Bureau du vérificateur général

V.10. Physical Intrusion Testing

TABLE OF CONTENTS

V.10. PHYSICAL INTRUSION TESTING

1. INTRODUCTION

The Ville de Montréal (the city) and its controlled agencies have many essential and vital assets located, stored or kept in various buildings and premises.

Given their importance, these assets must be properly safeguarded to guarantee the safety of people and goods and also ensure the continuity of services essential for the operation, well-being and prosperity of the municipality.

Physical intrusion is one of the first avenues considered by malicious individuals who are intent on defacing, destroying or tampering with the assets or data housed in these assets. Physical security, therefore, is the first line of defence needed to manage risks to the city's assets.

To prevent theft or sabotage, effective protection, monitoring and access controls must be implemented.

Security best practices advocate conducting physical intrusion tests under real conditions to ensure a reasonable level of confidence in the quality of controls used to safeguard the physical protection of existing assets.

Accordingly, the city's Bureau du vérificateur général (BVG) decided to perform an audit involving physical intrusion tests. Contrary to the BVG's normal procedures, prior notice of the audit was not given to the owners of the assets being audited. This was done to ensure that physical safety controls would be tested under real conditions and not temporarily reinforced for our visits.

Physical Security and Control Mechanisms

Physical security consists of protecting assets using physical access control mechanisms, for example fences, access doors equipped with mechanical or electronic locks, security gates, surveillance cameras or a human presence (e.g., security guards). These control methods are required to prevent unauthorized acts, whether intentional or not, that could compromise the assets' security.

Defining the level of physical protection needed should be based on the assets' importance and in proportion to the risks and threats they represent. The security mechanisms must take into account the geographic location, type of building and physical layout of the premises containing the assets.

Physical safety requirements vary according to the roles and responsibilities of the business units and the importance of the activities they provide citizens. For example, a business unit such as the SPVM requires a very high level of physical security, whereas other business units, such as municipal shops, require a lower level. Concepts of securing the periphery, control of physical access and protective measures for equipment apply universally when formulated and planned with the principle of proportionality in mind.

In the case of computer assets on magnetic media, electronic security methods will be inadequate and costly if physical security fails to prevent malicious individuals from accessing the computer equipment housing the data and stealing, damaging or destroying it.

2. AUDIT SCOPE

Our audit consisted of performing physical intrusion tests under real conditions. This is the first part of a more comprehensive audit of city management of physical security.

The objective of our audit was to obtain reasonable assurance that the control mechanisms in place adequately protect physical access to the city's assets.

This audit dealt exclusively with physical security and did not cover computer security such as access to electronic data.

The primary method used to carry out our physical intrusion tests was social engineering.

Social engineering is the preferred method of conducting physical intrusion tests when there are employees in the target. This method exploits procedural flaws and employee judgment in the targeted unit to obtain goods, services or confidential material.

Social engineering exploits the gullibility of people by using the power of persuasion and lack of appropriate procedure to pass oneself off as a city employee, for example. The BVG auditors used their knowledge, personalities and impersonation to attempt to access city premises and goods. More specifically, our social engineering methodology was as follows:

- Using an approach phase to gain the client's trust by passing oneself off as a city employee (e.g., Direction des immeubles)
- Presenting an important reason related to the safety of individuals (e.g., checking fire detection systems)
- Creating a diversion, e.g., a phrase or situation to reassure the employee and avoid raising any suspicions

At the time of our intrusions, we photographed the premises that we entered. We developed a description for each successful intrusion. In particular, we:

- noted the date and time of the intrusion
- detailed the steps followed and approaches used to carry out our intrusion tests
- specified our intrusion process, i.e., access doors entered, premises visited and hallways used
- described the assets that we observed

Before beginning the social engineering process, reconnaissance of the outer perimeter of each of the premises audited was carried out to visually detect the presence of any unlocked access points.

Our physical intrusion tests covered 31 of the city's sites and facilities and those of the Société de transport de Montréal (STM) selected through the results of our impact analysis on the importance of the assets held in buildings.

