Extending Cognitive Fit Theory Towards Understanding Wireless Network Security Management in Small Organisations

K.Njenga and N.Manganyi

University of Johannesburg, Johannesburg, South Africa
e-mail: knjenga@uj.ac.za

Abstract

While large organisations effectively manage wireless network security through implementation of proper control procedures, anecdotal evidence suggest that smaller organisations lack such capacity (cognitive fit). The paper extends Cognitive Fit Theory as a theoretical lens towards understanding smaller organisations perceptions. In this paper we argue that the incapacity for small businesses to adequately deal with emergent wireless network security threats is as a result of a lack of match between understanding threats (problem representation) and how to mitigate against these threats (problem solving performance). The outcome of the paper is the development of a theoretical model that presents the perception of wireless network security threats from small organisations. The research takes specific focus on wireless network threats posed through war-driving under environments such as the 802.11x. From qualitative data analysis, empirical work confirms that smaller organisations *exhibited lack of cognitive fit,* in wireless network security management.

Keywords

Cognitive Fit, Wireless Network Security, Small Organisations

1. Introduction

Wireless computing technology is increasingly playing a major role in organisations (Varshney, 2003a). Many smaller organisations are becoming entirely dependent on the use of wireless network technologies for process level operations, while underestimating the consequences of security breaches (Loo, 2010). Empirical research suggests that it has been standard practice for large organisations to effectively manage and control the risk of wireless networks through implementing of proper control procedures. According to Bin, Yi-xian, Dong, Qi and Yang (2010), there are four main categories of research into wireless network security applicable to large organisations. These four categories of research depicted in Table 1, have provided large organisations with a framework for understanding and planning for best practice wireless network security (Bin *et al.,* 2010).

Category and Field	Classification
1. Research on standards for encryption key management	*Pre-distribution schemes, cryptography schemes, hash schemes, key infection schemes, and key management in hierarchy networks.*
2. Research on attacks and intrusion detection	*Managing awareness on external attacks and internal attacks on corporate networks.*
3. Research on standards for secure transmission of data across wireless networks	*Multi-path routing, reputation based schemes, secure routing for cluster or hierarchical sensor networks, broadcast authentication, secure routing defence against attacks.*
4. Research on identification of secure locations to place wireless access points	*Secure location scheme with beacons and secure location scheme without beacons.*

Table 1: Categories of Research for Wireless Network Security (Source: Bin *et al.*, 2010)

1.1. Small Organisations

Small organisations have been found to be lacking in applying frameworks such as listed above (cognitive fit for network security), in strict normative compliance when compared to their larger counterparts and often '*play-by-ear'* (Loo, 2010). In trying to understand why small organisations lack such fit, we use and extend Cognitive Fit Theory. The Theory of Cognitive Fit suggests that a match between the problem representation and the task results in a better problem solving performance. In this paper we argue that the incapacity for small businesses to adequately deal with emergent wireless network security threats is as a result of a lack of match between understanding wireless network security threats (problem representation) and how to mitigate against such threats (problem solving performance). The main research questions have therefore been outlined as follows:

a) To what extent do network security practitioners in small organisations understand problem representations? (Wireless network security threats); and
b) How does congruence in problem representation in small organisations affect problem solving performance? (Wireless network security threat mitigation).

In trying to address and discuss the context and objectives of the research, this paper divides itself into eight sections. Section 1 has introduced and laid context for the key theme. Section 2 discusses wireless networks and security management in the context of small South African organisations. The proceeding and penultimate sections (sections 3-7) discuss the research methodology, data analysis and nature of findings while the conclusion of this paper follows thereafter in section 8.

2. Wireless Networks

A wireless network refers to any kind of computer network that is wireless and associated with a telecommunication network. Generally, there are three main types of wireless networks technologies that include; wireless personal area networks (wPAN), wireless local area networks (wLAN) and wireless wide area networks (wWAN). Large and small organisations typically use wLAN networks to broadcast data using radio frequencies. There are standards for security defined by Institute of Electrical and Electronics Engineers (IEEE) such as the IEEE 802.11 that specifies "*over the air*" broadcasts between access points and clients. The IEEE specification for wLANs comprises several 802.11 specifications. These specifications represent the manner in which wireless networks communicate with a wireless access point (AP) and are depicted in Table 2 below.

