Chapter VII

Bringing Secure Wireless Technology to the Bedside: A Case Study of Two Canadian Healthcare Organizations

Dawn-Marie Turner, DM Turner Informatics Consulting Inc., Canada
Sunil Hazari, University of West Georgia, USA

Abstract

Wireless technology has broad implications for the healthcare environment. Despite its promise, this new technology has raised questions about security and privacy of sensitive data that is prevalent in healthcare organizations. All healthcare organizations are governed by legislation and regulations, and the implementation of enterprise applications using new technology is comparatively more difficult than in other industries. Using a configuration-idiographic case-study approach, this study investigated challenges faced by two Canadian healthcare organizations. In addition to interviews with management and staff of the organizations, a walk-through was

also conducted to observe and collect first-hand data of the implementation of wireless technology in the clinical environment. In the organizations under examination, it was found that wireless technology is being implemented gradually to augment the wired network. Problems associated with implementing wireless technology in these Canadian organizations are also discussed. Because of different standards in this technology, the two organizations are following different upgrade paths. Based on the data collected, best practices for secure wireless access in these organizations are proposed.

Introduction

Technology, the Internet, and healthcare reform are converging to change the healthcare environment and create a seamless integrated healthcare network. This seamless network will facilitate the flow of information from multiple sources to multiple healthcare providers, administrators, patients, and other support services 24 hours a day, seven days a week, among multiple sites (Masys & Baker, 1997). Implementing and managing such a network within the healthcare environment poses unique challenges. First, medical and health information is highly sensitive; therefore security and privacy of the information must be a top priority. Security and privacy in healthcare is governed by legislation and regulation. In Manitoba, this means the Personal Health Information Act (PHIA). PHIA specifies how medical information can be accessed, by whom, and for what purposes. It also states the security and privacy regulations for all health information systems used within the province. Second, unlike other industries, medical care is not delivered in the same place even by the same healthcare professional, necessitating the need for multiple access points (APs) for the same information. For example, a physician on rounds moves from one patient to another, each of whom may reside in a different room, necessitating the need for network access in each room to record and receive data and communicate with other needed services such as pharmacy or nursing.

The challenge in creating a seamless network in healthcare is how to provide information to multiple users at the point in which they will require the information to deliver effective patient care. A wireless network may offer the opportunity to meet this challenge and provide significant benefits to the healthcare system. A wireless local area network (WLAN) offers improved accuracy and efficiency for documenting nursing care, decreased preventable medication error through better point-of-care medication-administration systems, an increase in patient satisfaction, and efficiency in admission and discharge and other health administration processes (Sims, 2004). Additional technical benefits include lower costs, less cabling, availability of the network in locations not accessible with a wired connection, and the ability to adapt to growth easier.

The implementation of a WLAN is not without its challenges. Some challenges such as performance, speed, and accessibility are similar to those of a wired network, but others such as limited battery power of the devices, necessitating the need for an electrical source if the device is required for extended use; higher risk of equipment loss; and interference with medical equipment are unique to the WLAN environment (Karygiannis & Owens, 2002). Multiple standards and the fact that a WLAN does not usually replace a wired network but augments it increases the complexity of the management and compatibility of new systems (Drew, 2003). However, security is the biggest challenge facing a healthcare organization contemplating a wireless network. Wireless networks pose an increased risk of eavesdropping, hackers, and rogue devices (Sims, 2004). Securing a WLAN and the perception of its security may be one of the most limiting factors in the widespread use of WLAN in healthcare today (Campbell & Durigon, 2003).

Objectives of the Study

The objectives of this study were the following:

a. To gain an understanding of wireless-technology standards and their application within healthcare.
b. To articulate the security issues of wireless technologies within healthcare.
c. To identify the potential for best practice in the implementation of wireless technology in healthcare using a case-study methodology.

Wireless Technology in Healthcare

As the development and use of the electronic patient record progresses, mobile devices will become more common. Healthcare providers will begin to use these devices to access information previously only available in the paper-based chart or record. The increased use of wireless will help to stabilize wireless communication standards (Campbell & Durigon, 2003). Currently there are three standards used for wireless networking, wireless fidelity (Wi-Fi), mobile communications (cell phones), and Bluetooth. Wi-Fi was the standard used in the case studies in this research, therefore it is the standard discussed in this literature review.

