The Effect of Using WLANs on Data Breaches: The Examination of the Moderating Role of Meaningful-Use Attestation

Emergent Research Forum papers

Dheyaaldin Alsalman
Dakota State University
Madison, SD 57042
Diya2060@hotmail.com

Insu Park
Dakota State University
Madison, SD 57042
Insu.park@dsu.edu

Abstract

Organizations have increasingly deployed wireless local area networks (WLANs) due to the benefits they can have such as mobility and flexibility. Unfortunately, the usage of wireless networks has raised many security concerns due to its capability of mobility. For instance, wireless networks are susceptible to many attacks such as eavesdropping, traffic analysis, data tampering and denial of service (DoS). Our study aims to identify a variable that moderates the effect of the usage of wireless local area networks (WLANs) on the occurrence of data breaches. Therefore, we propose a model that provides a basis for identifying the impact of meaningful-use attestation on the relationship between WLANs and the occurrence of healthcare data breaches. Our contribution is to extend existing research on security mechanisms of WLANs by empirically investigating the impact of meaningful-use attestation on the reduction of data breaches (hacking or malware) when using WLANs.

Keywords

Wireless local area networks (WLANs), meaningful-use attestation, hacking or malware breaches.

Introduction

Organizations have increasingly deployed wireless local area networks (WLANs) due to the benefits they can have such as mobility and flexibility. The importance of wireless local area networks (WLANs) has become popular because they provide users with much more freedom when accessing the network. Unlike the traditional wired local area network, users will be able to connect wirelessly by using a variety of compatible mobile devices such as laptop computers and handhelds (Agarwal & Wenye, 2005; Zeynep Gurkas, Zaim, & Aydin, 2006). Unfortunately, organizations cannot have all these advantages without dealing with many consequent security issues. The usage of wireless local area networks (WLANs) has raised many security concerns due to its capability of mobility. For instance, wireless networks are susceptible to many attacks such as eavesdropping, traffic analysis, data tampering and denial of service (DoS) (Agarwal & Wenye, 2005; Barka et al., 2006; Karnik & Passerini, 2005; Zeynep Gurkas et al., 2006).

In order to avoid most of these attacks, there have been many security mechanisms proposed by several research studies. These security mechanisms include three security protocols, which are the wired equivalent privacy (WEP), Wi-Fi protected access (WPA) and the (WPA2). Wired equivalent privacy (WEP) is a security feature that can overcome most of the security threats by encrypting data and preventing unauthorized access to the wireless network. According to previous studies, the wired equivalent privacy (WEP) has been known to be susceptible to many types of attacks. Also, the encryption provided by the wired equivalent privacy (WEP) was identified to be easy to crack by intruders (Arbaugh,

Shankar, Wan, & Kan, 2002; Barka et al., 2006). The Wi-Fi protected access (WPA) is an improved security mechanism that can provide reliable communication, enforce data integrity and apply stronger network access control, but still pose some threats and concerns such as encryption weaknesses. Therefore, the (WPA2) was launched in the early 2004, which eliminates most of the security flaws in the wired equivalent privacy (WEP) and the Wi-Fi protected access (WPA). With all these security mechanisms, wireless networks cannot be considered fully secure because most of its pitfalls are due to the lack of consistent configuration, implementation, and by human error (Karnik & Passerini, 2005).

Since wireless local area networks (WLANs) still pose security threats, data breaches could occur. Therefore, we aim to identify a variable that moderates the effect of the usage of wireless local area networks (WLANs) on the occurrence of data breaches. In this study, the moderating variable that will be used is meaningful-use attestation, which is an effective certification that requires healthcare providers to establish systematic procedures for improving clinical quality and ensuring privacy and security. To our knowledge, no empirical study has examined the effect of meaningful-use attestation on the relationship between the usage of wireless local area networks (WLANs) and the occurrence of healthcare data breaches. Therefore, we seek to answer the following questions: How does meaningful-use attestation influence the relationship between the usage of wireless local area networks (WLANs) and the occurrence of healthcare data breaches (i.e., hacking or malware)? Does meaningful-use attestation improve the security performance of using wireless local area networks (WLANs)? The overall goal of the current study is to examine the moderating role of meaningful-use attestation in the wireless network environment. Accordingly, we propose a model that provides a basis for identifying the impact of meaningful-use attestation on the relationship between wireless local area networks (WLANs) and the occurrence of healthcare data breaches in Figure 1.

