Chapter 8

Wireless Network Security

Winnipeg Regional Health Authority and Manitoba eHealth

Manitoba Lotteries Corporation

Executive Management
Carol Bellringer
Mala Sachdeva

Principal
Doug Harold

Table of contents

Main points

What we examined

Our audit examined the security of wireless networking solutions within Manitoba eHealth (eHealth) and Manitoba Lotteries Corporation (MLC).

Through enquiry we noted that the central Provincial Government does not use wireless networks. However, many of the organizations in the Government Reporting Entity do. We selected 2 such organizations handling sensitive data for our review.

Our audit program and assessment criteria were based on internationally recognized standards including CoBIT – (Control Objectives for Information and related Technology) issued by ISACA and the 802.11i standard issued by the Institute of Electrical and Electronics Engineers (IEEE).

Why it matters

The use of mobile devices and wireless networks has increased dramatically over the past decade. This growth can be attributed to wireless devices becoming progressively smaller, cheaper and more powerful. Nearly all new smartphones, tablets, netbooks and laptops come preconfigured with wireless networking capability. Wireless networks offer tremendous benefits to homeowners and businesses.

What is often overlooked, however, is that a wireless network has many more vulnerabilities than a traditional wired network. By their very nature, wireless transmissions can travel well beyond the walls of a house or business. This significantly increases the complexity and importance of securing those wireless signals. An unauthorized individual no longer needs to gain physical access to the inside of an organization to maliciously connect to a network.

Attacks against wireless networks are costly in terms of the time an organization needs to resolve the incident and the potential financial losses and damages incurred. While it may seem like a daunting task to ensure the security of a wireless network, it can be done. Organizations need to be aware of the risks that wireless networks and equipment can pose and adopt a comprehensive risk management strategy to effectively address them. This strategy must include processes whereby new threats and vulnerabilities are tracked, identified and mitigated. Failure to do so will leave an organization with a false sense of security, unaware of the true risks presented by using this technology.

What we found

Despite many examples of good practices, we found weaknesses that need to be addressed to protect the wireless networks. We provided our detailed findings to both eHealth and MLC to enable them to remedy all of the weaknesses we encountered. We also provided our findings for eHealth to the Winnipeg Regional Health Authority (WRHA) because eHealth is administratively housed there. Our findings were that:

- Wireless risks are identified, but not managed effectively over time
- Information technology security policies do not exist at eHealth; and exist, but are not current, at MLC
- Wireless security policies do not exist
- Network security controls need improvement
- Access point configuration standards need improvement
- Wireless client device configuration standards need improvement
- Wireless monitoring is not performed
- Wireless network administrators require additional training
- Security awareness training is lacking at eHealth.

Background

eHealth

In 2006, Treasury Board approved the establishment of eHealth. The program facilitates the healthcare delivery transformation through the use of Information and Communication Technology (ICT) for health system users in Manitoba. Wireless security issues and compliance with the Province of Manitoba`s *Personal Health Information Act* (PHIA) and its regulations are of significance.

eHealth's mandate is to provide a single integrated organization capable of delivering province-wide solutions under the direction of a Manitoba eHealth Program Council to:

- Integrate health systems across regions and healthcare sectors
- Improve and expand health services by managing ICT to achieve economies-of-scale
- Improve the efficiency and effectiveness of ICT services
- Creating reliable and secure connections to the Department of Health.

eHealth reports to the Deputy Minister of Health through a Provincial Program Council that is composed of senior executives of the major stakeholders. This includes representation from regional health authorities, CancerCare Manitoba, Diagnostic Services of Manitoba and Manitoba Health.

The eHealth program is managed by a Chief Information Officer (CIO) that reports directly to the WRHA Chief Operating Officer & VP Long Term Care and Community Health Services.

After formal establishment, eHealth inherited and consolidated numerous diverse IT systems and applications from sites within the WRHA. This included the existing legacy wireless networks. An Infrastructure Strategy plan was developed in order to migrate towards a more cost effective and sustainable enterprise IT architecture.

The eHealth Information Security program consists of 5 pillars:

- Information security governance
- Risk management
- Incident management
- Configuration and change management
- Education and training.

An enterprise security architecture has been designed based upon the Sherwood Applied Business Security Architecture (SABSA). This is a risk-based, business-driven architecture that develops security controls to meet the needs of the business. The architecture incorporates strict logical and physical zoning requirements.

eHealth is operating in a sector which has made the natural transition to wireless networks due to the tremendous benefit of mobility that wireless devices offer. Doctors, nurses and other healthcare professionals rely on networked information systems. In fact, many medical devices themselves have become networked in order to send and receive critical heath data within the healthcare environment.

While wireless security vulnerabilities present risks to any network, the risks are magnified in healthcare. A patient record used to be an actual paper document that could be adequately protected by physical security controls. Today, personal health information is being stored electronically, which increases the risk of security and privacy breaches. The WRHA, operating as the host for the Manitoba eHealth program, is considered the trustee and as such is responsible for requirements in the following areas:

- Written security policy and procedures
- Access restrictions and other precautions
- Additional safeguards for electronic health information systems
- Authorized access for employees and agents
- Orientation and training for employees
- Audit.

Manitoba Lotteries Corporation (MLC)

"Under the authority of 207(1)(a) of The Criminal Code of Canada and Manitoba Lotteries Corporation Act, MLC manages and conducts provincial gaming including:

- *Casino Gaming (table games and slot machines) at Club Regent, McPhillips Street Station, Aseneskak and South Beach Casinos**
- *VLTs*
- *Ticket Games (e.g., Lotto 6/49 and scratch tickets) which are administered by Western Canada Lottery Corporation*

**By agreement, Aseneskak and South Beach Casinos (registered by the MGCC as gaming operators), provide premises, employees and equipment and, meet provincially-set casino operating standards. (Source: Manitoba Gaming Commission website)*

MLC is a Crown corporation, reporting to the Minister responsible for The Manitoba Lotteries Corporation Act through a Board of Directors. The Board sets corporate policy for the corporation and provides strategic direction to the CEO and senior executives, who are responsible for business operations."