The Wi-Fi standard encodes the data and then sends them over a selected channel using radio-wave frequencies. The connection is made through the use of a wireless network card within the device and a connection to an access point creating a wireless LAN. If the access point is connected directly to the corporate network or the Internet, the wireless user will have direct access to the corporate network or

Internet (Campbell & Durigon, 2003). The standard for Wi-Fi (802.11) has been established by the Institute of Electrical and Electronics Engineers (IEEE), a professional organization of engineers, students, and scientists. This standard (802.11) was the original standard set for wireless computing and established the protocols to be used between a wireless device and access point, or two wireless devices (Drew, 2003). Revisions and updates to 802.11 have resulted in several versions of the 802.11 standard. Prior to implementing WLAN, a healthcare organization needs to select the variation of the Wi-Fi standard it will use. Choosing which variation will depend on the data-transmission needs, cost, and the number of devices accessing the network. Three variations of the 802.11 standard currently being used by the case studies within this chapter will be discussed (802.11a, 802.11b, 802.11g).

Specification 802.11b, completed in 1999, is probably the most widely used standard. It is a physical-layer standard and operates in the 2.4 GHz frequency, providing users with 11Mbs throughput between the wireless device and the AP, depending on the distance between the device, the number of users, and any other interference. This standard has three available radio channels (Campbell & Durigon, 2003; Drew, 2003). One disadvantage to 802.11b is it operates in the same frequency as most medical devices such as ultrasound, sterilizers, and treatment or diagnostic devices. Therefore using a wireless device at this frequency requires all devices to be tested for potential interference with existing medical equipment sharing the same frequency, special consideration to the placement of the access nodes, and frequent retesting for possible interference.

Specification 802.11a also completed in 1999 provides users with a faster throughput at 54Mbs using the 5 GHz frequency spectrum. In addition to its faster throughput, 802.11a offers two advantages over 802.11b. First, the 5 GHz frequency is not shared by other commonly used devices such as microwaves, cellular phones, and medical monitoring equipment, making interference from these devices less of an issue. Second, 802.11a opens more channels, making the network more available; with eight vs. three channels, it offers better protection against possible interference from neighboring access points (Campbell & Durigon, 2003). However, its disadvantage is the need for more access points because the higher throughput is gained at the cost of a shorter transmission distance, making 802.11a more expensive to implement, something that must be considered when choosing which standard to use. 802.11a is also not backward compatible. This means a healthcare organization that has already implemented a wireless network using 802.11b must replace their access nodes for compatibility with 802.11a. One solution for this is the use of dual-band access points that are certified to work with 802.11b and 802.11a, allowing organizations to leverage existing technology when upgrading to the new standard (Karygiannis & Owens, 2002). The newest standard, 802.11g, was developed in 2001 as a direct result of the compatibility issues between 802.11b and 802.11a. It provides the throughput of 802.11a but is backward compatible with 802.11b (Campbell & Durigon). As such, organizations that have already invested

in 802.11b technologies without the use of dual-band access points can upgrade to the new standard without the expense of new hardware.

Authentication is a very important component for healthcare organizations. It refers to the ability to verify the identity of client stations or individuals accessing health data over a network, and deny access to those not providing the correct electronic credentials. The Wired Equivalent Privacy (WEP) protocol defines two types of authentication: open-system and shared-key authentication. Open-key authentication is not a true authentication process because it only requires a one-way channel. Access points using open-system authentication will accept a mobile device on the basis of it having a media access control (MAC) address and does not verify if it is an authenticated address within the network. Shared-key authentication requires a two-way interchange between the access point and the device based on cryptography. In this scenario, the client requesting access to the WLAN sends a message to the access point, and the access point responds with a challenge to the client requesting it to identify itself using its special key. The access point then decrypts the message and if it matches the values allowed, the client is authenticated to the network. The WEP protocol only requires open-system authentication, creating a potential security risk if shared-key authentication is not also implemented within the organization (Newman, 2003). The need for authentication of wireless devices within a healthcare facility is extremely important because of the number of transient population (e.g., patients, visitors) that has the potential to tap into the health information network and have access to sensitive patient records.