Hypotheses Development

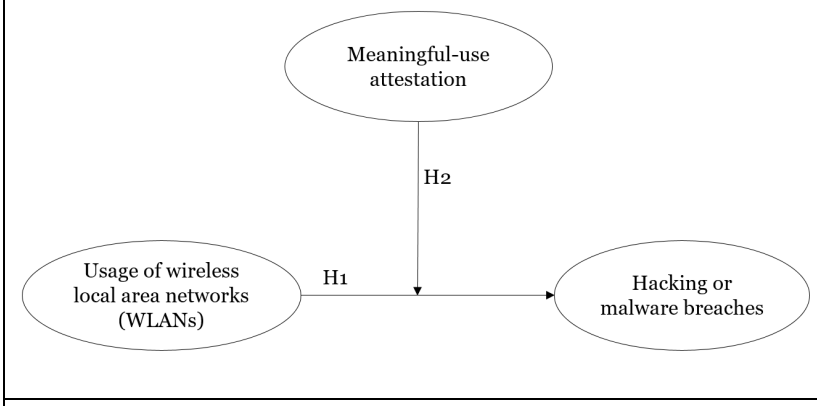

Figure 1. The Proposed Model

Wireless Local Area Networks and Data Breaches

The existing literature notes that WLAN is considered less secure than the wired LAN, which leads to privacy and security concerns (Elliott & Phillips, 2004; Green, Rosenbush, Crockett, & Holmes, 2003). Wireless local area networks (WLANs) have been implemented as an extension to the wired local area networks due to their capability of minimizing wired connections by transmitting and receiving the data over the air through using the radio frequency technology. Data sent over wireless LANs is quite literally broadcast for anyone to hear, which can be easily broken and compromised (Nicopolitidis, Pomportsis, Papadimitriou, & Obaidat, 2003). For instance, wired local area networks provide a probable entry point for outside intruders because of using broadband modem or gateway for internet access, otherwise wireless local area networks (WLANs) provide an easy point of entry for gaining access to the network. Since the medium of transmission is easily available outside the physical building, outside intruders can bypass the firewall by cracking the Wi-Fi key, which gives them an easy access to the private information inside the network (Patel, Ghaghda, & Nagecha, 2014). Furthermore, wireless network access points can be easily installed and very often connected to the wired network behind the company firewall, which

increases external hacking risks, especially for the company workstations that have no firewall capabilities (Von Solms & Marais, 2004). According to a case study, a wireless LAN audit was performed on the buildings of an organization while the 64-bit WEP encryption was enabled, and the SSID was not being broadcasted. They discovered that regardless of the secure configuration, the wireless LAN still creates easy entry points for outside intruders. They were able to capture packets and decrypt the WEP key by using a WLAN sniffer. They also discovered the SSID because the sniffer was able to capture it from frames that stations use when associating with an access point. Moreover, they illustrated that the footprint of this network makes it more convenient for attackers to collect enough packets to obtain the WEP key safely due to its well extension outside the buildings (Lo & Marchand, 2004). According to another case study in Malaysia, incidents reported to wireless threats such as web defacement or phishing websites due to the ease of acceptability to wireless networks. Because some wireless threats are in passive form such as sniffing, the end users were not aware that their privacy was compromised, therefore hackers can make those malicious activities more active and untraceable (Noor & Hassan, 2013).

In addition, wireless networks are susceptible to many attacks such as eavesdropping, traffic analysis, data tampering and denial of service (DoS). Eavesdropping is the possibility that the information being transmitted over the wireless networks could be intercepted by intruders. Traffic analysis is a process that enables intruders to gain information about data transmission and network activity. Data tampering is a description of the risk that wireless data can be captured and deleted during the course of transmission. Denial of service (DoS) is the possibility that attackers can block the entire frequency of the communication channel in order to disrupt access to the network (Agarwal & Wenye, 2005; Barka et al., 2006; Karnik & Passerini, 2005; Pan, 2012; Singh, Mishra, & Barwal, 2014; Zeynep Gurkas et al., 2006).

In summary, because the wireless local area network uses the radio frequency technology to transmit and receive data over the air and its footprint can be easily discovered due to its extension, we think that it will be the primary target for hackers to attack. Therefore, we expect that the occurrence of data breaches will be higher under the wireless local area network (WLAN) due to its various threats, especially passive attacks such as sniffing. So in order to examine the effect of wireless local area networks (WLANs) on the occurrence of healthcare data breaches, we specify a primary type of data breaches, which is hacking or malware. As we have mentioned before, wireless networks are susceptible to many attacks such as eavesdropping, traffic analysis, data tampering and denial of service (DoS). Based on these vulnerabilities, the usage of WLANs can pose hacking or malware breaches. Thus, we hypothesize:

Hypothesis 1: *Under the wireless local area network (WLAN), the occurrence of hacking or malware breaches will be higher than under the wired one.*