(Source: www.mlc.mb.ca)

Cheating, theft, and fraud from both customers and employees are some of the traditional threats that casinos face. The increased reliance on networked gaming solutions and the introduction of Player Reward systems make MLC a potential target of cyber-criminals.

Personal information, patron gambling history, and facial recognition data are examples of the sensitive data that MLC handles on a daily basis. MLC has developed a Privacy Policy and Privacy Compliance Standard. Both have been implemented to ensure the protection of all information collected, used, disclosed, or stored by MLC.

Wireless Local Area Networks – General information

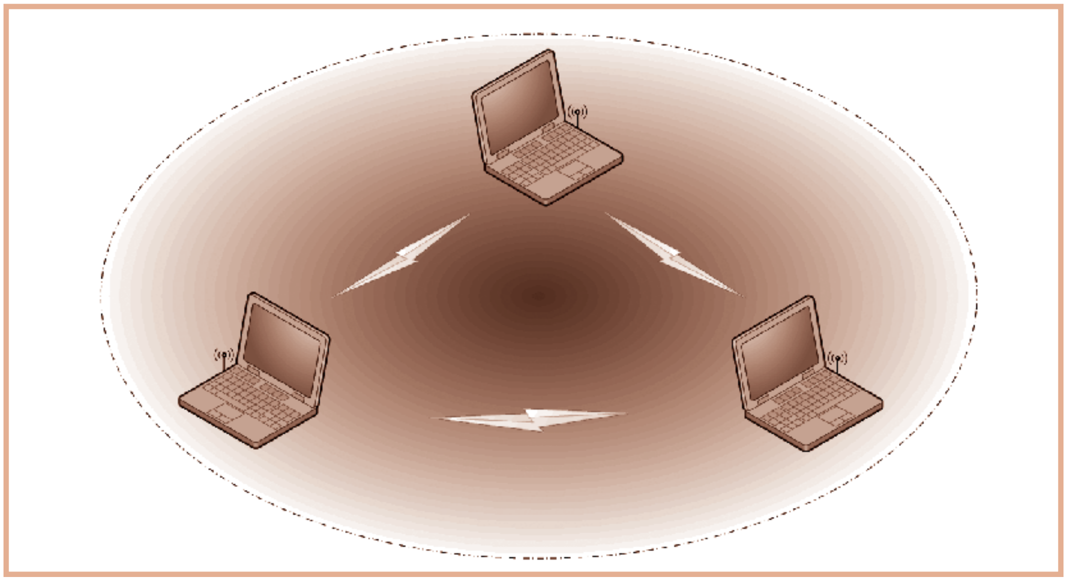
Wireless Local Area Networks (WLANs) use Radio Frequency (RF) technology for transferring data. Often referred to as "Wi-Fi" networks, they complement existing computer networks by providing mobility to end users. In 1997, The Institute of Electrical and Electronics Engineers (IEEE) established a working group (802.11) that defines the standards for these networks. While there are numerous different wireless standards (listed alphabetically), the most commonly used are: 802.11a, 802.11b, 802.11g and the new 802.11n standard. Predominantly, WLANs are configured in two different modes:

- Ad Hoc Mode
- Infrastructure Mode

Ad Hoc Mode

An Ad Hoc Mode wireless network (**Figure 1**) has no "access points" (AP). Client devices communicate with each other through their wireless interfaces. This mode is primarily used for data transfers and printing. There are increased risks associated with using this mode. If a user is connected to the corporate network and is configured to allow ad hoc networking, an attacker could connect to the user's wireless station and then attempt to use this connection to gain a foothold to the internal network. Given this risk, industry standards recommend that organizations establish and enforce a comprehensive wireless security policy that prohibits ad hoc networks unless there is a specific business requirement that has been supported by an up-to-date risk assessment.

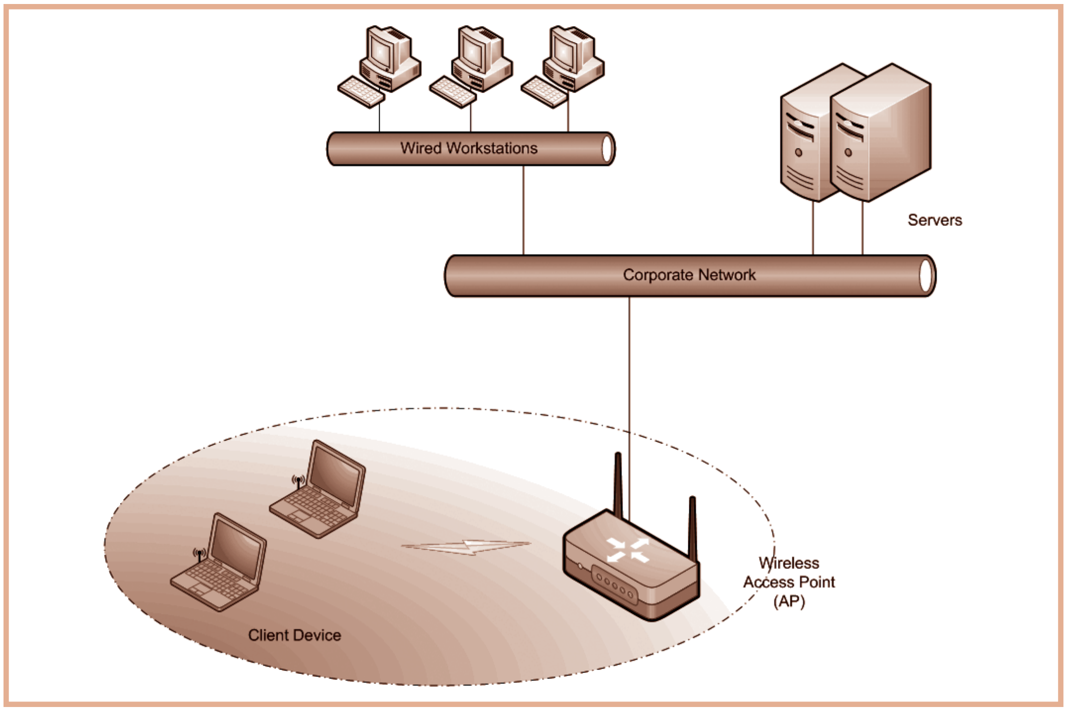
Figure 1: Ad hoc Mode



Infrastructure Mode

Infrastructure Mode (**Figure 2**) is the most common implementation of a wireless LAN. It requires an AP and at least one client device (i.e., laptop). The AP connects a number of wireless devices with a wired network giving the wireless client access to the network.

