td>
<td>0.041</td>
<td>0.081</td>
<td>0.806</td>
<td>0.061</td>
<td>-0.004</td>
<td>-0.113</td>
</tr>
<tr>
<td>P2</td>
<td>0.102</td>
<td>-0.461</td>
<td>0.206</td>
<td>0.134</td>
<td>-0.001</td>
<td>0.798</td>
<td>-0.08</td>
<td>0.024</td>
<td>-0.308</td>
</tr>
<tr>
<td>P3</td>
<td>-0.125</td>
<td>0.416</td>
<td>-0.182</td>
<td>-0.208</td>
<td>0.028</td>
<td>0.851</td>
<td>-0.021</td>
<td>-0.135</td>
<td>0.196</td>
</tr>
<tr>
<td>P4</td>
<td>-0.048</td>
<td>-0.029</td>
<td>0.199</td>
<td>0.044</td>
<td>-0.101</td>
<td>0.864</td>
<td>0.038</td>
<td>0.114</td>
<td>0.197</td>
</tr>
<tr>
<td>RC1</td>
<td>-0.055</td>
<td>-0.003</td>
<td>-0.366</td>
<td>-0.099</td>
<td>0.352</td>
<td>-0.06</td>
<td>0.765</td>
<td>-0.252</td>
<td>0.273</td>
</tr>
<tr>
<td>RC2</td>
<td>-0.095</td>
<td>-0.12</td>
<td>0.228</td>
<td>-0.072</td>
<td>-0.378</td>
<td>0.318</td>
<td>0.815</td>
<td>0.073</td>
<td>0.029</td>
</tr>
<tr>
<td>RC3</td>
<td>0.224</td>
<td>-0.072</td>
<td>0.064</td>
<td>0.197</td>
<td>-0.28</td>
<td>-0.04</td>
<td>0.689</td>
<td>0.225</td>
<td>-0.146</td>
</tr>
<tr>
<td>RC4</td>
<td>-0.046</td>
<td>0.199</td>
<td>0.067</td>
<td>-0.001</td>
<td>0.306</td>
<td>-0.247</td>
<td>0.754</td>
<td>-0.029</td>
<td>-0.175</td>
</tr>
<tr>
<td>VS1</td>
<td>0.062</td>
<td>0.131</td>
<td>-0.43</td>
<td>0.182</td>
<td>0.082</td>
<td>-0.172</td>
<td>0.056</td>
<td>0.816</td>
<td>0.334</td>
</tr>
<tr>
<td>VS2</td>
<td>0.002</td>
<td>-0.14</td>
<td>0.189</td>
<td>-0.181</td>
<td>0.202</td>
<td>-0.066</td>
<td>-0.025</td>
<td>0.857</td>
<td>-0.039</td>
</tr>
<tr>
<td>VS3</td>
<td>-0.06</td>
<td>0.015</td>
<td>0.218</td>
<td>0.008</td>
<td>-0.276</td>
<td>0.227</td>
<td>-0.028</td>
<td>0.869</td>
<td>-0.275</td>
</tr>
<tr>
<td>BI1</td>
<td>0.13</td>
<td>0.073</td>
<td>-0.15</td>
<td>-0.097</td>
<td>0.131</td>
<td>-0.116</td>
<td>-0.021</td>
<td>-0.107</td>
<td>0.937</td>
</tr>
<tr>
<td>BI2</td>
<td>0.028</td>
<td>0.111</td>
<td>-0.026</td>
<td>-0.011</td>
<td>-0.063</td>
<td>0.051</td>
<td>-0.06</td>
<td>-0.021</td>
<td>0.933</td>
</tr>
<tr>
<td>BI3</td>
<td>0.183</td>
<td>-0.032</td>
<td>-0.156</td>
<td>0.01</td>
<td>-0.003</td>
<td>0.023</td>
<td>-0.073</td>
<td>0.031</td>
<td>0.909</td>
</tr>
<tr>
<td>BI4</td>
<td>-0.577</td>
<td>-0.263</td>
<td>0.565</td>
<td>0.169</td>
<td>-0.113</td>
<td>0.076</td>
<td>0.26</td>
<td>0.169</td>
<td>0.543</td>
</tr>
</tbody>
</table>
5.4.2. Structural Model Analysis

Fig 5.4.2.1 shows the results of the research hypotheses, their path coefficients and respective P-values along with the amount of variance explained by behavioral intention and the observed security.