Meaningful-Use Attestation

Based on the economics literature, a moral hazard problem can occur due to the non-observability of effort, which results in an inefficiently low level of investment (Greene, 2003). According to previous studies, two possible approaches were suggested in order to encourage organizations to invest an appropriate high level of effort. The first approach is by reducing information asymmetry through certification schemes. The second approach is by increasing effort through incentive schemes (Baiman, Fischer, & Rajan, 2001; Balachandran & Radhakrishnan, 2005; Hwang, Radhakrishnan, & Su, 2006). Based on the theoretical background of moral hazards with certification and incentive schemes, our study will use meaningful-use attestation, which is an effective certification that requires healthcare providers to establish systematic procedures for improving clinical quality and ensuring privacy and security. Healthcare providers are mandated by meaningful-use attestation to conduct a security risk analysis in accordance with HIPAA Security Rule provisions. In addition, they are mandated to implement security updates as necessary and correct identified security deficiencies (Kwon & Johnson, 2014). According to the Centers for Medicare & Medicaid Services (CMS), meaningful-use attestation comes in a three-stage phased approach. Stage 1, which focuses on the protection of the confidentiality, integrity, and availability of electronic health information by requiring healthcare providers to implement administrative, physical and technical safeguards based on HIPAA Security Rule provisions. Stage 2, which expands meaningful-use criteria to advanced care processes with decision support. The last one is stage 3, which focuses on further improvements in quality, safety, and efficiency. Meaningful-use attestation can prevent common risk factors and reinforce security by requiring organizations to implement the standardized security risk analysis procedures under HIPAA. Meaningful-use attestation requires clear and standardized controls in

order to meet its standards for security risk analysis and internal assessment procedures. Based on these features, hospitals that have attested to meaningful-use would have a better performance of security in the usage of wireless local area networks (WLANs). In other words, hospitals with meaningful-use attestation will have a low level of data breaches when using wireless local area networks (WLANs). Therefore, we hypothesize the following:

Hypothesis 2: *The positive relationship between wireless local area network (WLAN) and hacking or malware breaches will be weakened with hospital's meaningful-use attestation.*

Proposed research method

Method

We will collect hospital data from the Healthcare Information and Management Systems Society (HIMSS) Analytics™ Database, which has been widely used in previous studies to examine the impact of healthcare information systems (Angst & Agarwal, 2009; Hillestad et al., 2005; Miller & Tucker, 2009). The database provides information about hospital meaningful-use attestation and wireless local area networks (WLANs). Our data will be limited to hospitals that are subject to Stage-1 meaningful-use and wireless local area network (WLAN). Data breaches will be collected from two sources, which are U.S. Health & Human Services (HHS) and Privacy Clearinghouse.

Wireless Local Area Networks (WLANs): In this study, the wireless local area network (WLAN) variable will be coded as one if a hospital adopted a wireless local area network and zero otherwise.

Meaningful-Use Attestation: In this study, the meaningful-use attestation will capture a hospital's formal attestation of Stage-1 meaningful-use. The meaningful-use attestation variable will be coded as one if a hospital achieved Stage-1 meaningful-use status and zero otherwise.

Data Breaches: Healthcare data breaches will stem from hacking or malware breaches. We will categorize data breaches into only one type (i.e., hacking or malware breaches) based on the actor who breached the data. The actor of each data breach will be recognized through the breach type provided by Privacy Clearinghouse and HHS. Hacking or malware breaches are described as any unauthorized electronic entry by an outsider, malware and spyware. Data breaches will be coded as one if a hospital had the breach and zero otherwise.

Data Analysis

In this study, we will use analysis of variance (ANOVA) for data analysis. The ANOVA approach is used to assess group differences on a single dependent variable. It provides the tools necessary to judge the observed effects (Hair, Black, Babin, Anderson, & Tatham, 2006). Since our study includes a single dependent variable and a single independent variable, we will apply One-Way ANOVA.

Conclusion and Contribution

The overall objective of this study is to answer our yet unanswered research question of whether meaningful-use attestation has an impact on the relationship between the usage of wireless local area networks (WLANs) and the occurrence of healthcare data breaches, which will then explain to us if meaningful-use attestation plays an important role in improving security performance when using WLANs in the healthcare sector. The findings of this study will contribute to extend existing research on security mechanisms of WLANs by empirically investigating the impact of meaningful-use attestation on the reduction of data breaches (hacking or malware) when using WLANs. By focusing on meaningful-use attestation, the current study addresses the gap in the literature concerning the security issues of WLANs and its relationship to the occurrence of data breaches. Overall, the main contribution of this research is to understand the role of meaningful-use attestation in the wireless environment, especially in terms of the performance of security in wireless local area networks (WLANs).