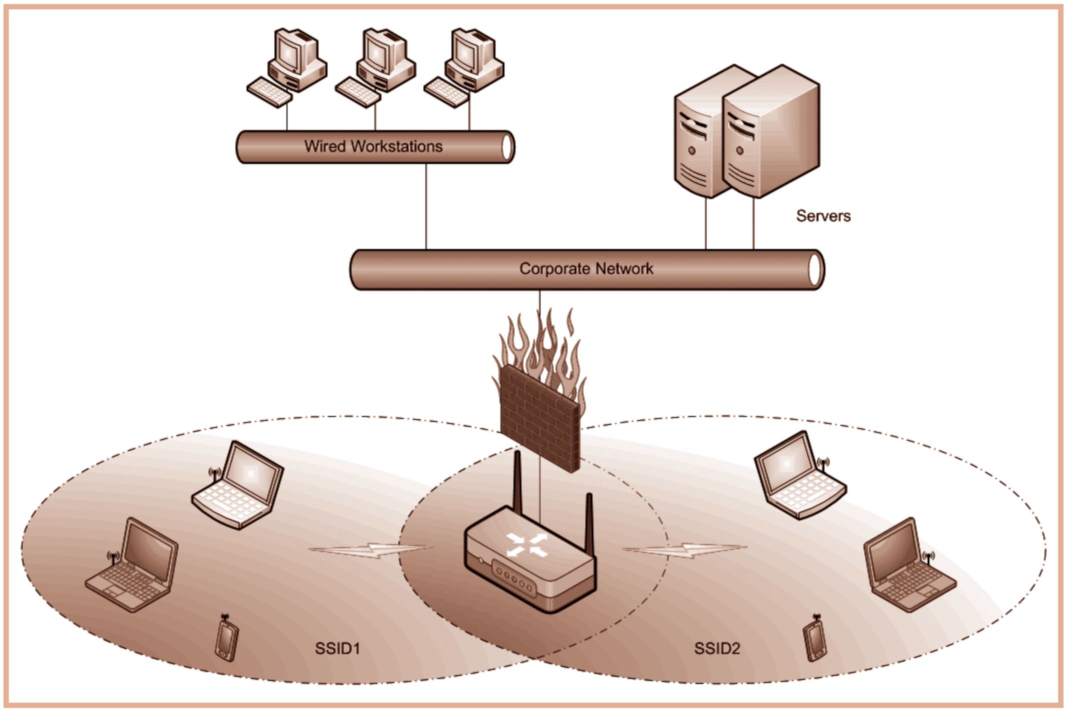
Figure 2: Infrastructure Mode



Many vendor enterprise wireless APs can host several Service Set Identifiers (SSIDs). An SSID is the name of the wireless network. Even though each SSID appears and acts as if it is an independent wireless network, in many cases, several different SSIDs could be using the same infrastructure (**Figure 3**). Each SSID can have its own authentication and encryption protocols assigned to them. Effective network security controls are critical. Wireless security is only as strong as the weakest link.

Throughout this audit, we examined both organizations' Infrastructure Mode architecture.

Figure 3: Shared WLAN infrastructure



Wireless threats

Most users are not aware of the wide variety of threats and associated risk of using this technology. National Institute of Standards and Technology (NIST) outlines common wireless threats, as noted in **Figure 4**.

Figure 4: Wireless threats

Denial of service	Attacker prevents or limits the normal use or management of networks or network devices.
Eavesdropping	Attacker passively monitors network communications for data, including authentication credentials.
Man-in-the-middle	Attacker actively impersonates multiple legitimate parties, such as appearing as a client to an AP and appearing as an AP to a client. Allows attacker to intercept communications between an AP and a client, thereby obtaining authentication credentials and data.
Masquerading	Attacker impersonates an authorized user and gains certain unauthorized privileges.
Message modification	Attacker alters a legitimate message by deleting, adding to, changing, or reordering it.
Message replay	Attacker passively monitors transmissions and retransmits messages, acting as if the attacker were a legitimate user.
Misappropriation	Attacker steals or makes unauthorized use of a service.
Traffic analysis	Attacker passively monitors transmissions to identify communication patterns and participants.

Source: From NIST 800-48 Rev1

Wireless radio waves are extremely vulnerable to undetected interception and exploitation. Attackers and security researchers are constantly discovering new vulnerabilities and ways to attack wireless networks and clients.

Rogue wireless devices can significantly threaten the overall security of an organization. The most common threat is a device that has been deployed by an authorized user who does not appreciate the severity of their actions. While this may increase the user's productivity, an outside attacker could use that rogue AP as a point of entry into the network, and avoid all perimeter security controls.

Information security involves protecting the confidentiality, integrity and availability of systems. The confidentiality and integrity of corporate wireless information remains a primary concern. However, reliance on wireless technologies for critical services could potentially present some of an organization's greatest risks. As most wireless networks operate in the unlicensed frequency band, the equipment could suffer interference from numerous sources (i.e., microwave ovens, cordless telephones, Bluetooth devices, or even a deliberate Denial of Service attack). This could disrupt access to critical services and should be an important consideration before adopting wireless solutions.

WLAN security basics

Wireless networks are more complex than their wired equivalent. Not only do the wireless devices need to send and receive the data, there is a tremendous amount of additional overhead associated with data synchronization, confidentiality, and integrity of each packet of information. One of the major challenges that organizations face is simply trying to understand the numerous technical and complex encryption and authentication protocols that are required to secure wireless transmissions.

The key for any organization is to select the appropriate encryption and authentication protocols based upon a thorough requirements and risk assessment. As well, both the wireless infrastructure and client devices must be configured to industry standards.