Wireless LANs → / Characteristics ↓	802.11	802.11b	802.11a	802.11g
Spectrum	2.4 GHz	2.4 GHz	5 GHz	2.4 GHz
Maximum physical rate	2 Mbps	11 Mbps	54 Mbps	54 Mbps
Layer 3 data rate	1.2 Mbps	6-7 Mbps	32 Mbps	32 Mbps
Frequency selection	Frequency Hopping or Direct Sequence	Direct Sequence only	Orthogonal Frequency Division Multiplexing	OFDM
Compatible with	None	802.11	None	802.11 and 802.11b
Major advantage	Higher range	Widely deployed High range	Higher bit rate in a less crowded spectrum Smaller range	Higher bit rate in 2.4 GHz spectrum Higher range than 802.11a

Table 2: Multiple Versions of 802.11 (Source Varshney 2003b)

2.1. Wireless Network Security

Wireless network security is seen as a "*combination of physical, administrative and technical controls that ensure data is protected as it traverses broadcasted wireless networks"* (Loo, 2010). Wired Equivalent Privacy (WEP) is a security protocol designed to provide a wireless network that uses 802.11 with a level of security and privacy using encryption technology over data as it crosses wireless networks (Winget, Housley, Wagner, and Walker, 2003). WEP was introduced in 1997 to provide confidentiality. In WEP, data moving between computers and access points that apply 802.11x standards is encrypted using a 64 bit key algorithm (Winget *et. al.,* 2003). In 2001 cryptanalysts identified several WEP weaknesses. Despites its weakness, WEP is still widely used (Winget *et. al.,* 2003). Another security measure that is commonly being used and which eventually might supersede WEP due to inherent weaknesses is Wifi Protected Access (WPA). There are two versions of WPA namely WPA and WPA2 which are seen as the latest standard wireless network security measure that has rapidly gained acceptance with organisations.

2.2. Wireless Network Security Management in Small Organisations

There are various small organisations in South Africa that use wLANs for common business purposes. Security has often been a neglected attribute in small organisations and can be compromised through *war-driving* (Carter and Shumway, 2002; Loo, 2010). The act of war-driving typically resonates around driving around neighbourhoods searching weak wLAN security settings (particularly WEP use). The attacks range from trivialities such as accessing free internet to more serious issues that concern attacks on confidentiality and data integrity. *Wireshark* is an example of an application popularly used by hackers when *war-driving*. The application graphically displays access points and *ad-hoc* adapters in tabular format. It also detects the presence and/or use of Wired Equivalent Privacy (WEP) (Carter and Shumway, 2002).

3. Cognitive Fit and Wireless Network Security Management

Cognitive Fit Theory is a framework that assists in the understanding of relationships between information presented (problem representation) and how such information shapes problem-solving performance (Vessey, 1991). Cognitive Fit Theory posits that it is possible to model relationships between problem solving elements and problem-solving performance. These models can correspondingly be used to predict future problem-solving performance (Vessey, 1991). Within the domain of wireless network security, problem representation is seen as essential in influencing the management of wireless security networks which in turn shapes how threats are mitigated. We could argue that, the performance of a decision-making task such as threat mitigation in a wireless network using IT resources, will be enhanced and made effective if there is a cognitive fit between *internal and external problem representation on wireless network threats* and information required regarding wireless threat mitigation. We could further argue that larger organisations that exhibit cognitive fit, are organisations that are in a position to have information regarding wireless threats presented to them timely, and that information being both necessary and needed/required. This in turn will influence successful wireless network problem solving performance. We note that larger organisations are better placed to have the right information because these are financially endowed and are better placed to attract the right skills sets and procure the latest sets of technology. With the same reasoning we argue that small organisations lack such capacity, and lack the necessary resources to ensure that they have at their disposal, relevant *problem representation* regarding wireless threats that is needed at the right time. This argument is presented in Figure 1.