Confidentiality or privacy refers to protecting the data from eavesdropping either intentionally or unintentionally through cryptographic techniques. (Privacy issues in healthcare are discussed later.) The WEP protocol uses the Rivest Cipher 4 (RC4) symmetric key, stream cipher algorithm to generate a pseudo-random data sequence supporting a 40-bit encryption for the shared key. This is a weak encryption system and on a busy network could be cracked in a matter of hours (Sims, 2004). Integrity ensures messages sent are not modified during transmission. The service was developed to reject any messages that appeared to have been modified during transmission. The technique used within the WEP is "a simple encrypted cyclic redundancy check (CRC) approach that after sealing the packet encrypts it for transmission where on receipt of the packet, it is decrypted and compared to the original. If they are not equal, an error message is sent. Unfortunately, CRC, unlike a hash code or message authentication code, is not cryptographically secure. Although the WEP provides security services, it is clear they are not sufficient to provide the level of security required for the sensitive information being transmitted within a healthcare institution (Berghel & Uecker, 2005).

It appears clear from this discussion that standards alone will not create a secure network, and controls are also needed. Controls are the mechanisms that reduce or eliminate threats to the organization's computer systems and network (Fitzgerald & Dennis, 2002). There are typically three types of controls. Preventative controls,

as the name implies, prevents or mitigates the chance of a security breach such as the use of passwords and locking the computer equipment (such as those located in areas like nursing stations and administrative offices). Detective controls are those strategies and mechanisms used to identify when a security breach has occurred such as identifying when an unknown address has tried to gain entry (such as by implementing an intrusion-detection system on the hospital's internal network). Detection controls usually include reporting and may include an alarm function to alert network personnel of potential threats. Corrective controls correct or fix an unwanted event or threat. Controls should be used to develop specific countermeasures to address the vulnerabilities with using a WLAN. The application of specific countermeasures minimizes the risks to create a more secure network. As with wired networks, risks cannot be completely eliminated, but through the appropriate application of countermeasures and the use of controls, risk can be reduced to a level that is acceptable to the organization. Countermeasures can be divided into three broad areas: management, operational, and software.

Management countermeasures usually focus on the preventative level. They start with a comprehensive security policy outlining such things as who has access to the network, authorization levels, the installation of access points, configuration management, and the reporting of loss or stolen wireless devices. In Manitoba, the security policy must also include a signed confidentiality agreement between the user and the organization outlining what constitutes a breach and the consequences of any breaches.

Operational countermeasures offer both preventative and detection controls. These include the physical security measures taken to ensure only authorized personnel have access to the devices and networks through such things as identification badges, locking the equipment, security guards and video cameras, the use of passwords or biometrics, and the use of site survey tools for mapping access points and ensuring coverage remains within the intended range. It should also include logging and auditing of all accesses and attempted access to the network to identify if unauthorized use has occurred.

Technical countermeasures include the use of software and hardware to protect the network such as proper access-point configurations, software patches and upgrades, authentication, intrusion-detection systems, encryption, the use of a virtual private network (VPN), firewalls, and public-key infrastructure (PKI). The use of a VPN within a wireless network can afford the same level of protection it does within the wired environment. Like in a wired environment, a VPN creates an encrypted secure channel between the user's wireless device and the network, thus hiding the transmission (Kilpatrick, 2003). A firewall is one of the most formidable lines of system defense because it prevents unauthorized users and creates an invisible wall to potential intruders (Campbell & Durigon, 2003; Derba & Siegal, 2003). The goal is to ensure that only authorized individuals are able to view an individual's healthcare record.

Implementing a wireless network in any healthcare environment should be considered carefully with a clear business need. It must also consider the highly sensitive nature of the information being transmitted coupled with the risk of any potential breach of the system. Once the decision has been made to implement wireless, a careful assessment of capabilities must be matched to the goals and objectives for the wireless network. Only then can related decisions about standards, hardware, and software be made.