Audit scope and approach

Our objective was to assess the security of wireless networking solutions within eHealth and MLC. While many wireless audits focus primarily on the technical encryption and authentication standards used, we took a more holistic approach. Effective wireless security cannot simply rely on technical security solutions. Wireless networks are merely extensions of internal networks and share most network security controls. Therefore, policies, procedures and processes are equally important. As such, we assessed whether these 2 organizations have:

- Processes to identify wireless risks and monitor any changes to them
- A high-level organizational IT Security Policy
- A comprehensive Wireless Security Policy
- Robust network security controls
- Current wireless AP configuration standards
- Current client configuration standards
- An established wireless monitoring program
- Fully trained wireless network administrators
- Annual user awareness training.

We did not examine other wireless technologies such as WiMax, Bluetooth, and Radio-Frequency Identification (RFID). Also, we did not audit for compliance with PHIA and its regulations. However, several of the PHIA requirements are similar to our audit objectives.

Our examination was performed in accordance with the value-for-money auditing standards recommended by the Canadian Institute of Chartered Accountants. We included tests and other procedures necessary to obtain sufficient and appropriate evidence to support our conclusions. Our audit program and assessment criteria were based on Control Objectives for Information and related Technology (CoBIT), Establishing Wireless Robust Security Networks: a Guide to IEEE 802.11 issued by NIST, and the Wireless Security Baseline from the Center for Internet Security.

We carried out our procedures for eHealth at their main offices, their primary and secondary data centres, and 1 other building location. Our audit of MLC included corporate headquarters, Club Regent and McPhillips Street Station casinos, and an MLC warehouse.

At the beginning of each audit, we conducted an in-depth technical wireless assessment from the outside of selected buildings. This external "war-driving" style assessment was conducted using free readily available software and inexpensive wireless equipment. This simulated the capabilities available to today's wireless attackers. We used methodologies and techniques developed from SANS GIAC Assessing and Auditing Wireless Networks course (www.sans.org). This information was corroborated using commercial wireless assessment software. Internal technical scanning was also performed in order to validate system configurations and to determine if there were any rogue AP.

All high risk findings were immediately reported to senior management. A confidential technical findings document was presented to each organization and the eHealth report was also provided to the WRHA. These documents contain technical and sensitive findings that, until properly addressed, would increase the risk of network compromise to these organizations. Therefore, these findings are not included within this report. Our Office will follow up with both organizations in order to ensure they have adequately addressed these findings.

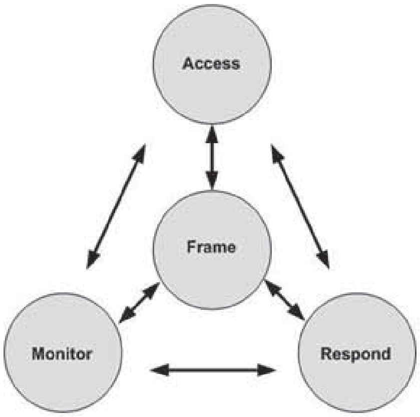
Audit findings and recommendations

1. Wireless risks are identified, but not managed effectively over time

Organizational risk can include many different types of risk. Security risk related to the operation and use of information systems is a risk that senior management must address as part of their corporate risk management responsibilities.

Risk management is a comprehensive process that requires an organization to:

- Frame risk (i.e., establish the context for risk-based decisions)
- Assess risk
- Respond to risk once determined
- Monitor risk on an on-going basis using effective organizational communications and a feedback loop for continuous improvement in the risk-related activities of organizations.



Source: (ref. NIST 800-39)

Not only do organizations need to assess wireless risks, but they also need to monitor and manage them over time. New vulnerabilities that affect wireless infrastructures are frequently discovered.

> *"Remember that because systems degrade and the environment changes over time, risk management must be considered a continuous process that requires the commitment, involvement and support of the organization's senior executives and board of directors."* (2011 Coach Guidelines for the Protection of Healthcare Information)

Many organizations perform initial risk assessments when implementing wireless networking projects. However, once the wireless network is operational, they neglect to monitor changes. Failure to track changes to threats and new vulnerabilities significantly increases an organization's overall risk. Many legacy wireless networks used Wired Equivalent Protocol (WEP) as a security protocol. This decision would have been supported by a thorough risk assessment. WEP has since been proven to be flawed and ineffective leaving these networks extremely vulnerable to attack. Some of these same organizations are still using WEP today because they do not have the processes in place to monitor the changes to their wireless risk.

eHealth

eHealth has adopted the Royal Canadian Mounted Police Harmonized Threat and Risk Assessment (HTRA) methodology. This risk assessment framework is used by federal departments particularly those that manage extremely sensitive and classified data. An HTRA is completed for each new IT project.

Wireless risks were identified and addressed when the wireless systems were initially installed. However, eHealth has not managed these risks appropriately since then. Some wireless networks were installed in 2004 and the risks have not been reassessed since. We determined that there are no established processes for managing changes to the threats and vulnerabilities of wireless networks within eHealth.

Recommendation 1: We recommend that eHealth conduct a current wireless risk assessment. All residual risk should be reduced and formally accepted by senior management.

Recommendation 2: We recommend that eHealth develop processes to effectively identify and manage changes to threats and vulnerabilities to all IT systems, including wireless networks.

MLC

MLC has implemented a comprehensive Enterprise Risk Management (ERM) framework that has aligned strategy, people, processes and knowledge to better understand its threats. They have dedicated risk management staff members that assess risk and document them in corporate Risk Registers. MLC has formalized a strategic approach to managing risk.

A wireless Risk Register was completed prior to the installation of the wireless networks. However, we determined that MLC has not established a formal process for monitoring changes to these risks.

Recommendation 3: We recommend that MLC develop processes to effectively identify and manage changes to threats and vulnerabilities to all IT systems, including wireless networks.

2. Information technology security policies do not exist at eHealth; and exist, but are not current, at MLC

A formally documented and communicated information technology (IT) security policy is an essential component of a successful information security program. The single greatest threat to information security is the lack of awareness and understanding of the threats that commonly exist. Senior management approval, end user education, and a general awareness program for the information security policies and standards are essential to the success of an information security program. The IT security policy provides management direction and support for information security.

This policy should include a statement of direction from senior management supporting the goals and principles of information security. It should outline the minimum security requirements for the protection of the confidentiality, integrity, and availability of information systems. It should also clearly define information security, associated responsibilities and accountabilities.