Figure 5.4.2.1: Results of the Structural Model Testing
78% of the total variance of the intention to secure Wi-Fi networks and 5% of that of the security observed was explained.

Hypotheses H3 (β = 0.25, P = 0.03), H4 (β = 0.32, P < 0.01) and H8 (β = 0.79, P <0.001) were strongly supported whereas H1 (β = 0.02, P = 0.45), H2 (β = 0.06, P = 0.33), H5 (β = 0.69, P = 0.26), H6 (β = 0.12, P = 0.19), H7 (β = 0.05, P = 0.37) and H9 (β = 0.22, P = 0.06) were not supported.

The effect size of the latent variables in this study was large $f^2 = 48\%$ while the predictive relevance of intent to adopt Wi-Fi security was $Q^2=0.74$ and that of the observed security was $Q^2=0.055$. Table 5.3.2.1 shows the latent variables contribution to effect size $f^2$.

The magnitude of the effect sizes indicates that the greatest motivator of enabling Wi-Fi security measures is pressures (effect size = .639).

**Table 5.4.2.1: Effect size contributions**

<table>
<thead>
<tr>
<th>Construct</th>
<th>$f^2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Perceived Vulnerability</td>
<td>0.003</td>
</tr>
<tr>
<td>Perceived Severity</td>
<td>0.02</td>
</tr>
<tr>
<td>Rewards</td>
<td>0.147</td>
</tr>
<tr>
<td>Response Efficacy</td>
<td>0.203</td>
</tr>
<tr>
<td>Self-Efficacy</td>
<td>0.051</td>
</tr>
<tr>
<td>Response Cost</td>
<td>0.039</td>
</tr>
<tr>
<td>Vendor Support</td>
<td>0.02</td>
</tr>
<tr>
<td>Pressure</td>
<td>0.635</td>
</tr>
</tbody>
</table>
Table 5.4.2.2: Summary of Tests of Hypotheses

<table>
<thead>
<tr>
<th>Hypothesis</th>
<th>Path Coefficients</th>
<th>P – Values</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>H1: Perceived vulnerability → Intention</td>
<td>β = 0.02</td>
<td>P = 0.45</td>
<td>Not Supported</td>
</tr>
<tr>
<td>H2: Perceived severity → Intention</td>
<td>β = 0.06</td>
<td>P = 0.33</td>
<td>Not Supported</td>
</tr>
<tr>
<td>H3: Rewards → Intention</td>
<td>β = 0.25</td>
<td>P = 0.03</td>
<td>Supported</td>
</tr>
<tr>
<td>H4: Response efficacy → Intention</td>
<td>β = 0.32</td>
<td>P &lt; 0.01</td>
<td>Supported</td>
</tr>
<tr>
<td>H5: Self-efficacy → Intention</td>
<td>β = 0.69</td>
<td>P = 0.26</td>
<td>Not Supported</td>
</tr>
<tr>
<td>H6: Response Cost → Intention</td>
<td>β = 0.12</td>
<td>P = 0.19</td>
<td>Not Supported</td>
</tr>
<tr>
<td>H7: Vendor Support → Intention</td>
<td>β = 0.05</td>
<td>P = 0.37</td>
<td>Not Supported</td>
</tr>
<tr>
<td>H8: Pressures → Intention</td>
<td>β = 0.79</td>
<td>P &lt; 0.001</td>
<td>Supported</td>
</tr>
<tr>
<td>H9: Intention → Observed Security</td>
<td>β = 0.22</td>
<td>P = 0.06</td>
<td>Not Supported</td>
</tr>
</tbody>
</table>

5.5. Chapter Summary

The research model and hypotheses for this study were tested using WarpPLS v5.0, a PLS-SEM statistical tool. The measures for composite reliability, convergent and discriminant validity of the model were found to be statistically acceptable.

The model explained 78% of the total variance of the intention to secure Wi-Fi networks and 5% of that of the security observed.

Rewards, Response Efficacy and Pressures were the hypotheses that were found to be supported. Perceived vulnerability, perceived severity, self-efficacy, response cost, vendor support and behavioral intention were not supported by the model.
CHAPTER 6: DISCUSSION, CONCLUSIONS & RECOMMENDATIONS

6.1 Introduction
This chapter presents a summary of the study, discussion and conclusions drawn from the findings and finally recommendations for practice and further research on the problem. It also suggests possible theoretical and practical implications from the results.