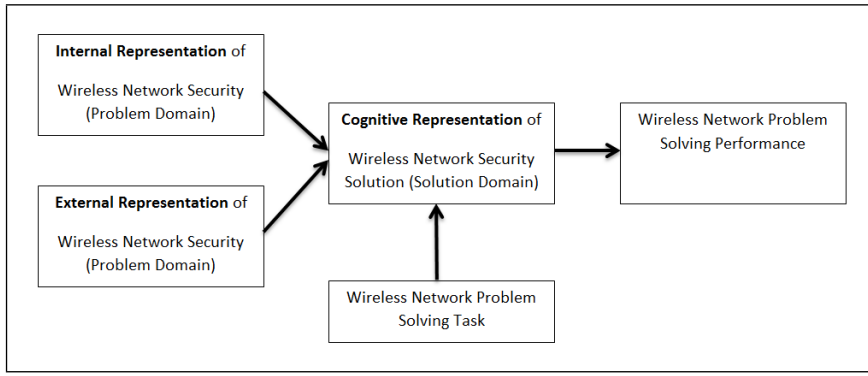

Figure 1: Cognitive Fit between problem representation and performance in Wireless Network Security, Adopted from Shaft and Vessey, (2006*)*

Underlying the reasoning in Figure 1, is the notion that, external (social, environmental and financial) and internal factors may shape the nature and value of problem representation which influences wireless network problem-solving performance. How small businesses perform will depend on Cognitive fit, (cognitive problem representation). In order to test the above model, a research was carried out. The next section explains the methodology and methods that underlie the extension of Cognitive Fit Theory into the Wireless Network Security domain.

4. Research Methodology

Welman, Kruger and Mitchel, (2007) define research as "*a systematic inquiry aimed at providing information to solve problems"* and differentiates between qualitative and quantitative research. Qualitative approach was the method chosen for the research to enable the understanding of congruence between problem representation of wireless network security threats and problem-solving performance within small organisations. Kaplan and Duchon (1988) define the qualitative approach as that which is an evolving process of data discovery, description and understanding. Kaplan and Duchon (1988) see qualitative research as an immersion in context. The research approach selected was the embedded case study (of 4 small organisations). The research aim was to gain knowledge by means of interviews, direct observation and testing. Direct observation is perceived as receiving knowledge of the outside world through senses or receiving of data using scientific instrument.

4.1. Data collection and Discussion

The first stage of the research involved interviews. From the interviews, was revealed on a number of cases selected that small organisations did not implement stringent wireless security (particularly WEP encryption). To confirm what was said during interviews the researchers observed wLAN settings using W*ireshark*. As an illustration, data from *wireshark* from a particular sampled region revealed more than **5** SSIDs being broadcasted as shown is Figure 2 below.

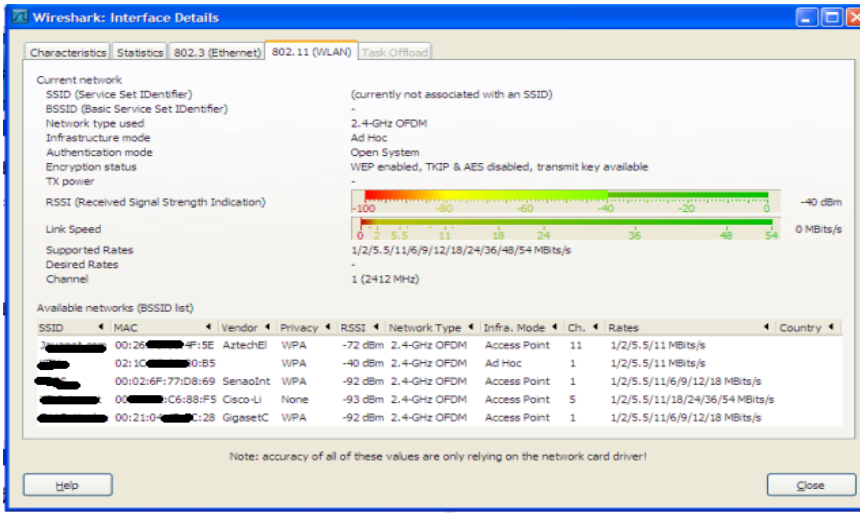

Figure 2: Wireshark data revealing one organisation with no Security

Figure 2 shows vendor names (SSIDs) being broadcasted and a quick review revealed the name of popular vendors. For most of these organisations the typical security and encryption standard was WPA. Figure 2 which hides the identity of the SSID for these organisations also shows one organisation ***with no encryption or security!*** A detailed review of how these small organisations perceive information *problem representation* is explained in the section below;