Without a formal up-to-date IT security policy, there is an increased risk that IT security objectives will not be properly aligned with business needs, critical IT assets and healthcare/business data may not be properly protected, and security practices may not be consistent with applicable laws and regulations.

All employees should be required to sign off on their understanding of the information security policy at the time they are hired. The information security policy should be reviewed at planned intervals to ensure it is still suitable, effective and adequate.

eHealth

We began our audit by investigating the wireless networks used and operated by eHealth. Our expectation was that these systems were for eHealth corporate use. It quickly became evident that eHealth, in addition to their provincial electronic health record mandate, provides the entire technical support function for the WRHA. The wireless networks we examined were, in fact, being used by the WRHA.

After contacting WRHA, we determined that they did not have an overarching IT security policy.

We acknowledge that, at the time of our audit, eHealth had a draft IT security directive in development. This draft directive, however, would not be adequate as it would have only been applicable to eHealth employees.

Recommendation 4: We recommend that WRHA develop, approve and enforce a comprehensive, overarching IT security policy.

MLC

We found that MLC had an existing IT security policy. This policy had been signed by the CEO and is a part of the organization's overall corporate policy framework. All of the organization's other IT policies and procedures refer to this document. MLC's "top-down" commitment to information security is evident.

New MLC employees must read all information security policies and formally sign a form acknowledging their receipt. We tested this process and found no exceptions.

However, all MLC IT security policies, including the main IT security policy, were originally signed in 2005. There have been no documented reviews or updates to these policies since then.

Recommendation 5: We recommend that MLC review all information security policies on a regular basis. This review should be formally documented and any changes effectively communicated to all staff.

3. Wireless security policies do not exist

A wireless security policy is the cornerstone for articulating the enterprise wireless philosophy. It should highlight senior management commitment to protecting the enterprise from wireless risks and govern how wireless technology will be used within the organization. It should clearly dictate management expectations of wireless users.

This policy should be ratified by senior management and be made available to all individuals who use the organization's wireless networks. It should be reviewed at planned intervals and revised to take into account changes to risk assessments, privacy assessments, vulnerability assessments, and privacy laws (Federal and Provincial). Changes to this policy must be documented, approved and communicated to all staff.

This policy should:

- Acknowledge the risks associated with using wireless networking
- Outline organizational roles and responsibilities
- Ensure that all wireless networking solutions undergo a formal risk assessment. This risk assessment must be reviewed annually to account for new threats and vulnerabilities

- Ensure that the highest level of authentication and encryption are used based upon a formal wireless risk assessment
- List authorized systems and/or data classification that have been approved for use on the wireless infrastructure
- Outline Acceptable Use and employee responsibilities
- Prohibit adhoc wireless networking (unless authorized by senior management)
- Ensure that only authorized users connect to wireless networks
- Ensure that only approved wireless user devices connect to wireless networks
- Ensure that wireless user devices are securely configured. This configuration must be approved by senior management
- Detail wireless monitoring procedures
- Detail wireless incident handling procedures.

eHealth

Corporate policies must be all encompassing and applicable to every employee. Therefore we make this recommendation to the WRHA since the wireless networks are installed throughout the entire organization.

We noted that WRHA does not have a wireless security policy. eHealth has developed a wireless security standard that does include some aspects of the expected policy statements. However, it does not meet the intent of this criteria.

> **Recommendation 6:** We recommend that WRHA develop, approve and enforce a comprehensive wireless security policy.

MLC

Similarly, MLC has not developed a wireless security policy. While MLC staff clearly understand many of the principles that would be outlined within, the policy must be formalized, presented and enforced within the entire organization.

> **Recommendation 7:** We recommend that MLC develop, approve and enforce a comprehensive wireless security policy.

4. Network security controls need improvement

All of eHealth and MLC business functions rely heavily upon reliable and secure network operations. Network Security is an important consideration for every organization particularly when implementing wireless network solutions.

Adequate and effective network security controls must be implemented to protect corporate systems and data. Organizations must adopt an in-depth defence model where multiple countermeasures are layered throughout the infrastructure to address the wide variety of vulnerabilities and attacks.

Our initial focus was to ensure that the connection between the wireless and wired infrastructure was secure. However, given the shared security services involved, our assessment included a more comprehensive assessment of the organization's:

- Network security architecture
- Firewall architecture and configuration
- Intrusion detection/prevention capabilities
- Anti-malware capabilities
- Access controls
- Account management processes
- Physical security measures
- Security log management
- Incident handling procedures
- Patch management procedures.

We found that both eHealth and MLC had implemented multifaceted, industry standard enterprise security architectures. These architectures have incorporated numerous layers of security. Both organizations have strong firewall architectures positioned effectively within their networks. These firewalls not only protect the organization from external threats, but they also provide additional protection of their internal data centers where sensitive corporate and healthcare information is stored.

eHealth has adopted IT Infrastructure Library (ITIL) as a service management framework. ITIL is a public framework that outlines best practices of IT service management. By adopting these processes, eHealth has shown a strong commitment in becoming a healthcare service provider and not simply an IT management organization. Strong change management, incident management, problem management, and release management processes were evident. An integral aspect of ITIL is Information Security Management (ISM). These ISM functions have greatly assisted with the development of eHealth's Enterprise Security Architecture.

We provided both organizations with findings that outline areas for improvement. Given the detailed technical nature and sensitivity of these particular findings, they are not presented within this document. Our office will follow up with both organizations in order to ensure they have adequately addressed these findings.

Recommendation 8: We recommend that eHealth address our findings in the area of Network Security Controls.

Recommendation 9: We recommend that MLC address our findings in the area of Network Security Controls.

5. Access point configuration standards need improvement

Properly configuring corporate wireless APs is arguably one of the most critical components in effectively securing a wireless infrastructure. There are numerous methods and standards that can be selected to authenticate wireless users and encrypt the information sent.

Corporate standards need to be developed that enforce the most secure authentication and encryption protocols. These standards should be supported by a current risk assessment. Organizations must ensure that all security patches associated with the wireless infrastructure are identified and applied as soon as possible. Failure to implement these patches in a timely fashion significantly increases the risk of a wireless network compromise.

Once the approved standards have been implemented, they should be validated by an independent technical security evaluation to ensure they are properly implemented and effective.