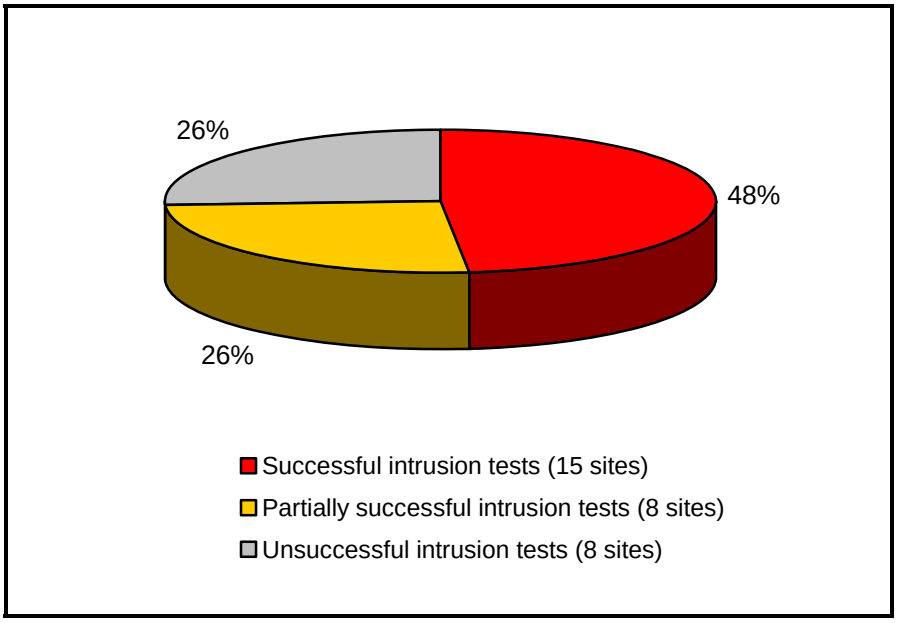
Because of the sensitive nature of these sites, we prefer keeping the list confidential.

3. FINDINGS, RECOMMENDATIONS AND ACTION PLANS

3.1. FINDINGS

We have succeeded, in whole or in part, with our physical intrusion tests for 23 of the 31 sites targeted, or **74%** of all the sites. The results appear in Graph 1.

Graph 1–Summary of Results



Successful intrusion tests: physical intrusion tests were conclusive for 15 of the 31 targeted sites. We were successful in accessing several critical areas and assets at these sites without being intercepted or raising suspicions.

Partially successful intrusion tests: physical intrusion tests were partially successful for 8 of the 31 targeted sites. We succeeded in accessing certain areas and assets at these sites without being intercepted.

Unsuccessful intrusion tests: physical intrusion tests were in vain or failed for 8 of the 31 sites targeted. We were either unsuccessful in accessing the sites because of the protection measures in place, or we were quickly intercepted and escorted off the site. In other words, only 26% of targeted sites had a level of physical protection sufficient to counter social engineering.

The three tables below show the detailed results of the intrusion tests by business unit, site and impact level (see Appendix 4 for the definition of impact levels.)

It should be mentioned here that, in the case of the successful or partially successful intrusion tests, at no time were any documents belonging to the audited unit removed or examined.

Table 1–Successful Intrusion Tests

Impact level	Number of business units	Number of sites*
Major	3	9
High	2	2
Moderate	2	4
Total	**7**	**15**

* A business unit can have several sites.

Table 2–Partially Successful Intrusion Tests

Impact level	Number of business units	Number of sites*
Major	2	2
High	1	1
Moderate	5	5
Total	**8**	**8**

* A business unit can have several sites.

Table 3–Unsuccessful Intrusion Tests

Impact level	Number of business units	Number of sites*
Major	3	6
High	1	1
Moderate	1	1
Total	**5**	**8**

* A business unit can have several sites.

This section lists our main findings for all business units. Due to the criticality of the sites where intrusions succeeded or partially succeeded, the decision was made to keep the details and results of the intrusion tests at each site secret. Under a seal of confidentiality, a detailed audit report was sent to the persons in charge of each business unit, who validated the findings and recommendations proposed for their specific business unit.

FINDING

In the case of one site that holds data of an extremely sensitive nature, we were able to move freely around the premises. We could have examined or even taken several documents without anyone noticing.