4.2. Organisation A

In organisation A, the SSID was not visible, (withheld) and the network required a password key. The organisation's WEP encryption was also not visible suggesting that the application could not pick the kind of security being used. This suggested that in this particular organisation, steps had been carried out to ensure that the network was secure. During the interview, assistant manager of this organisation [name withheld] said that "*they don't deal with information technology stuff*". The manager mentioned that they outsource from an organisation called [name withheld]. Whenever they have problems they report to this organisation. His honesty was revealed in the interview." *I will not be able to assist in anything to do with the wireless that we use, we never spend any time managing it because we outsource*". It remained clear for this specific organisation that any concern with security remained with third party providers. Outsourcing remains a popular option for some small organisations in Johannesburg, South Africa.

4.3. Organisation B

The interesting issue regarding organisation B was that *wireshark* picked that this organisation was still using its default SSID name "[name withheld]". It is a common practice for every organisation to change the default settings as soon wLAN is deployed. This was not the case for this organisation. On discussion with one of the interviewees, part of the reason for this was; "*We are a small health organisation,*

nobody would want to hack us". It can be noted that when third party vendors sold their product to this small organisation, they neglected to mention or explain possible risks and vulnerabilities of using wireless technologies that come along with such products and the actual costs and commitment involved in making these system usable and secure. When asked about wireless security concerns and the underlying security procedure and posture which governed them, the interviewee responded as follows;

> *"We don't govern [either] cyber security or wireless [security] in our organisation…"*
> *"Who would want to harm our [health] organisation?"*
> *"When it was installed we implemented WEP… why waste time in governing it when we could do something else that would benefit our [health] organisation?"*

On further prodding the interviewee revealed that they had no knowledge on how the wireless was configured or how it was to be protected.

4.4. Organisation C

This organisation (a coffee shop) happens to broadcast free internet on the basis that customers who want coffee can browse the Internet for free. The researcher parked outside this organisation in a car and could receive these free broadcast signals (without the requirement of an SSID password). *Wireshark* picked its wireless adapter and identified the SSID broadcasting as "*free public wifi*". The security issue here was that the shop was broadcasting beyond range making it easily available to non-patrons of the coffee shop. The researcher interviewed the owner and explained the concerns. The interviewee mentioned that they "*were testing the signal strength"*, and although they "*haven't restricted it*" they "*want to see how far it can go*". This did not make any sense to the researcher, since this was the very reason that would exposing this coffee shop and compromise its security. Possible risks could be outsiders browsing illegal sites or sites that infect its networks. Although a huge interest was shown by management towards this issue, it was clear that the management was not fully aware of the risks they were exposing the coffee shop to.

4.5. Organisation D

Organisation D remains a privately owned small organisation committed to promoting travel services for the Southern African region. Observation from this organisation revealed that they have set up stringent security measures on their wireless network. The SSID was not being picked up by *wireshark*. The interviewee was [name withheld] was the IT manager who described the network as "*a very small* network" in the sense that "*it has limited base station*", which uses standard technologies. Asked about the security management controls for wLAN, the interviewee responded that they "*don't have any formalised standards*". The interviewee mentioned that the IT department (which is fairly small) is the only department that "*knows the keys, there is no guest passwords [to network]*". Visitors that come in are allocated SSID passwords which are disabled when they leave. They