Privacy Issues in Healthcare

The significance of information privacy will continue to escalate in proportion to the value of information (Rust, Kannan, & Peng, 2002). Information privacy in healthcare organizations is related to information security. It is important to note that an organization may have information security without privacy, but it is not possible to have privacy without having information security controls (preventative, detective, or corrective as discussed earlier). While wireless technology offers convenience and potential that shows promise for improving healthcare delivery, the right to privacy for patients must be protected. In wireless transmission, data is not being confined to a physical medium so that it remains secure when being transmitted from node to node. Therefore, it is necessary that healthcare organizations should develop and implement system security and privacy strategies to protect data and information stored in research and clinical databases. According to Huston (2001), confidentiality and security of a patient's health information has always been important, and with the ease of access afforded electronically, security will likely be more difficult to provide without advanced planning.

As healthcare organizations move toward converting paper-based records and communication processes to digital formats that can be easily stored and manipulated for administrative decision making, intranets and extranets are established within and outside the boundaries of the healthcare organization. There needs to be a strategic aspect to maintaining security, privacy, and standardization of networks that carry data and information within and outside the organization. A common example is the use of a networked decision-support system that is specially developed for supporting decision making related to the solution of a particular healthcare-management problem (Turban, 1993). This type of system ties in with centralized databases so effectively, controls need to be present in these databases to ensure confidentiality, integrity, and availability of data.

Government regulations (e.g., PHIA in Canada, and HIPAA [Health Insurance Portability and Accountability Act] in USA) have provided guidelines to healthcare organizations to maintain privacy and security aspects of the transmission and maintenance of patient records. Healthcare organizations previously outsourced services such as transcriptions, which made it possible to identify patient data. Regulations

Implementing a wireless network in any healthcare environment should be considered carefully with a clear business need. It must also consider the highly sensitive nature of the information being transmitted coupled with the risk of any potential breach of the system. Once the decision has been made to implement wireless, a careful assessment of capabilities must be matched to the goals and objectives for the wireless network. Only then can related decisions about standards, hardware, and software be made.

Privacy Issues in Healthcare

The significance of information privacy will continue to escalate in proportion to the value of information (Rust, Kannan, & Peng, 2002). Information privacy in healthcare organizations is related to information security. It is important to note that an organization may have information security without privacy, but it is not possible to have privacy without having information security controls (preventative, detective, or corrective as discussed earlier). While wireless technology offers convenience and potential that shows promise for improving healthcare delivery, the right to privacy for patients must be protected. In wireless transmission, data is not being confined to a physical medium so that it remains secure when being transmitted from node to node. Therefore, it is necessary that healthcare organizations should develop and implement system security and privacy strategies to protect data and information stored in research and clinical databases. According to Huston (2001), confidentiality and security of a patient's health information has always been important, and with the ease of access afforded electronically, security will likely be more difficult to provide without advanced planning.

As healthcare organizations move toward converting paper-based records and communication processes to digital formats that can be easily stored and manipulated for administrative decision making, intranets and extranets are established within and outside the boundaries of the healthcare organization. There needs to be a strategic aspect to maintaining security, privacy, and standardization of networks that carry data and information within and outside the organization. A common example is the use of a networked decision-support system that is specially developed for supporting decision making related to the solution of a particular healthcare-management problem (Turban, 1993). This type of system ties in with centralized databases so effectively, controls need to be present in these databases to ensure confidentiality, integrity, and availability of data.

Government regulations (e.g., PHIA in Canada, and HIPAA [Health Insurance Portability and Accountability Act] in USA) have provided guidelines to healthcare organizations to maintain privacy and security aspects of the transmission and maintenance of patient records. Healthcare organizations previously outsourced services such as transcriptions, which made it possible to identify patient data. Regulations

now hold providers responsible for auditing policies and procedures of contracted firms (Walker & Spencer, 2000). This was done in an effort to safeguard the privacy of patient data. Similarly, policies and procedures for handling patient data that were previously written for the "paper world" are being revised to comply with electronic storage, access, sharing, and transmission of data (Shortell & Kaluzny, 1994).

