Vérificateur général
de la Ville de Montréal

Report of the Auditor General of the Ville de Montréal
to the City Council and to the Urban Agglomeration Council

For the Year Ended December 31, 2013

5.4

Security of Wireless Networks

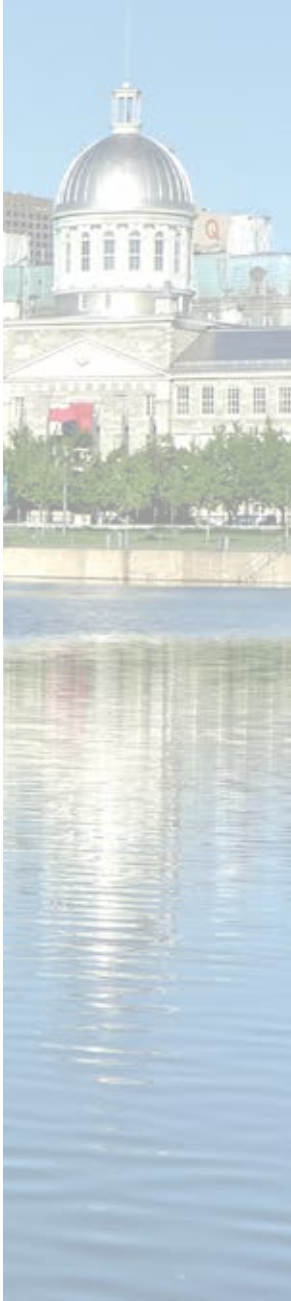

Table of Contents

List of Acronyms

MAC	Medium Access Control
NIST	National Institute of Standards and Technology
STI	Service des technologies de l'information
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access 2
WPS	Wi-Fi Protected Setup

5.4. Security of Wireless Networks

1. Introduction

With the rise of mobile communications and information equipment, wireless networks are everywhere. These networks make it possible to connect all kinds of equipment (e.g., laptop computers, tablets, smartphones) to corporate networks, such as that of Ville de Montréal (the city).

Wireless networks are widely used because they provide ease of access to the internal computer networks of companies and organizations without the major costs of a wired infrastructure. Each wireless network contains a varying number of wireless access points based on the number of connections and the office surface area.

To serve its population, the city uses a complex computer network that connects thousands of employees. In addition to wired connections, users can connect to the network via wireless access points. They thus enjoy greater flexibility since they are no longer restricted to fixed workstations.

Unlike a wired network, a wireless one is not bound by a defined geographical perimeter since its signal is broadcast well beyond the physical confines of the workplace (offices and buildings). As a result, wireless networks are often vulnerable to attacks by malicious individuals who attempt to access confidential information without needing to be physically present in the company.

As with a wired network, the infrastructure of wireless networks must be adequately protected to prevent unauthorized access. These entry points are equally important because they provide access to confidential information about citizens, elected officials and employees.

Given the above, we considered it expedient to audit the security of the wireless networks.

2. Purpose and Scope of the Audit

The purpose of our audit was to determine if the controls that were put in place ensure that only duly authorized wireless networks are present within the city and that their security mechanisms prevent unlawful access to the city's corporate network.

The audit focused on the wireless networks managed by the Service des technologies de l'information (STI), by the Division des ressources informationnelles reporting to the Direction des services administratifs et du greffe of Saint-Laurent borough and by the Division de l'informatique reporting to the Direction des services administratifs of Saint-Léonard borough.

Our audit included the participation of a recognized IT security specialist and our conclusions are based on industry best practices, in particular:

- *Recommandations de sécurité relatives aux réseaux WiFi,* Agence nationale de la sécurité des systèmes d'information, General Secretariat of Defence and National Security, French Ministry of Defence;
- *Establishing Wireless Robust Security Networks: A Guide to IEEE802.11i,* Special Publication 800-97, National Institute of Standards and Technology (NIST).[1]

Based on the results of our risk analysis, we chose eight buildings according to their strategic importance within the city, the type of information handled and the number of wireless networks in place.

We carried out the following steps in each of these buildings:

- Step 1: full visit of the premises to identify all wireless networks;
- Step 2: visit to each of the building's communications rooms to locate any non-authorized wireless equipment;
- Step 3: obtaining Medium Access Control (MAC)[2] addresses of the building's local area network for comparison with MAC addresses of the wireless networks (identified in Step 1) to locate any unauthorized wireless networks.

We also assessed administrative frameworks and wireless network inventory management.

Our audit was conducted between August and December 2013.

1 Agency of the U.S. Department of Commerce. Its role is to support the economy by working with industry to develop technology, measurements and standards.

2 Physical identifier stored on a network card and universally used to assign a unique address.

3. Summary of Findings

Table 1 presents security gaps identified during our audit.

Table 1 – Summary of Findings

Section of the report	Finding	Details	Impact level
4.1	Absence of a process to detect wireless networks	N/A	High
4.2	Unsecured wireless access points	3 wireless access points in 2 buildings	High
4.3	Inadequate security protocols	9 wireless access points in 5 buildings	Moderate
4.4	Unprotected wireless printers	2 printers in 1 building	Moderate

4. Detailed Findings and Recommendations

4.1. Process for Detecting Unauthorized Wireless Networks

4.1.A. Background and Findings

Within an organization such as the city, it is vital that a recursive process be put in place in the STI to detect unauthorized wireless networks.

Such a process makes it possible to detect and remove, in a timely manner, any wireless network that has been set up without proper authorization. It also makes it possible to close possible security loopholes introduced by these wireless networks.