References

Agarwal, A. K., & Wenye, W. (2005, 3-7 Oct. 2005). *Measuring performance impact of security protocols in wireless local area networks*. Paper presented at the Broadband Networks, 2005. BroadNets 2005. 2nd International Conference on.

Angst, C. M., & Agarwal, R. (2009). Adoption of electronic health records in the presence of privacy concerns: The elaboration likelihood model and individual persuasion. *MIS quarterly, 33*(2), 339-370.

Arbaugh, W. A., Shankar, N., Wan, Y. C. J., & Kan, Z. (2002). Your 80211 wireless network has no clothes. *Wireless Communications, IEEE, 9*(6), 44-51. doi:10.1109/MWC.2002.1160080

Baiman, S., Fischer, P. E., & Rajan, M. V. (2001). Performance measurement and design in supply chains. *Management science, 47*(1), 173-188.

Balachandran, K. R., & Radhakrishnan, S. (2005). Quality implications of warranties in a supply chain. *Management science, 51*(8), 1266-1277.

Barka, E., Boulmalf, M., Alteniji, A., Al Suwaidi, H., Khazaimy, H., & Al Mansouri, M. (2006, Nov. 2006). *Impact of Security on the Performance of Wireless-Local Area Networks*. Paper presented at the Innovations in Information Technology, 2006.

Elliott, G., & Phillips, N. (2004). *Mobile commerce and wireless computing systems*: Pearson/Addison Wesley.

Green, H., Rosenbush, S., Crockett, R., & Holmes, S. (2003). Wi-Fi means business. *Business Week*, 44-50.

Greene, W. H. (2003). *Econometric analysis*: Pearson Education India.

Hair, J. F., Black, W. C., Babin, B. J., Anderson, R. E., & Tatham, R. L. (2006). *Multivariate data analysis* (Vol. 6): Pearson Prentice Hall Upper Saddle River, NJ.

Hillestad, R., Bigelow, J., Bower, A., Girosi, F., Meili, R., Scoville, R., & Taylor, R. (2005). Can electronic medical record systems transform health care? Potential health benefits, savings, and costs. *Health Affairs, 24*(5), 1103-1117.

Hwang, I., Radhakrishnan, S., & Su, L. (2006). Vendor certification and appraisal: Implications for supplier quality. *Management science, 52*(10), 1472-1482.

Karnik, A., & Passerini, K. (2005, April 28-30, 2005). *Wireless network security - a discussion from a business perspective*. Paper presented at the Wireless Telecommunications Symposium, 2005.

Kwon, J., & Johnson, M. E. (2014). *Meaningful Healthcare Security: Does "Meaningful-Use" Attestation Improve Information Security Performance?* Paper presented at the Workshop on the Economics of Information Security (WEIS), Penn State University.

Lo, E. C., & Marchand, M. (2004). *Security audit: a case study [information systems]*. Paper presented at the Electrical and Computer Engineering, 2004. Canadian Conference on.

Miller, A. R., & Tucker, C. (2009). Privacy protection and technology diffusion: The case of electronic medical records. *Management science, 55*(7), 1077-1093.

Nicopolitidis, P., Pomportsis, A., Papadimitriou, G. I., & Obaidat, M. S. (2003). *Wireless networks*: John Wiley & Sons, Inc.

Noor, M. M., & Hassan, W. H. (2013). Wireless networks: developments, threats and countermeasures. *International Journal of Digital Information and Wireless Communications (IJDIWC), 3*(1), 125-140.

Pan, F. (2012, 3-5 June 2012). *Wireless LAN security issues and solutions*. Paper presented at the Robotics and Applications (ISRA), 2012 IEEE Symposium on.

Patel, A., Ghaghda, S., & Nagecha, P. (2014). *Model for security in wired and wireless network for education*. Paper presented at the Computing for Sustainable Global Development (INDIACom), 2014 International Conference on.

Singh, P., Mishra, M., & Barwal, P. N. (2014, 27-28 Feb. 2014). *Analysis of security issues and their solutions in wireless LAN*. Paper presented at the Information Communication and Embedded Systems (ICICES), 2014 International Conference on.

Von Solms, B., & Marais, E. (2004). From secure wired networks to secure wireless networks–what are the extra risks? *computers & security, 23*(8), 633-637.

Zeynep Gurkas, G., Zaim, A. H., & Aydin, M. A. (2006, 0-0 0). *Security Mechanisms And Their Performance Impacts On Wireless Local Area Networks*. Paper presented at the Computer Networks, 2006 International Symposium on.