One important consideration in developing the AP configuration standards is signal strength. Wireless networks are designed to provide maximum coverage and speed to their clients. This can result in signals being transmitted great distances outside of an organization. An attacker, sitting in his car in the parking lot or even a nearby home or business, can attempt to compromise the network. Without this exposed signal, the attacker would need to gain physical access to the building or get extremely close to the building where detective controls (i.e., monitored security cameras) could mitigate the risk.

During our technical assessment of both organizations we observed tremendous signal leakage. We detected wireless signals at distances beyond the physical boundaries of each facility we examined. We found that these signals extended into many adjacent residential and commercial properties.

Both eHealth and MLC outsourced the installation of their physical wireless AP antennas. These contracts did not include an expectation that the contractor would attempt to minimize signal leakage. Antenna power settings can be reduced and directional antennas deployed to ensure the wireless signal is directed towards the interior of the building.

While strong encryption and authentication are certainly more effective in reducing overall wireless risks, the distance a wireless signals travel outside of an organization should not be overlooked. Organizations must understand this risk and strike a balance between optimum WLAN coverage and minimizing signal leakage. In the event that there is a new vulnerability discovered in the current authentication and encryption methods, excessive signal leakage would drastically increase the organization's exposure.

eHealth

eHealth supports 7 different wireless networks. All of these WLANs operate on the same shared wireless infrastructure. During the initial exterior technical scan, we noted that the main eHealth corporate wireless network was using a weak legacy authentication protocol LEAP (Lightweight Extensible Authentication Protocol) in addition to their more robust authentication protocol. Fortunately the majority of wireless users were not using this weak authentication protocol and it was only minimally used. Due to the severity and potential risks in using LEAP, we immediately contacted eHealth senior staff and this configuration error was corrected.

During the technical scanning portion of the eHealth Secondary Data Centre, we noted that the hospital pharmacy network was using the very insecure Wired Equivalent Protocol (WEP). This information system automates the medication refill process to help ensure the right medication is getting to the right medical station. Once again, we contacted eHealth and reported this finding. eHealth technicians immediately reconfigured the network to a more secure configuration.

> *"WEP is viewed as insufficient for securing all forms of clinical communications. In short, WEP should not be used in any modern healthcare organization due to the security risks it creates."* (CISCO Medical-Grade Networks (MGN) 2.0 – Wireless Architectures)

Recommendation 10: We recommend that eHealth address our findings in the area of Access Point configuration standards.

MLC

MLC maintains and operates 4 wireless networks. All of these WLANs operate on the same enterprise wireless infrastructure. The main Lotteries wireless business network is configured to use the very secure authentication and encryption protocols. MLC provides wireless access to guests to provide internet access in the multipurpose rooms at the casinos or at the MLC corporate offices. Guest wireless internet access is not provided in any gaming areas within the MLC. We determined that this network is sufficiently and securely segmented from the internal corporate network.

The findings from our technical assessments were presented to both organizations. We consider these findings sensitive, and if disclosed, would increase the risk of network compromise to these organizations. They are therefore not included within this report. Our office will follow up with both organizations in order to ensure they have adequately addressed these findings.

Recommendation 11: We recommend that MLC address our findings in the area of Access Point configuration standards.

6. Wireless client device configuration standards need improvement

Wireless security expert Joshua Wright has stated: Whether attacking or auditing an enterprise wireless infrastructure, all eyes eventually fall on the client configuration. (ref Hacking Exposed Wireless by Cache, Wright, and Liu) A properly implemented enterprise wireless network infrastructure is extremely difficult to attack.

However, configuration errors are common in laptop configurations; therefore, malicious individuals will turn their attention to attacking these clients. This could expose organizations to a wide variety of attacks including network impersonation "evil twin" attacks. In this instance an attacker would mimic the enterprise AP name, simulate a real network, and then steal the user's credentials or attack the client directly.

Organizations must ensure that all wireless clients are securely configured in accordance with industry standards and best practice. This includes the installation of a personal firewall, antivirus software and effective patch management on all client devices. Once these devices have been securely configured, organizations must restrict the ability of the end user from changing these configurations. Many organizations grant local administrative rights to their users for convenience. Unfortunately, this increases the risk of the client being successfully attacked and makes them much more susceptible to the effects of everyday malware.

A confidential technical findings document was presented to both organizations. These documents contain extremely technical and sensitive findings that, until properly addressed, would increase the risk of network compromise to these organizations. They are therefore not included within this report. Our office will follow up with both organizations in order to ensure they have adequately addressed these findings.

Recommendation 12: We recommend that eHealth address our findings in the area of client device configuration standards.

Recommendation 13: We recommend that MLC address our findings in the area of client device configuration standards.

7. Wireless monitoring not performed

Commercial access points are inexpensive and available anywhere. Employees can build unauthorized wireless networks by simply plugging one into the existing wired network without the knowledge and consent of the corporate IT department. These rogue access points can be a serious breach of network security because they are installed behind the corporate firewall and effectively circumvent all corporate security controls. Unauthorized users could then attempt to use this rogue access point as a backdoor into an otherwise well-defended network.

Organizations should wirelessly monitor for rogue access points either periodically or continuously. Continuous monitoring can also identify a significant number of wireless attacks and can assist an organization in mitigating those risks. The monitoring system should be fully integrated with an organization's Security Event/Information Management (SEIM) System tool, Intrusion Detection, and Incident Handling capabilities.

Failure to wirelessly monitor increases the risk that a rogue access point could be installed and go undetected. This could ultimately affect the confidentiality, integrity and availability of information systems and data.

During the course of the audit, we conducted extensive wireless monitoring looking for any indications of rogue access points. No wireless rogue access points were found in either organization. Note: While this assessment was extremely thorough, some rogue APs lay dormant until an attacker signals for the device to activate. Only continuous monitoring will detect these types of rogue devices.

eHealth

eHealth enterprise wireless infrastructure has the ability to monitor and notify of rogue AP activity. However, this is not monitored or reviewed by administrative staff nor is it integrated into an SEIM tool. We determined that eHealth does not perform continuous or periodic monitoring.

> **Recommendation 14:** We recommend that eHealth implement continuous wireless monitoring in high risk locations that have been identified by a wireless risk assessment. Periodic monitoring of all other locations should be performed routinely.