We concluded that the STI has no process in place to detect unauthorized wireless networks. During our audit tests, for example, we found a wireless access point concealed in a city building and were unable to establish who owned it. According to the information we obtained, this access point was not connected to the city's corporate network.

We consider the impact level to be **high** since the city faces the following potential risk: the lack of a recursive detection process makes it difficult to uncover and locate unauthorized wireless access points. The installation of such access points could enable a malicious employee or external hacker to have hidden access to the city's corporate network and thereby access confidential information.

4.1.B. Recommendation

We recommend that the Service des technologies de l'information implement a recursive process to detect unauthorized wireless networks and, where necessary, to take the corrective action needed to remove them.

Business unit's response:

The action plan proposed by the STI is in line with our recommendation and, once implemented, should solve the problem at issue. The details of this plan cannot be divulged, however, due to the need for confidentiality in matters of security.

4.2. Wireless Access Points

4.2.A. Background and Findings

An unsecured wireless network allows access to all data shared on it. If confidential data is sent via this network, anyone can easily intercept the data, without any specialized knowledge, using tools that are freely available on the Internet.

During the course of our audit, we uncovered several open and unsecured wireless access points in two of the eight buildings we sampled.

We consider the impact level to be **high** since the city faces the following potential risks:

- An unsecured wireless access point used to freely surf the Web is not protected by the city's security infrastructure. As a result, the workstation of a person connected to this access point could become infected with malware that could compromise the security of the city's corporate network;
- A malicious person could use certain wireless access points to intercept potentially confidential data and attempt to compromise the security of the city's corporate network.

4.2.B. Recommendation

We recommend that the Service des technologies de l'information ensure that all wireless access points be configured with a robust security protocol.

Business unit's response:

The action plan proposed by the STI is in line with our recommendation and, once implemented, should solve the problem at issue. The details of this plan cannot be divulged, however, due to the need for confidentiality in matters of security.

4.3. Security Protocols

4.3.A. Background and Findings

Wireless networks broadcast their signals well beyond the physical confines of an organization's offices. To prevent unauthorized individuals from connecting to these networks and intercepting the data shared on them, security protocols must be put in place.

Wi-Fi Protected Access (WPA) is a wireless network security protocol implemented in the early 2000s as a temporary solution to replace the earlier Wired Equivalent Privacy (WEP), which was no longer considered secure.

In 2004, Wi-Fi Protected Access 2 (WPA2) succeeded WPA. This protocol, which features encryption to protect data sent over wireless networks, is considered completely secure. WPA2 is approved by the NIST and certified by the Wi-Fi Alliance.[3]

Another protocol, Wi-Fi Protected Setup (WPS), is used to simplify the parameterization of wireless network security. WPS is intended primarily for individual use and is not suited to organizations such as the city, because it contains a major security vulnerability.

During the course of our audit, we uncovered nine wireless access points that were configured to use WPA2 but that also allowed the use of less robust protocols, including WPA and WPS (in five buildings).

We consider the impact level to be **moderate** since the city faces the following potential risk: a malicious person could decipher the authentication key in a few hours and access the city's corporate network. The person would thus gain access to confidential information.

4.3.B. Recommendation

We recommend that the Service des technologies de l'information and the relevant boroughs ensure that wireless network equipment use only the most robust security protocols.

Business units' response:

The action plans proposed by the STI are in line with our recommendation and, once implemented, should solve the problem at issue. The details of these plans cannot be divulged, however, due to the need for confidentiality in matters of security.

[3] Global consortium that tests and certifies Wi-Fi products and technology.

4.4. Wireless Access Printers

4.4.A. Background and Findings

Some printers have wireless functionalities that enable workstations to connect to them directly without the need to connect to the corporate network. These printers, like all wireless equipment, must be protected to ensure that printed documents, which may contain sensitive information, are not intercepted.

Following our tests, we uncovered two printers in one building, whose wireless functionality was activated but not protected. These printers were being used by employees who handle confidential information.

We consider the impact level to be **moderate** since the city faces the following potential risk: a malicious person could intercept all confidential documents sent to the printers within a 100-metre radius.

4.4.B. Recommendation

We recommend that the Service des technologies de l'information deactivate its printers' wireless access functionality if it is not absolutely required. In cases where such access is required, we recommend activating a robust security protocol.

Business unit's response:

The action plan proposed by the STI is in line with our recommendation and, once implemented, should solve the problem at issue. The details of this plan cannot be divulged, however, due to the need for confidentiality in matters of security.

5. General Conclusion

Based on the results of our audit, we conclude that, overall, the wireless networks are adequately protected. Management of wireless network security, however, needs some improvement. The lack of a process to detect unauthorized wireless networks has allowed some potentially prohibited wireless access points to be installed, some of which are concealed. Furthermore, some wireless access points, which were unsecured or used security protocols that were not robust, did not meet the city's security requirements.

As a result, the city runs the risk of malicious persons taking advantage of security gaps in some wireless networks to access confidential information. The city should take all necessary measures to address these gaps in a timely manner.

Implementing our recommendations should provide the city with adequately secure wireless networks.

6. Appendix

6.1. Description of Impact Levels

Table A – Definition of Impact Levels

Impact level	Definition of impact levels
Critical	Direct consequences on the security of the data and systems of the city's corporate network: major impact on the city's reputation, general paralysis of the corporate network's systems and massive disclosure of confidential information.
High	The presence of security gaps would allow unauthorized individuals to access confidential information on elected officials, citizens or employees. This would seriously harm the city's reputation.
Moderate	The presence of some security gaps would moderately harm the operations of the corporate network's systems and the city's reputation, and some confidential information would be disclosed.
Low	Negligible repercussions on the city's operations and services. The loss of citizens' trust in the city is unlikely.