The main objective of the study was to determine the construct variables that could be used to predict intention to implement Wi-Fi security measures and compare this to the actual security implemented on Wi-Fi networks as observed by the researcher.

6.2 Summary
This study set out to determine the factors that influence level of security measures implemented on Wi-Fi networks in Nairobi’s Central Business District. By conducting two wardrives in the area on separate occasions and under different weather conditions, an average total number of 1816 wireless access points were identified.

On average, three hundred and thirty (330) access points implemented weak to no security measures (WEP and Open networks), whereas one thousand four hundred and eighty four (1484) access points implemented mixed levels of stronger security (WPA, WPA2 with TKIP or AES encryption).

By use of convenience sampling, access points that could be easily located and accessed based on their SSIDs were sampled. This resulted in a total of 45 wireless access point samples.

The research study adopted the protection motivation theory (PMT) from health psychology and expanded it by two latent constructs borrowed from (Lee & Larsen, 2009) to create survey questions that were administered to the sample size. The study proposed and validated a research model investigating the factors influencing the implementation of security mechanisms on Wi-Fi networks in Nairobi’s Central Business District.
Below is a summary of the hypotheses questions that were tested:

**Table 6.2.1: Displays a summary of hypotheses tested and their results.**

<table>
<thead>
<tr>
<th>Hypothesis</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>H1: Perceived vulnerability positively influences the intention to enable Wi-Fi security measures.</td>
<td>P=0.45 Not Supported</td>
</tr>
<tr>
<td>H2: Perceived severity positively influences the intention to enable Wi-Fi security measures.</td>
<td>P=0.33 Not Supported</td>
</tr>
<tr>
<td>H3: Rewards positively influences the intention to enable Wi-Fi security measures.</td>
<td>P=0.03 Supported</td>
</tr>
<tr>
<td>H4: Response efficacy positively influences the intention to enable Wi-Fi security measures.</td>
<td>P&lt;0.01 Supported</td>
</tr>
<tr>
<td>H5: Self-efficacy positively influences the intention to enable Wi-Fi security measures.</td>
<td>P=0.26 Not Supported</td>
</tr>
<tr>
<td>H6: Response Cost positively influences the intention to enable Wi-Fi security measures.</td>
<td>P=0.19 Not Supported</td>
</tr>
<tr>
<td>H7: Vendor Support positively influences the intention to enable Wi-Fi security measures.</td>
<td>P=0.37 Not Supported</td>
</tr>
<tr>
<td>H8: Pressures positively influences the intention to enable Wi-Fi security measures.</td>
<td>P&lt;0.001 Supported</td>
</tr>
<tr>
<td>H9: Intention to secure a Wi-Fi network significantly influences the security observed</td>
<td>P=0.06 Not Supported</td>
</tr>
</tbody>
</table>

The model explained 78% of the variance of the intention to secure Wi-Fi networks whereas the 5% of variance for intent on the influence of actual security implemented was not statistically supported. This suggests that intent has a significant positive influence on making the decision to secure Wi-Fi networks. However, intent to secure Wi-Fi networks did not directly translate to the actual prediction of whether the Wi-Fi networks were indeed protected. The findings on intent were compared to the Wi-Fi security implementations observed by the researcher on the wardrives conducted.

Three of the nine proposed hypotheses were supported. Rewards, response efficacy and pressures were found to have a positive influence on the intent to implement security on Wi-Fi networks. Perceived vulnerability, perceived severity, self-efficacy, response cost
and vendor support were not supported. This did not reflect findings from previous research studies however, this may be attributed to the sample size used. (Joe F. Hair et al., 2011) recommends at least ten times the largest number of structural paths directed at a particular latent construct in the structural model.

It was surprising to note that the strongest motivator contributing to the intent to secure Wi-Fi networks was pressure (H8) from competitors and clients. Vendor support (H7) did not motivate owners of Wi-Fi networks to employ security even where self-efficacy (H5) to secure networks by themselves was absent.

6.3. Discussion

6.3.1. Wi-Fi Security Mitigations against Vulnerabilities and Risks

To ensure users are secured against Wi-Fi vulnerabilities, use of WPA2, VPNs and firewalls is strongly recommended. Users should also ensure they connect to websites using the Secure Hypertext Transfer Protocol (HTTPS) (Raju & Nair, 2015).

In this research, a guest network was set up for non-regular users. This is important as it secures the main networks’ secret key (password). WPS is also disabled from the automatic configuration panel. This is because WPS is vulnerable to attacks and negates the security achievements of WPA2 (Sagers et al., 2015).