have certain user access requirement that define authorisation regarding "*who gets access [to networks] and who doesn't*". The interviewee also stated that they have deployed WAP2, and thought of it as being "*robust*". The interviewee also mentioned that they moved from WEP (encryption security) because "*it was very insecure and, it was so easy to break*". The interviewee also mentioned that they *"monitor performance*" and that "*If there is more traffic than usual on the network we will be able to see if something is wrong".* They followed the standard known ways of configuring the wireless network. Asked about familiarity with war-driving, the interviewee seemed particularly knowledgeable and said that "*we are aware of war driving*" and that is why "*we have the [made] wireless [networks] to be indoors and not high powered".* The interviewee recalled a while back of an instance when Google "*was going around picking up wirelesses*". The security measure as described by this interviewee was that "*apparently if you disable your SSID, it makes it hard for hackers to hack*". They also seemed to be aware of a lot of best practice procedure that was available online and have a network policy that was created by the human resource department to meet their business requirements.

4.6. Problem Representation and Problem-Solving Performance

Based on empirical results obtained from Organisations **A**,**B**, **C** and **D**, it was clear that the selected respondents lacked an understanding of wireless network threats they faced (*poor problem representation*). By interpreting *qualitative data*, it was observed that only one organization represented congruence regarding problem representation (wireless security networks threats) and problem solving performance (wireless security threat mitigation). The rest of the smaller organisations exhibited risk in terms of poor problem representation. In short, from interviews conducted, smaller organisations *exhibited lack of cognitive fit,* in wireless network security management. These findings above can be summarised in Table 3 below.

	Cognitive Representation regarding Wireless Network Security Risk					
	SSID Visibility is understood	Use of WEP *vis a vis* WAP/WAP2 is understood	Public use of Network resources is understood *e.g. access point location, broadcast range*	Risk of third party outsourcing is understood	Problem Representation and Tasks are in Congruence is understood	Technical Representation , use of Intrusion Detection Systems (IDS) is understood
	Problem representation	*Problem representation*	*Problem representation*	*Problem representation*	*Problem-solving performance*	*Problem-solving performance*
Org **A**	✔	✔	✔	*Risk*	*Risk*	*Risk*
Org **B**	*Risk*	✔	✔	*Risk*	*Risk*	*Risk*
Org **C**	*Risk*	✔	*Risk*	*Risk*	*Risk*	*Risk*
Org **D**	✔	✔	✔	✔	✔	*Risk*

Table 3: Problem Representation, Wireless network threats against Problem-solving performance

Based on the above findings a framework that extends Cognitive Fit Theory into wireless network security management can be developed. The next section expounds on this.

5. Framework for Managing Wireless Network Security for Small Organisations

From the discussions in the previous sections, it can be noted that the main deficiencies in perceptions held by small organisations is the lack of ***awareness***, ***effective planning*** and ***stringent security implementation***. Due to the highlighted problems facing small organisations, we note that these perceptions have tended to influence problem representation for such organisations, and correspondingly this has affected their problem-solving performance (Vessey 1991; Vessey 2006). From a theoretical viewpoint, Cognitive Fit Theory, suggest that network security practitioners and decision makers in small organisations who lack understanding about wireless network threats will have a slower response rate towards dealing with emergent network threats and this will limit further their capacity to provide adequate solutions to those threats. A framework of Cognitive Fit Theory can be extended to incorporate these empirical findings as follows.

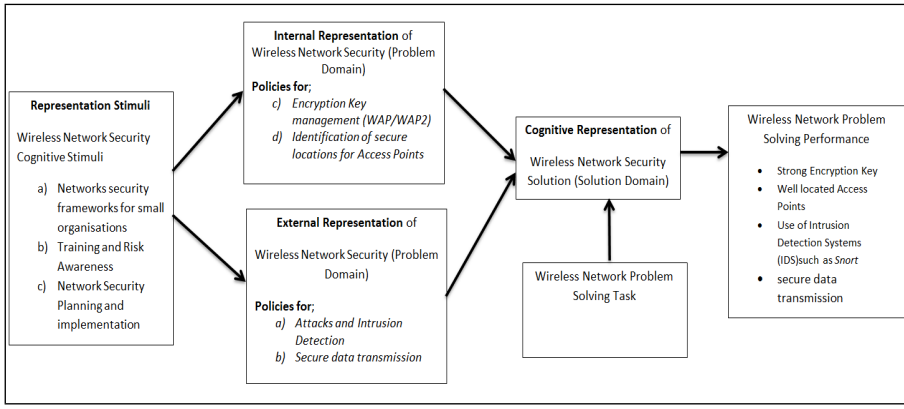

Figure 3: Extended Cognitive Fit Framework for Wireless Network Security for Small Organisations, Adopted from Shaft and Vessey (2006)