Methodology

The case study is a widely used method of qualitative research within information systems and is an effective design for understanding the organizational context of information-technology innovations. A case study is defined as "an empirical enquiry that investigates a contemporary phenomenon within its real-life context, especially when the boundaries between phenomenon and context are not clearly evident and it relies on multiple sources of evidence" (Darke, Shanks, & Broadbent, 1998, p. 273). Case-study research is often used to describe, test, or develop theory. This type of case-study research is called the configuration-idiographic study, which is used to describe events and their circumstances to identify relationships but not necessarily generate theoretical interpretations (Smith, 1990). As the purpose of this study was explanatory, case selection was based on the available cases offering the greatest explanatory power.

Two midsize healthcare organizations in Canada using a WLAN were approached and agreed to participate in the case study. Both organizations provide inpatient and outpatient treatment facilities and clinics. One organization's WLAN extended beyond the physical boundaries of the institution, enabling wireless access to the corporate network in two satellite facilities approximately 2 to 5 km away. Interviews were conducted using a semi-structured interview format with one or all of the following personnel: the network manager, and IT security and systems analysts. The interview questions were developed to identify the characteristics of the network and current practices used to secure the organization's wireless network and devices. In addition to the interviews, a walk-through was conducted at one of the sites to view the wireless device within the clinical environment.

The interview questions from each case study were analyzed using a qualitative inductive approach. The goal of this approach was to explore and analyze existing practices of the organizations within the context of recommendations, practices, and standards identified in the literature. There was no effort made to quantify results or compare one organization with the other. The responses to the interview questions were analyzed to answer each of the research questions. Responses to the first research question were assessed against the three primary wireless threats (identified in the literature): malicious hackers, eavesdropping (war driving), and

now hold providers responsible for auditing policies and procedures of contracted firms (Walker & Spencer, 2000). This was done in an effort to safeguard the privacy of patient data. Similarly, policies and procedures for handling patient data that were previously written for the "paper world" are being revised to comply with electronic storage, access, sharing, and transmission of data (Shortell & Kaluzny, 1994).

Methodology

The case study is a widely used method of qualitative research within information systems and is an effective design for understanding the organizational context of information-technology innovations. A case study is defined as "an empirical enquiry that investigates a contemporary phenomenon within its real-life context, especially when the boundaries between phenomenon and context are not clearly evident and it relies on multiple sources of evidence" (Darke, Shanks, & Broadbent, 1998, p. 273). Case-study research is often used to describe, test, or develop theory. This type of case-study research is called the configuration-idiographic study, which is used to describe events and their circumstances to identify relationships but not necessarily generate theoretical interpretations (Smith, 1990). As the purpose of this study was explanatory, case selection was based on the available cases offering the greatest explanatory power.

Two midsize healthcare organizations in Canada using a WLAN were approached and agreed to participate in the case study. Both organizations provide inpatient and outpatient treatment facilities and clinics. One organization's WLAN extended beyond the physical boundaries of the institution, enabling wireless access to the corporate network in two satellite facilities approximately 2 to 5 km away. Interviews were conducted using a semi-structured interview format with one or all of the following personnel: the network manager, and IT security and systems analysts. The interview questions were developed to identify the characteristics of the network and current practices used to secure the organization's wireless network and devices. In addition to the interviews, a walk-through was conducted at one of the sites to view the wireless device within the clinical environment.

The interview questions from each case study were analyzed using a qualitative inductive approach. The goal of this approach was to explore and analyze existing practices of the organizations within the context of recommendations, practices, and standards identified in the literature. There was no effort made to quantify results or compare one organization with the other. The responses to the interview questions were analyzed to answer each of the research questions. Responses to the first research question were assessed against the three primary wireless threats (identified in the literature): malicious hackers, eavesdropping (war driving), and

rogue wireless devices. Best practice was assessed using the National Institute of Standards and Technology (NIST) steps for a secure wireless LAN and the fit with current organizational practices to these recommendations. Data was also collected to assess the rationale for selecting wireless technology, the current standard implemented, and the location of wireless within the organization. These areas were not categorized but will be discussed.