Setup of a wireless access point with WPA2 was successfully conducted in this research. Use of a VPN was also successfully implemented on an Android phone. A trial version of the application, F-Secure was installed from Google Play – the Android application market. This is particularly useful in public environments where the user has no control on the level of security implemented on WAPs.

VPNs and firewalls can be implemented on all personal devices connecting to public internet.

6.3.2. Current State of Wi-Fi Security Implementations in Nairobi’s CBD

Results from the two wardrive studies conducted show different number of access points discovered. The first wardrive discovered a total of 2,333 WAPs while the second wardrive discovered 1,299 WAPs. The difference in number can be attributed to the fact that the second wardrive was conducted on a rainy day which may have resulted in signal attenuation. According to Anastasi et al. (2004) signal strength decreases and packet loss
increases in rainy and foggy weather conditions. This is similar to a study conducted by
Vilius et al. (2015) where a lower number of access points was recorded when a wardrive
was conducted on a rainy day.

The same study goes on to show that the speeds used during a wardrive affect the number
of access points recorded. Wardrives conducted for study were in the Central Business
District which is prone to traffic snarl ups. This may have helped in the collection and
logging of access points. However, according to Tsui et al. (2010), warwalking provides
more accurate logging of WAPs.

Compared to studies conducted in other countries Aloul (2010), Nisbet (2012), Osorio
(2008), Sathu & Sarrafa-zadeh (2015) and Vilius et al. (2015), Wi-Fi networks in Nairobi
are more secure. 16% were open/ had no security measures in place, 1.8% used WEP,
6.1% used WPA, 27.5% used WPA-Mixed Mode, and 45.3% used WPA2.

6.3.3. Assessing Factors Influencing Wi-Fi Security Implementations Using
PMT.

6.3.3.1. Effect of Perceived Vulnerability on implementation of Wi-Fi security
measures

In Protection Motivation Theory, perceived vulnerability refers to an individual’s
perception of the likelihood to experience a harmful situation when engaging in risky
behavior. It follows that when an individual’s perceived vulnerability is high, they are
more likely to engage in coping appraisal which in this study involves implementation of
Wi-Fi security measures.

The significance of perceived vulnerability on the intent to enable Wi-Fi security
measures was not supported in this study. This is similar to a study by Woon et al. (2005)
which sort to examine the decision variables influencing home wireless network users to
implement security. Woon et al. found that perceived vulnerability was not a significant
predictor of behavior. Matt & Peckelsen (2016) also found no significant support for the
perceived susceptibility construct in their study (perceived susceptibility is similar to the
perceived vulnerability construct in other studies).

The studies attributed this to substantial differences in people’s perception of various
threats. Despite the occasional reporting of security breaches by mainstream media, the
reports did not specifically highlight whether breaches arose from the use of improperly
secured wireless networks. This is similar to our study as various news reports of cyber-attacks in recent years have been reported in our country resulting to billions of shillings lost. The attack vector is however, rarely reported. This results in a loss of vulnerability perception to users of Wi-Fi networks as the news reports do not address them specifically.

Numerous respondents of this study that used open networks/ employed no security reported no perceived vulnerability. They justified this with the fact that they did not use their Wi-Fi network to browse but only to download and transfer software applications to devices they were setting up. These networks are susceptible to injection attacks where malicious attackers can replace software applications with malicious software masquerading as legitimate applications.

6.3.3.2. Effect of Perceived Severity on implementation of Wi-Fi security measures
Perceived severity refers to “an individual’s assessment of the severity of the consequences resulting from a threatening event occurring” (Crossler, 2010, p. 5).

This research did not find perceived severity to be a significant predictor of the intention to implement Wi-Fi security. This is in direct contrast to Woon et al. (2005) study which supported perceived severity as a significant predictor security being enabled in Wi-Fi networks. He cites the reason for this as the consequences of computer threats being more uniform in impact when compared to threats found in health problems (e.g. alcohol being more detrimental to an individual with liver related problems).

In this research, perceived vulnerability was not found to be a significant predictor of intention to secure Wi-Fi networks. It then follows that individuals who do not perceive Wi-Fi security threats as applying to them will not perceive the consequences stemming from Wi-Fi threats as being applicable to them.

6.3.3.3. Effect of Rewards on implementation of Wi-Fi security measures
Rewards in the PMT context are defined as the extrinsic or intrinsic rewards that could motivate individuals to engage in adaptive behavior. The rewards for the owners of the businesses, as tested in this study, is the satisfaction of the customer.