FINDING

For several business units that had a high or major impact level on public security, we were able to access a building using a false identity and motive. In other business units, we were also able to enter without meeting anyone in charge. At some of these, we were even left to our own devices, i.e., we were able to move freely about the building without being accompanied. We accessed control rooms containing equipment that is highly critical to the safety and well-being of citizens. We were also able to access, without impunity:

- **confidential information**
- **material and equipment that was vital to public safety or comfort**
- **strategic city assets**

FINDING

In some business units, there were several unlocked main or secondary entrance doors providing access to critical areas. We gained entry to some sites easily through these doors. We were able to walk around inside several sites without being intercepted by employees, even though, in several cases, employees were aware of our presence.

FINDING

At several sites, we were able to gain access to critical locations that were not equipped with any surveillance and whose doors were left unlocked.

We also concluded that, in several business units:

- There were no procedures in place to:
  - control visitors' identity
  - formally identify visitors with a badge
  - check the motive of the visit
  - accompany visitors at all times
- There was no visitors' log containing:
  - visitor names
  - visitors' service or company
  - person visited
  - reason for the visit
  - arrival date and time

  - departure time
  - signature of a person in charge
- Most of the employees do not confront and question non-authorized individuals who are walking freely about the premises.
- Surveillance cameras were installed in some critical locations, but never did a security guard notice our presence and challenge us.

In many of the audited business units, the physical safety weaknesses noted were extremely worrisome since, in our opinion, they could lead to the following threats:

- sabotage of equipment that is vital to public safety and comfort
- theft of highly sensitive documents that could affect the integrity and safety of persons
- theft of strategic equipment
- theft of valuable equipment
- terrorist act on equipment of vital importance to public safety
- theft of uniforms for identity theft

If these threats were to materialize, the consequences could be serious, even catastrophic, for the safety of the public and Montréal's social and economic activities.

3.2. RECOMMENDATIONS

We met with each business unit to explain the results of our intrusion tests. We explained the process used, our conclusions and our suggested recommendations for improving the level of physical protection of the audited sites under their responsibility. It should be understood that these conclusions are based solely on the results of our intrusion tests. A more in-depth audit on the quality of access and physical protection mechanisms, including existing procedures, is planned for 2011.

This section contains our most important recommendations. Obviously not all of these apply to all business units due to their unique characteristics and impact levels.

In order to prevent unauthorized physical access and ensure adequate protection of assets and information stored at business unit sites, we recommend the following:

- **Define strict visitor controls requiring, among other things:**
  - **the systematic verification of visitors' identity**
  - **a valid reason for the visit**

  - **an ID badge for visitors (the badge could be a different colour for each type of visitor)**
  - **that visitors be accompanied throughout the visit**
  - **raising awareness among staff of the importance of confronting and questioning strangers or unknown persons in the site**
- **Implement visitors' logs and assign someone to oversee it. This log should contain the following information:**
  - **visitor's name**
  - **visitor's service or company**
  - **reason for the visit**
  - **name of the person being visited**
  - **signature of the person in charge**
  - **date and time of arrival**
  - **date and time of departure**
- **Control and check surveillance camera monitors and take necessary action when suspicious activities or individuals are detected.**
- **Advise staff of the risks and threats of social engineering and the security measures to take.**
- **Identify the access points for each site and implement appropriate protection measures.**
- **Control physical access by ensuring doors to main and secondary entrances are properly locked.**

3.3. ACTION PLANS OF THE RELEVANT BUSINESS UNITS

The relevant business units have been made aware of our recommendations and will forward their action plan to us at a later date.

4. APPENDIX

4.1. DESCRIPTION OF IMPACT LEVELS

IMPACT LEVELS	DEFINITIONS OF IMPACT LEVELS
Major	Direct consequence on public safety and health that endangers the safety of individuals. If there is the least tangible effect on public security and public health, a “major” impact level is assigned to a site or facilities.
High	While the presence of many high value assets and/or confidential and strategic information poses less of a threat to public safety, an intrusion would severely damage the city’s reputation and operation and economic activity.
Moderate	Because of the presence of certain high value assets or confidential and strategic information, an intrusion would interfere moderately with the city operations or harm its reputation.