The framework presented by Figure 3 above is to be seen as further development of Cognitive Fit Theory and should provide a useful guide to small businesses that have implemented wireless network technologies. Based on Figure 3 above, it can be concluded that inferior problem representation can serve to influence problem solving performance. The aspects (***awareness***, ***effective planning*** and ***stringent security implementation***) embody what we will call "***representation stimuli***". This is the contribution to theory. We show that the correct representation stimuli will influence both internal and external problem representation for wireless network security that is bound to influence correct problem solving performance. We argue also that the converse also holds.

6. Conclusion

The research has raised concern about small organisations and the exposures and threats that these organisations face when they deploy wireless network systems. Lack of awareness regarding standard procedures for securing wireless systems has been noted to be a reason why small organisations constantly face threats to wireless

networks. These findings are also confirmed by the National Cyber Security Alliance, (NCSA) which has raised concerns about the public including organisations not being fully and completely aware of the dangers of not implementing and governing wireless security (Loo 2010). As a contribution, we have proposed and extended Cognitive Fit Theory as a suitable framework that provides insights in the way management and network practitioners' awareness is raised. The aims and results of the research has been to present small organisations with useful insights about how to manage wireless networks securely. The research supports the need for small organisations to stringently implement and continuously govern wireless networks using stated and accepted best practice procedures commonly used by security professionals in larger organisations. It is hoped that this work has provided insights that will instil a sense of responsibility to smaller organisations on how they should carry out wireless security and risk management. It is hoped that the work has achieved this intended outcome and adds value to small organisations.

7. Reference

Bin T., Yi-xian Y., Dong L., Qi L. and Yang, X., (2010), A security framework for wireless sensor networks, *The Journal of China Universities of Posts and Telecommunications Vol* 17:2 pp. 118–122.

Carter, B., and Shumway, R., (2002), *Wireless Security End-to-End*, Wiley Publishing Indianapolis, IN.

Kaplan, B. and Duchon, D., (1988), Combining Qualitative and Quantitative Methods in Information Systems Research: A Case Study, *Ninth Annual International Conference on Information Systems*, November 30-December 3, Minneapolis.

Loo AW. (2010) Illusion of Wireless Security, *Advances in Computers,* Vol 79 pp. 119-167.

Shaft, TM. and Vessey I., (2006), The Role of Cognitive Fit in the Relationship between Software Comprehension and Modification, *MIS Quarterly,* Vol 30:1, pp. 29-55.

Varshney, U., (2003a) Wireless I: Mobile And Wireless Information Systems: Applications, Networks, And Research Problem *Communications Of The Association For Information Systems* VoL 12 pp. 155-166.

Varshney, U., (2003b) The Status and Future of 802.11-based WLANs, *IEEE Computer*, Vol 36:6 pp. 90-93.

Vessey, I., (1991), Cognitive Fit: A Theory-Based Analysis of the Graphs Versus Tables Literature. *Decision Sciences* Vol 22:2 pp. 219-240.

Vessey, I. (2006), The theory of cognitive fit: One aspect of a general theory of problem solving, in P. Zhang and D. Galletta (eds.), *Human-computer interaction and management information systems: Foundations, Advances in Management Information Systems Series*, Armonk, NY

Welman, C., Kruger, F. & Mitchel, B., (2007), *Research Methodology*, 3rd Edition, Oxford University Press Southern Africa, Cape Town.

Winget, N R., Housley, D., Wagner, and Walker J., (2003), Security Flaws in 802.11 Data Link Protocols, *Communications of the ACM*, Vol 46:5 pp. 35-39.