Bulgurcu (2010) study found rewards as exerting a significant impact on an employee’s perception of the benefit of compliance to information security policies. Similarly, in this
research, rewards is found to be a significant predictor of the intent to secure Wi-Fi networks.

The use of Wi-Fi networks by small-medium businesses sampled in this study was as an additional feature to attract more clients to their businesses. Where customers think it necessary for businesses to secure their networks, businesses secure their networks. This is because businesses gain profits by satisfying their customers. Making adjustments to incorporate customer needs promotes customer loyalty as well.

**6.3.3.4. Effect of Response Efficacy on implementation of Wi-Fi security measures**

Response efficacy in the PMT context refers to an individual’s review of the recommended behavior as being adequate to protect against the threat appraised. Where the individual determines the recommended behavior as being appropriate, they adopt the recommended behavior.

Response efficacy was found to be a statistically significant predictor of the intention to implement Wi-Fi security measures. This finding is consistent with those of several previous studies such as Crossler (2010), Matt & Peckelsen (2016), Siponen et al. (2006) and Woon et al. (2005). Individuals who believe enabling security on their access points will keep the threat of attack from happening are more likely to enable security measures on their Wi-Fi networks.

**6.3.3.5. Effect of Self Efficacy on implementation of Wi-Fi security measures**

Self-efficacy in the PMT context refers to an individual’s assessment of their skills to be able to perform a recommended behavior by themselves. Where individuals do not believe themselves to be capable of performing a recommended behavior, self-efficacy will be low.

In Chenoweth et al. (2009) and Salleh et al. (2013) research studies’, self-efficacy was not found to be a significant predictor in influencing a user’s intention to adopt protective technologies. This is in contrast with the majority of research studies implementing the PMT. Chenoweth et al. (2009) attributes this difference to a contextual artifact where rather than considering an individual’s ability in performing the recommended behavior, the difficulty associated should be considered instead.
This study also found no statistical support for self-efficacy as a predictor of the intent to secure Wi-Fi networks (P=0.26). The items measuring self-efficacy concentrated on the individuals’ ability to enable Wi-Fi security measures and not on the difficulty that the procedure may entail. Future studies may want to specifically assess individuals’ ability to enable security measures based on the ease of understanding the underlying software functions.

6.3.3.6. Effect of Response Cost on implementation of Wi-Fi security measures
Response cost in the PMT context refers to the costs perceived by an individual in performing a recommended coping behavior. They may include monetary expense, inconvenience, difficulty, and the side effects of performing the coping behavior.

The findings for this research study did not find response cost to be a statistically significant predictor of the intent to implement security measures on Wi-Fi networks. This was similar to the findings of Crossler (2010) who attributed the results to mean that the costs associated with taking on preventive measures to avoid loss of personal data were not significant enough to influence individuals’ decision in backing up their data.

The same reason could be used in the context of this research. The costs associated with enabling Wi-Fi security measures were not significant enough to influence individuals’ decision to implement security measures.

6.3.3.7. Effect of Vendor Support on implementation of Wi-Fi security measures
Vendor support was not found to be a statistically significant predictor of the intent to implement Wi-Fi security measures. This was contrary to the findings of Lee & Larsen (2009) who predicted that the provision of 24/7 support services, on-site training and user-friendly online and paper based operator manuals would be crucial in persuading executives to adopt anti malware software.

The reason for this disparity in findings may be due to the response by a majority of the users in this study claiming to receive little to no vendor support or training from the vendors whose Wi-Fi network services they subscribe to.

If vendors took on the responsibility of training and affording user manuals to their clients, we may see a rise in the overall number of Wi-Fi security implementations.
6.3.3.8. Effect of Pressures on implementation of Wi-Fi security measures

In Siponen et al. (2006) study, social pressures are found to have a significant effect on the degree to which information security measures in organizations are taken into account by employees. Lee & Larsen (2009) found significant social influence on executives’ decision to adopt anti-malware software. Similarly in this study, social pressures were found to be statistically significant in predicting the intention to implement Wi-Fi security measures.

Local businesses offering Wi-Fi services to their customers as a means to attract more business are more likely to implement security on their Wi-Fi networks when their customers urge or require them to have secure networks. This is a likely scenario as many people are nowadays found working and socially interacting over Wi-Fi networks in restaurants, schools, airports and even public service vehicles.