Findings

Both organizations in the case study indicated wireless was not a stand-alone network but augmented the existing wired network to provide healthcare professionals with point-of-care access to patients' electronic records housed on the corporate network. Wireless was also implemented to reduce overall costs and ease the management of providing point-of-care access because the wireless technology allowed multiple users to use the same equipment vs. requiring the purchasing of a laptop for each user. Additionally, IEEE 802.11b was the current standard within both organizations. However, future upgrades were split with one organization choosing to upgrade to 802.11a and the other choosing 802.11g. An increased volume of users in one organization was the rationale for the planned upgrade to 802.11a. Although prior implementation of dual-band access nodes meant compatibility with the existing network was not an issue, the increased cost due to the greater number of required access nodes was slowing down the rate of growth. The need for higher transmission rates and compatibility with the existing WLAN was the second organization's rationale for upgrading to 802.11g.

In both organizations, interference with medical equipment was a consideration and required all wireless devices to be tested for compatibility by the biomedical engineering department. Although no issues were found in either organization, one organization had implemented a policy that dictated wireless devices were not permitted in areas with highly critical medical monitoring equipment such as the intensive care units. Each organization identified their first step in securing wireless for healthcare was to enable security within the wireless standard, usually WEP. However, it was identified that this level of security was not enough as one network specialist indicated: "It is not enough to use the security that comes with the system. You need to layer your security; the default settings are not secure enough."

Securing and protecting the wireless network from eavesdropping, malicious hackers, and rogue devices or access points was approached in both organizations from four perspectives: securing the wireless network, securing the device, protecting the data, and protecting the larger corporate network. Securing the wireless network was accomplished through the configuration of the MAC addresses requiring authentication to the network (access nodes will only talk to addresses they know), and hiding the name of the network was also done through the configuration. As

one organization indicated, this means "anyone scanning for a network might still find it, but because they don't know its name, it will be inaccessible." In addition to authentication of the MAC address, one organization installed a firewall between the WLAN and the corporate network; the firewall actively scanned the airwaves for unrecognized MAC addresses and when it detected something, it sent a warning that unidentified addresses had attempted access to the system. Additionally, the firewall provided the organization with end-to-end 128-bit encryption and authentication between the WLAN and the corporate network. Furthermore, protection of the network was provided through software monitor switches that looked for and detected unauthorized access nodes. Unauthorized nodes were immediately removed and the organization maintains a strict policy regarding the installation of unapproved access points.

Securing the devices was accomplished in both organizations first through a security policy that specified who could use a wireless device, what authorization level they had, and what their access level was. Second, each device was inventoried and a hardware log was maintained. Finally, the devices themselves were secured. Both organizations in this study use computers on wheels (COWS) as the wireless devices. These are laptop computers secured to a cart or mobile station allowing for easy movement within the organization, but making it difficult to remove from the property. Consideration was given to the use of other wireless devices such as personal digital assistants (PDAs); however, these were considered to pose an increased security risk due to their lack of direct connectivity to the network and the need to store personal health information (even temporarily) on the device. As one organization noted, "When personal health information resides on the device, the loss or theft of a device jeopardizes the confidentiality of the information stored on that device." The storage of personal health information on the device even for a short time also prevented real-time access to information by the health professional. The need to synch the device created a time lag between when the device recorded the information and when it is was entered into the network and available to another healthcare professional.

Protecting health and medical information residing on the corporate network was done through enhanced 128-bit encryption that was centrally controlled and configured for end-to-end data encryption. As one network manager stated, "We made the assumption that people may break in, so we make the data stream unreadable…essentially they get garbage." One organization also indicated the wireless network is treated as a hostile environment, therefore without the proper authentication; even someone that manages to get into the wireless network cannot access the corporate network. As indicated previously, authentication was a two step process, authenticating first to the wireless network and then to the LAN. Finally, access to the corporate network in both organizations was role based as defined by PHIA, giving access to the corporate network only to the level required for the user to deliver safe patient care.