MLC

Similarly, MLC enterprise wireless infrastructure has the ability to monitor and notify of rogue AP activity. However, this is not monitored or reviewed by administrative staff nor is it integrated into an SEIM tool. We determined that MLC does not perform continuous or periodic monitoring.

> **Recommendation 15:** We recommend that MLC implement continuous wireless monitoring in high risk locations that have been identified by a wireless risk assessment. Periodic monitoring of all other locations should be performed routinely.

8. Wireless network administrators require additional training

As organizations adopt wireless networking technology they need qualified professionals who can design, install, support, and operate these technically complex infrastructures. Wireless administrators require a comprehensive understanding of the technology, the threats, and cost-effective defensive countermeasures. Current vendor specific technical training is necessary in order to implement and maintain effective security configurations.

Wireless security training should be essential for any wireless network. Security for wireless solutions cannot come from a single software program or hardware solution, but rather from trained wireless administrators and implementing multiple layered safeguards.

Failure to ensure that all wireless administrators receive thorough, up-to-date technical and security training could result in a system configuration error or a failure to identify and implement essential security controls.

eHealth

eHealth network administrative staff is responsible for the configuration and day-to-day operation of the wireless infrastructure. The original wireless training was provided to several staff in 2004. There has been no subsequent technical training nor any wireless security training provided since. We acknowledge that supervision on the job, experience, and informal training is in place. However, this does not fully replace specific formal training.

> **Recommendation 16:** We recommend that eHealth ensure that all wireless network administrators receive current vendor-specific wireless training and wireless security training.

MLC

MLC network administrative staff is also responsible for wireless network operations. We determined that these employees had received recent and sufficient training in wireless networking. We acknowledge that MLC's Enterprise Security Architect has received recent wireless specific security training. However, the wireless administrators have not received any wireless security training.

> **Recommendation 17:** We recommend the MLC ensure that all wireless network administrators receive wireless security training.

9. Security awareness training lacking at eHealth

The final key aspect of an effective Information Security program is Security Awareness training. Security Awareness is the human knowledge and behaviors that the organization uses to protect itself against information security risks.

All employees of an organization should receive initial training in order to educate them on written security policies and procedures as well as the associated risks. This training should include wireless networking risks and how to adequately protect against them.

> *"Security Awareness is designed to educate users on the appropriate use, protection and security of information, individual user responsibilities and ongoing maintenance necessary to protect the confidentiality, integrity, and availability of information assets, resources, and systems from unauthorized access, use, misuse, disclosure, destruction, modification, or disruption."* (ref: securingthehuman.org)

It is generally understood by IT security professionals that people are one of the weakest links in attempts to secure systems and networks. (ref: NIST 800-50) Actions these end users take can negatively impact the overall organizational security posture. Even organizations with robust enterprise security architectures and information security programs may still fail to protect their systems should an employee give away critical information (i.e., passwords) or open a malicious file. However, with the proper security awareness training, these same end users will recognize the critical role they have within the organization and can become the foundation of a strong information security program.

eHealth

eHealth has previously identified the requirement for Security Awareness in a funding request to Government. At the time of our audit, eHealth had provided some basic Security Awareness training to the Senior Management Team and Project Management staff. There has been no formal security awareness training provided to the remainder of eHealth staff members. eHealth does not have a formal Security Awareness program.

Recommendation 18: We recommend that eHealth implement a comprehensive Information Security Awareness program. Wireless security threats and risks should be included in this core program.

MLC

MLC has developed an impressive and well rounded Security Awareness program. Posters, briefings, payroll inserts, and even Security Awareness contests are included within. Additionally, they have taken key security policies and converted them into interesting pamphlets that provide a summary of the policy, useful context and additional key security information.

The Security Awareness program has created a listing of all Information Security topics. We confirmed that "wireless network security" is a topic that has been included in this list and is scheduled for future Security Awareness initiatives.

Responses of officials and summary of recommendations

Winnipeg Regional Health Authority – eHealth

The Winnipeg Regional Health Authority (WRHA) and Manitoba eHealth agree with the findings of the Auditor General in its report on Wireless Network Security dated December 2011. The WRHA and Manitoba eHealth place a high priority on the protection of information, and we believe that the wireless security audit has provided valuable feedback and advice that will assist us in our ongoing efforts to achieve the highest possible standard in the protection of health information and information technology assets, especially as the use of wireless networks within our sites continues to grow.

In June 2011, the WRHA formally approved an overarching information security policy that helps address potential security threats and risks. Further, the WRHA is in the final stages of approving a regional wireless LAN security policy as of October 2011. In concert with these policy initiatives, Manitoba eHealth is preparing a Wireless Technical Standard, which will be published within the WRHA, and which will be shared with all Manitoba RHAs, in December 2011.

All of the recommendations contained in the report are in various stages of implementation (see attached responses to the recommendations), and many have already been addressed. Manitoba eHealth, as the WRHA's IT Service provider, is leading the WRHA's improvement effort in regards to network security, access point configurations, and client device configurations, consistent with the recommendations in this report.

Beyond these important measures, Manitoba eHealth continues to improve its information security risk management program and is increasing efforts to improve security awareness within all RHAs, and will work collaboratively with all other RHAs to ensure that similar measures are put into place across the province, as appropriate.

Recommendation 1: We recommend that eHealth conduct a current wireless risk assessment. All residual risk should be reduced and formally accepted by senior management.

Response:

- Manitoba eHealth is presently performing a comprehensive Wireless Threat Risk Assessment which will be completed in November 2011.
- Manitoba eHealth will develop a management action plan to formalize the risk reduction and improvement efforts. This plan will be submitted

for approval to WRHA senior management by the end of December 2011.

Recommendation 2: We recommend that eHealth develop processes to effectively identify and manage changes to threats and vulnerabilities to all IT systems, including wireless networks.