To ensure that their customer base is maintained and continues to grow, businesses are likely to comply with their customers wishes.

6.3.3.9. Effect of Intent on actual implementation of Wi-Fi security measures

The lack of statistical significant support in this study for perceived vulnerability and severity of Wi-Fi risks suggests that self-report on intention to secure Wi-Fi networks by users will have no correlation to the actual security implemented. Results of the analysis support this implication (P=0.06).

This is because a user who doesn’t feel threatened or at risk of suffering significant losses from a breach of their network will take no measures to secure their Wi-Fi network despite reporting intention of doing just that. Dupuis et al. (2016) point out that behavioral intention may not be the best predictor of behavior. This observation is supported in this study, as self-reports on intention did not correlate with the behavior observed by the researcher.

Dupuis et al. (2016) also point out that the administration of the survey instrument may influence the respondent’s intention to perform a certain action despite them not having intended to execute it before its administration. This explains the difference in correlation between respondents’ intention and the observed behavior.
6.4 Conclusion
This study contributed significant data to the existing body of knowledge. Wireless access points that were discovered and logged during this study were uploaded to the WiGLE – an online database of wireless access points contributed to by wardrivers. By using and extending the Protection Motivation Theory, this research assessed the cognitive motivating factors influencing the decision to implement Wi-Fi security measures.

There has been a significant number of observed secure Wi-Fi networks in Nairobi’s Central Business District. This research has however determined that the observed security implementations do not stem from user’s awareness of the security risks afforded to unsecured Wi-Fi networks.

The research observed no correlation between the intent to implement security measures and the actual implementation of security on Wi-Fi networks. Managers of these networks were observed to have no perceived vulnerability or perceived severity in relation to use of Wi-Fi security risks. Consequently, coping appraisal methods – self-efficacy and response cost – are not initiated.

Vendor support, another crucial factor that may have contributed to the implementation of secure Wi-Fi networks, was often reported to be absent. In cases where vendors provided support to their clients, no user training or awareness exercises were conducted. This contributes to users’ lack of perceived vulnerability to Wi-Fi risks as well as lack in perceived severity were a threat to become successful.

Vendors should consider educating clients on the importance of implementing security on Wi-Fi networks. Internet users would be more concerned for their online safety if frequent warnings were issued when connecting via insecure methods as is the practice in health sciences where alcohol and cigarette consumption are concerned.

6.5 Recommendations & Future Work
6.5.1. Wi-Fi Security Mitigations against Vulnerabilities and Risks
Wi-Fi users need to invest in securing their personal devices when accessing public Wi-Fi hotspots. This can be done by purchasing easy to use firewall and VPN software in the market.
Use of WPA2 and https should also be strictly followed when accessing the internet from Wi-Fi access points.

Despite prior research by Woon et al. (2005) showing that broadcast of SSID should be disabled, recent findings have shown that this does not enhance security. Wireless sniffers, such as Kismet used in this study, are capable of detecting hidden WAPs defeating the purpose of disabling broadcast of SSID.

6.5.2. Current State of Wi-Fi Security Implementations in Nairobi’s CBD
To enable the logging of all available access points within an area, it is recommended that warwalking be performed rather than wardrives.

Conducting similar wardrives in future would also allow the researcher comparative analysis to find out whether recommended security on Wi-Fi networks has been better implemented. As studies have shown, at the time of writing this study, WPA2 is currently the strongest form of wireless encryption.

Future work may want to consider conducting penetration tests on Wi-Fi networks to find out the information derivable. After gaining consent from participants, the researcher could provide powerful motivating reason for users to consider stronger security implementations on their Wi-Fi network. This would also serve as a form of awareness campaign to get more users to be risk aware and risk averse.

6.5.3. Assessing Factors Influencing Wi-Fi Security Implementations using PMT
Finding the exact location of Wireless Access Points (WAPs) to enable questionnaire distribution was difficult. Future researchers may want to invest in GPS devices that provide better mapping of objects of interest. Researchers may also need to consider a form of compensation that will influence more respondents to answer survey questionnaires. Respondents from this study were not very willing to participate in the study because they did not receive direct gains from it.

