CENTRE FOR PUBLIC MANAGEMENT INC.
CENTRE DE GESTION PUBLIQUE INC.

Public Service Labour Relations Board

Audit of Internet Security

March 31, 2006

Executive Summary

Suite /Pièce 1016,
130 rue Albert Street,
Ottawa, ON K1P 5G4

(T) 613-567-7752
(F) 613-567-7790
cpm.ca

Executive Summary

Background, Audit Objectives and Scope

Centre for Public Management Inc. was contracted by the Public Service Labour Relations Board (PSLRB) to perform an internet audit on the use of, and security over, the internet. The PSLRB believes in easy and wide access to its services and information, and a secure infrastructure has been put in place to protect its technical infrastructure. However, the internet is a potential access point into government networks, and in response to this risk this audit was performed with the following objectives:

- To assess the PSLRB usage of the internet;
- Assess the security measures preventing unauthorized access to the PSLRB's networks from the internet, including the implementation and compliance with the relevant sections of the Government Security Policy and Management of IT security Standards.

Findings

Employee use of the Internet

In the absence of an internet use policy, we found that the majority of employee use of the internet (87%) was work related. The personal use consisted of expected items such as news, personal email, shopping etc. However, there were occasional visits to questionable behaviour sites for a work environment. Although these represented less than 1/10th of 1% of all websites visited, they do increase the risk to the PSLRB of viruses, malicious computer code and complaints raised by employees who may be inadvertently exposed to this material by a co-worker.

1. We recommend that an internet use policy be drafted which clearly specifies acceptable use of the internet.

   Management Response: The PSLRB already has in place a Policy on the use of Electronic Networks which is posted on its Intranet site. Electronic networks are defined in the policy as being groups of computers and computer systems that can communicate with each other, including the Internet, internal networks and public and private networks external to the PSLRB. The objective of this policy is as follows:

   ....The Public Service Labour Relations Board encourages authorized individuals to use electronic networks to conduct the business of the Board, to communicate with other authorized individuals and with the public, to gather information relevant to their duties, and to develop expertise in using such networks. Because electronic networks permit individuals who use them to inadvertently or deliberately, damage a positive work environment, to disclose classified or designated information in an unauthorized fashion, to incur costs or to participate in unlawful activities, the PSLRB is instituting this policy to ensure that anyone authorized to access electronic networks uses those electronic networks appropriately. A list of unacceptable activities relating to the access to electronic networks is annexed to the policy (Annex C).

Notwithstanding the above, the PSLRB plans to develop and implement in 2006-2007 a new policy on the use of the Internet which will meet the requirements of the Management of IT Security (MITS) standards and address concerns raised by this internal audit. Effectively, the new policy will seek a more controlled and secure Internet environment.

2. We further recommend that the firewall be configured to block suspect web sites.

Management response: The PSLRB agrees that suspect web sites must be blocked. However, instead of reconfiguring the firewall for this purpose, it plans instead to purchase and implement in 2006-2007 an Intrusion Detection System (IDS) that will not only monitor and search for evidence of external intrusions or attempted external intrusions, but will also detect and report the existence of other security vulnerabilities within the network, such as misuse of systems. Depending on the capacity of the IDS, the PSLRB could also decide to purchase a blocking software program such as Websense to complement its security infrastructure.

Internet Security

We found that the network perimeter is reasonably secure. We reviewed network documentation, policies and procedures, operating system software levels and firewall rules and found them to be adequate. We further conducted an external scan of the PSLRB's networks and found nothing unexpected.

To further increase security, we recommend that the PSLRB:

3. Implement a policy for the management of passwords.

Management Response: A new procedure for the assignment and management of passwords was presented to the IT Committee of the PSLRB on August 30, 2005, as part of the strategy for migrating from a Novell to a Windows environment. This procedure which aims to transfer the responsibility for the management of passwords from IT Services to all users will be communicated to all employees and implemented by May 30, 2006.

4. Formalize the planning, testing and release of patches to the Demilitarized Zone (DMZ) systems

Management Response: The PSLRB agrees with the recommendation to formalize the management of patches to DMZ systems, which in principle pertain to its web server only. A schedule will be developed and implemented by June 30, 2006.

5. Restrict the utilization of the Microsoft Exchange server to Microsoft Exchange activities only.

Management Response: The PSLRB acknowledges the importance of limiting activities being run on the MS Exchange server. For functionality reasons, a splash page prompting internal users to accept network policy when they log on was installed on the MS Exchange server. This is the only non-Exchange content on the MS Exchange server. This approach was used for functionality reasons, and to respect established protocols for intranet access. The PSLRB commits to a strict utilization of the MS Exchange server and will not proceed with any further installation of non-MS Exchange applications on this server.