Response:

- Formal Threat and Risk Assessments (TRAs) have become standard practice since April 2010 within Manitoba eHealth for major IT systems, including the wireless network infrastructure. These assessments and the resulting management action plans have formalized the risk reduction and improvement effort for all major IT systems.
- A Vulnerability Management software solution is in the process of being implemented. This solution will provide an ongoing capability to identify and track technical vulnerabilities within eHealth IT systems. The initial implementation will be completed by December 2011 and an expanded implementation is planned for the first half of 2012.
- An ongoing challenge faced in comprehensive risk mitigation is the large number of legacy technologies and applications that predate the creation of the health regions; these are being addressed within our overall capital and operating plans on a priority basis.

Recommendation 4: We recommend that WRHA develop, approve and enforce a comprehensive, overarching IT security policy.

Response: WRHA has established an overarching IT Security Policy (June 2011) and has updated the existing Computer and Internet Usage Policy (June 2011). These policies have also been shared with the Provincial CIO Committee which includes representation from all Regional Health Authorities (RHAs).

Recommendation 6: We recommend that WRHA develop, approve, and enforce a comprehensive wireless security policy.

Response:

- WRHA is in the final stages of approving a wireless LAN security policy (October 2011).
- Consistent with the WRHA policy initiatives, Manitoba eHealth is preparing technical and security standards, which include wireless LAN technology. These standards, referenced in the above policies, will be shared with all RHAs once available. The eHealth standards will be

completed during the 4th quarter of fiscal 2011/12. The Wireless LAN technology standard will be completed in December 2011.

Recommendation 8: We recommend that eHealth address our findings in the area of network security controls.

Response: Manitoba eHealth is continuing network security improvement efforts based on internal assessments which will include the wireless security audit results. A risk mitigation plan to address all recommendations over time is currently in place.

Recommendation 10: We recommend that eHealth address our findings in the area of Access Point configuration standards.

Response: Manitoba eHealth has completed an update of the configuration of production wireless Access Points to address the most significant audit findings. Upon completion of the wireless LAN technical standard and the wireless threat risk assessment, Manitoba eHealth will update all wireless Access Point configurations to reflect the approved standard. A plan is in place to implement the remaining by the end of March 2012.

Recommendation 12: We recommend that eHealth address our findings in the area of client device configuration standards.

Response: Manitoba eHealth has developed a client device configuration standard. This standard does not allow end user access to the device's configuration and has been implemented in over 70% of the wireless devices. The client device configuration standard will be finalized upon completion of the wireless LAN technical standard and the wireless threat risk assessment that are referenced previously. A plan is in place to implement the remaining items by the end of March 2012.

Recommendation 14: We recommend that eHealth implement continuous wireless monitoring in high risk locations that have been identified by a wireless risk assessment. Periodic monitoring of all other locations should be performed routinely.

Response: The wireless LAN security policy establishes a clear mandate for wireless network management and monitoring and assigns responsibilities to Manitoba eHealth and WRHA site management as appropriate. Pursuant to this mandate, Manitoba eHealth has prepared a wireless monitoring strategy which includes routine monitoring, with priority monitoring to be based upon the wireless threat/risk assessment.

Recommendation 16: We recommend that eHealth ensure that all wireless network administrators receive current vendor-specific wireless training and wireless security training.

Response: Manitoba eHealth is training all designated network administrators on wireless technology. They are being provided vendor-specific wireless training and wireless security training and ongoing training will also be provided.

Recommendation 18: We recommend that eHealth implement a comprehensive Information Security Awareness program. Wireless security threats and risks should be included in this core program.

Response:

- Manitoba eHealth has completed an Information Security Awareness and Training strategy. One of the key goals of this strategy is to raise awareness of the various security related policies at the WRHA (IT Security, Computer and Internet Usage and Wireless LAN Security).
- A Senior Security Analyst has been hired in March 2011 to implement a Security Awareness and Training program. This program effort will be ongoing.

Manitoba Lotteries Corporation

Recommendation 3: We recommend that MLC develop processes to effectively identify and manage changes to threats and vulnerabilities to all IT systems, including wireless networks.

Response: Manitoba Lotteries (MLC) agrees with this recommendation. MLC has a contract with KPMG to perform an annual network security review. All risks identified in this year's review are being addressed. MLC will have KPMG review the network security risk assessment including wireless as part of their annual network security review.

The next annual review is scheduled to commence prior to end of fiscal 2011/12.

Recommendation 5: We recommend that MLC review all information security policies on a regular basis. This review should be formally documented and any changes effectively communicated to all staff.

> ***Response:*** Manitoba Lotteries agrees with this recommendation. MLC will publish a plan to update and develop information security policies. The new policies will be taken from the PWC Year 1 Network Security Assessment report.
>
> This plan will be developed prior to end of fiscal 2011/12.

Recommendation 7: We recommend that MLC develop, approve, and enforce a comprehensive wireless security policy.

> ***Response:*** Manitoba Lotteries agrees with this recommendation. MLC plans to start developing a wireless policy in January 2012.
>
> This policy will be completed by end of fiscal 2011/12.

Recommendation 9: We recommend that MLC address our findings in the area of Network Security Controls.

> ***Response:*** Manitoba Lotteries agrees with this recommendation. MLC has already addressed one finding and is developing a program to complete the other findings.
>
> This program will be implemented by Q2 fiscal 2012/13.

Recommendation 11: We recommend that MLC address our findings in the area of Access Point configuration standards.

> ***Response:*** Manitoba Lotteries agrees with this recommendation. Since the security review was done, MLC addressed the findings.
>
> Manitoba Lotteries considers this item complete.

Recommendation 13: We recommend that MLC address our findings in the area of client device configuration standards.

> ***Response:*** Manitoba Lotteries agrees with this recommendation.
>
> This program is in progress and will be completed by Q4 fiscal 2011/12.

Recommendation 15: We recommend that MLC implement continuous wireless monitoring in high risk locations that have been identified by a wireless risk assessment. Periodic monitoring of all other locations should be performed routinely.

> ***Response:*** Manitoba Lotteries agrees with this recommendation. Since this recent security review was done a program has been formalized and put in place.
>
> Manitoba Lotteries considers this item to be complete.

Recommendation 17: We recommend that the MLC ensure that all wireless network administrators receive wireless security training.

> ***Response:*** Manitoba Lotteries agrees with this recommendation. Training will be added to the training curriculum for appropriate MLC staff.
>
> The training for these MLC staff will be completed by Q4 fiscal 2011/12.