Another aspect that may be explored is the use of an online survey instrument since the target respondents are internet users. This may help reach more people.
REFERENCES


https://www.netresec.com/?page=Blog&tag=NetworkMiner


https://doi.org/10.1109/TMC.2010.121

https://doi.org/10.1109/HICSS.2012.620

https://doi.org/http://dx.doi.org/10.1036/1097-8542.802040

https://doi.org/10.1109/INCoS.2015.56

https://doi.org/10.1080/03637759209376276


https://doi.org/10.1109/JPROC.2016.2558521
APPENDICES

Appendix A: Cover Letter Accompanying Survey Questionnaire

Dear Respondent,

SUBJECT: LETTER FOR DATA COLLECTION

This is to certify that Janet Njeri Wachira of student identification number 631182 is a graduate student at the United States International University-Africa carrying out research on “Wi-Fi Security Implementation and User Awareness in Nairobi’s Central Business District.”. This is in fulfillment of the requirement of the Master of Information Systems Technology degree program.

You have been randomly selected to participate in this study.

It is estimated that it will take less than ten (10) minutes of your time to complete the questionnaire. Please respond as honestly and objectively as possible. Your participation is very essential for the accomplishment of this study and is highly appreciated.

Please note that any information you give will be treated confidentially and will be reported in collective terms and will not be personally identifiable to you.

Kindly spare some time to complete the attached questionnaire. Should you require any additional information regarding this study, do not hesitate to contact me.

Thank you for supporting her in her studies and for your prompt response.

Yours faithfully,

Paula Musuva-Kigen

Lecturer, School of Science and Technology

United States International University - Africa (USIU-A)

Phone: +254 20 3606152 | +254 20 3606554

Fax: +254 20 3606100
Appendix B: WI-FI SECURITY SURVEY

SECTION A: DEMOGRAPHIC DATA

1. What is your gender?
   □ Male  □ Female

2. What is your age?
   □ less than 18 years  □ 18 - 25 years  □ 26 - 35 years
   □ 36 - 45 years  □ 46 - 55 years  □ above 55 years

3. How would you rate your computer skills?
   □ Low (little or no skill; requiring a lot of assistance to perform tasks on a computer)
   □ Basic (I can navigate a computer and perform simple tasks such as print and respond to emails)
   □ Intermediate (in addition to basic tasks I can prepare and analyze data on spreadsheets, make presentations with little or no assistance)
   □ Advanced (in addition to intermediate tasks, I can change configuration settings, customize applications, backup and manage personal data)
   □ Expert (in addition to advanced tasks, I can write applications, audit and secure computer systems, troubleshoot and solve computer problems)

4. What category does your business fall under?
   □ Food and Beverages  □ Retail Store  □ Beauty  □ Health Care  □ Transportation
   □ Other: ____________________________

5. What is your job role?
   □ IT professional  □ Non - IT professional

6. How many people use your Wi-Fi network in a day?
   □ 1 - 20  □ 21 - 50  □ 51 - 100  □ 100 - 200  □ 200 - 300  □ More than 300

7. To what extent do you agree that your Wi-Fi network is used mostly for the following online services?

<table>
<thead>
<tr>
<th>ONLINE SERVICES</th>
<th>Strongly Disagree</th>
<th>Disagree</th>
<th>Neutral</th>
<th>Agree</th>
<th>Strongly Agree</th>
</tr>
</thead>
<tbody>
<tr>
<td>OS1 E-mail</td>
<td>1 2 3 4 5</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OS2 Social media</td>
<td>1 2 3 4 5</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OS3 Online shopping</td>
<td>1 2 3 4 5</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OS4 Online banking</td>
<td>1 2 3 4 5</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

SECTION B: THREAT APPRAISAL

To what extent do you agree with the following statements?

<table>
<thead>
<tr>
<th>PERCEIVED VULNERABILITY</th>
<th>Strongly Disagree</th>
<th>Disagree</th>
<th>Neutral</th>
<th>Agree</th>
<th>Strongly Agree</th>
</tr>
</thead>
<tbody>
<tr>
<td>PV1 Our Wi-Fi network could be subjected to a malicious hacking attempt</td>
<td>1 2 3 4 5</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PV2 We are at risk of becoming victims of an unsecured Wi-Fi network</td>
<td>1 2 3 4 5</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PV3 It is likely that we will experience Wi-Fi hacking incidents</td>
<td>1 2 3 4 5</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PV4 It is possible that we will experience Wi-Fi hacking incidents</td>
<td>1 2 3 4 5</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

87
### PERCEIVED SEVERITY

| PS1 | Having an unsecured Wi-Fi network poses a severe security risk to our network and its users | 1 | 2 | 3 | 4 | 5 |
| PS2 | Having an unsecured Wi-Fi network can enable remote access of sensitive data by third parties | 1 | 2 | 3 | 4 | 5 |
| PS3 | Having an unsecured Wi-Fi network can allow remote access to our mobile devices and computers | 1 | 2 | 3 | 4 | 5 |
| PS4 | I believe that the consequences of using an unsecured Wi-Fi network are severe. | 1 | 2 | 3 | 4 | 5 |
| PS5 | I believe that the consequences of using an unsecured Wi-Fi network can be serious. | 1 | 2 | 3 | 4 | 5 |
| PS6 | I believe that the consequences of using an unsecured Wi-Fi network can be significant. | 1 | 2 | 3 | 4 | 5 |

### REWARDS

| R1 | Securing our Wi-Fi network would be worthwhile to its users | 1 | 2 | 3 | 4 | 5 |
| R2 | Enabling security on our Wi-Fi network would provide gains to its users | 1 | 2 | 3 | 4 | 5 |
| R3 | Enabling security measures on our Wi-Fi network would be beneficial to its users | 1 | 2 | 3 | 4 | 5 |
| R4 | Securing our Wi-Fi network would be favorable to its users | 1 | 2 | 3 | 4 | 5 |

### SECTION C: COPING APPRAISAL

To what extent do you agree with the following statements?

### RESPONSE EFFICACY

| RE1 | Enabling security measures on our Wi-Fi network will prevent hackers from stealing network bandwidth | 1 | 2 | 3 | 4 | 5 |
| RE2 | Enabling the security measures on our Wi-Fi network is an effective way of deterring hacker attacks | 1 | 2 | 3 | 4 | 5 |
| RE3 | Enabling security measures on our Wi-Fi network will prevent hackers from gaining important personal/financial information | 1 | 2 | 3 | 4 | 5 |
| RE4 | Enabling security measures on our Wi-Fi network will prevent hackers from stealing my identity | 1 | 2 | 3 | 4 | 5 |

### SELF EFFICACY

| SE1 | It would be easy for us to enable security features on the Wi-Fi network | 1 | 2 | 3 | 4 | 5 |
| SE2 | We could enable Wi-Fi security measures if there was no-one around to tell us what to do | 1 | 2 | 3 | 4 | 5 |
| SE3 | We could enable Wi-Fi security measures if we only had manuals for reference | 1 | 2 | 3 | 4 | 5 |
| SE4 | We are able to set up Wi-Fi security features without much effort | 1 | 2 | 3 | 4 | 5 |
### RESPONSE COST

<table>
<thead>
<tr>
<th>RC1</th>
<th>The cost of enabling security measures on our Wi-Fi network would decrease its convenience</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>RC2</td>
<td>There are too many overheads associated with trying to enable security measures on our Wi-Fi network</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>RC3</td>
<td>Enabling security features on our Wi-Fi network would require considerable effort</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>RC4</td>
<td>Enabling security features on our Wi-Fi network would be time consuming</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
</tbody>
</table>

### VENDOR SUPPORT

<table>
<thead>
<tr>
<th>VS1</th>
<th>Our vendors provide support to help with the difficulties of setting up Wi-Fi security</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>VS2</td>
<td>Our vendors offer training on how to setup Wi-Fi security</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>VS3</td>
<td>Our vendors provide us with technical support for the Wi-Fi network</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
</tbody>
</table>

### PRESSURES

<table>
<thead>
<tr>
<th>P1</th>
<th>Our network users/customers believe we should have a secure Wi-Fi network</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>P2</td>
<td>Our network users require us to setup strong Wi-Fi security</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>P3</td>
<td>My colleagues think we should set up a secure Wi-Fi network</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>P4</td>
<td>My managers/supervisors require us to setup strong Wi-Fi security</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
</tbody>
</table>

### BEHAVIORAL INTENTION

<table>
<thead>
<tr>
<th>BI1</th>
<th>It has been our intention to setup a secure Wi-Fi network</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>BI2</td>
<td>It has been our intention to operate a secure Wi-Fi network</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>BI3</td>
<td>It has been our intention to protect the users of our Wi-Fi network from hacking attempts</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>BI4</td>
<td>We have always thought our Wi-Fi network was secure</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
</tbody>
</table>

### SECTION D: GENERAL FEEDBACK

Please describe other things that may have been relevant to this research on Wi-Fi Security

THANK YOU FOR TAKING TIME TO PARTICIPATE IN THIS RESEARCH