Project Report

Security Enhancement Project

For IM/IT

April 15, 2005

1. INTRODUCTION

The purpose of this update is to provide a:

- high level overview of the Security Enhancement Project (SEP);
- description of project achievements during FY 2004/2005;
- description of planned project achievements for FY 2005/2006.

2. SECURITY ENHANCEMENT PROJECT OVERVIEW

Malicious code, identity theft, cyber vandalism and a variety of other threats face computer users and administrators around the world. At the same time, technology has made it increasingly easy to interconnect a wide range of computers and supporting devices.

The Information Management/Information Technology (IM/IT) network supporting the BC government and a wide variety of public agencies has slowly expanded to be one of the largest private networks in North America. While it is extremely functional and wide reaching it was not designed with security requirements in mind.

Today the BC government network and information systems are vulnerable to attacks that could result in breaches of confidentiality, integrity and availability. Compounding this situation is the ever increasing business requirement to have high volume data links outside of the government network.

Adequate security measures are required to ensure that high speed, high volume interconnection with a variety of outside agencies and the internet can occur, while at the same time protecting the broader public sector's network and information systems.

The Security Enhancement Project was initiated in November, 2004, and broadly tasked with improving the security of government's information assets. The project was organized with one stream dealing with security policies and standards; another with developing the model and implementation plan for a "Next Generation" Security Program and a third with the technical architecture necessary to deliver the new model.

In summary, the overall objective of SEP is to enhance trust and protect the interests of all parties relying on government-managed information and information systems from harm resulting from failures of availability, integrity and confidentiality.

Anticipated results associated with the new IM/IT Security Program will be:

- Complete set of government policies, standards and guidelines respecting IM/IT Security;
- A further reduction of current vulnerabilities to unauthorized access;
- An increase in the ability to prevent disruption of the government's critical infrastructure and business systems;
- An increase in the ability to minimize the damage and recovery time related to any disruption that does occur as the result of a security breach;
- Rationalizing ongoing roles, funding and resource requirements for the Security Program.

3. ACHIEVEMENTS IN FY 2004/2005

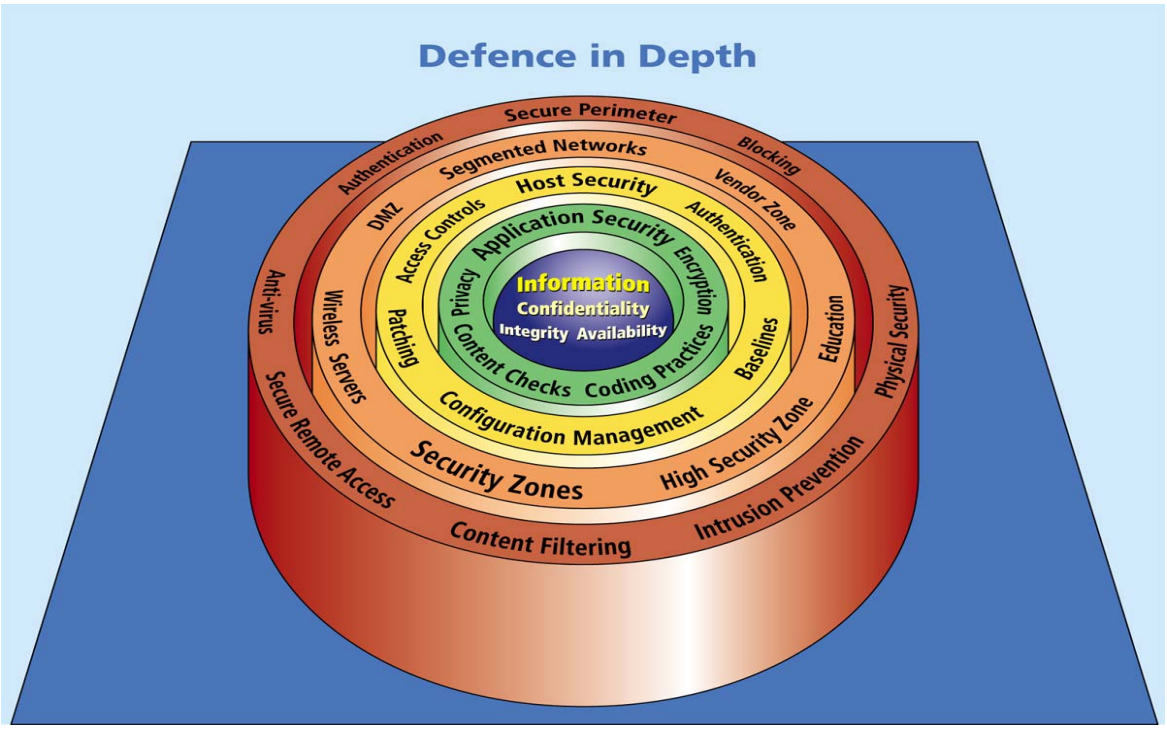
The Policies and Standards work stream staff are well underway in their process to draft and vet security policies and standards. From November, 2004, to the end of March, 2005, the following was achieved:

- Sign off of the complete rework of Chapter 12 Core Policy Manual concerning IM/IT security;
- Development of process to vet rework of Chapter 12 through external approval process;
- Redrafting and sign off of the framework to be used for security policies and standards development work;
- First draft policies and standards drafted and reviewed;
- Process to vet drafts through ministry and central agencies established;
- Critical Incidence Management procedures documented and approved.

The Security Program design team has accomplished a significant amount of improvements over the past five months. From November, 2004, to the end of March, 2005, the following was achieved:

- Blueprint Document for IM/IT Security completed and distributed;
- IM/IT Business Requirements for security collected from all Ministries and report drafted;
- Ministry Business Review Committee created to provide input to program design;
- Security Managers Committee formed to provide input into program design;
- Security Inventory underway gathering detailed information from Ministry contacts;
- Security Awareness Initiative underway with senior government committees and agencies.

The Security Blueprint document proposed a “Defense in Depth” approach to IM/IT security. This approach has been widely accepted within major public and private organizations. The graphic below illustrates the many levels of a modern security strategy. There is no one single technology or approach that will achieve good security but rather the combination and application of several that will significantly improve overall IM/IT security for the BC government and Broader Public Sector.



The Technical Architecture stream has planned and overseen the implementation of several technical improvements aimed at providing an immediate increase in IM/IT security. As well, the design principles have been established for the long term technical infrastructure required to deliver the new Security Program. From November, 2004, to the end of March, 2005, the following has been achieved:

- Third Party secure connectivity zone architected and implemented;
- Anti-virus patch management standardized;
- Up to date operating system patching applied to all desktops and servers;
- Devices to protect critical infrastructure purchased and deployed;
- Zone model for segmenting central information assets established and implementation initiated;
- Technical security training for core infrastructure staff.

4. SUMMARY OF EXPENDITURES 2004/2005

Budget Source

CITS	**$500,000**
CIO	**$350,000**
TB approved contingency	**$1,500,000**

Total	***$2,350,000***
Capital	***$1,000,000***

Budget Plan	***As per Charter***	***Est. at March 31, 2005***
Project Office	**$400,000**	**$275,500**
Policies & Standards	**$200,000**	**$236,000**
Business Requirements & Security Program Design	**$350,000**	**$353,750**
Network Segmentation	**$650,000**	**$473,000**
Technical Enhancements	**$750,000**	**$901,000**
	----------	**----------**
Total Operating (including amortization)	***$2,350,000***	***$2,239,250***

5. ACHIEVEMENTS PLANNED FOR FY 2005/2006

The Policies and Standards work stream will continue to draft security policies and standards achieving the following results by March 31st 2006:

- Core Policy updated and adopted;
- All security policies drafted and vetted;
- All security standards drafted;
- Detailed Roles and Responsibilities paper drafted.

The Program Design team will achieve the following in 2005/2006:

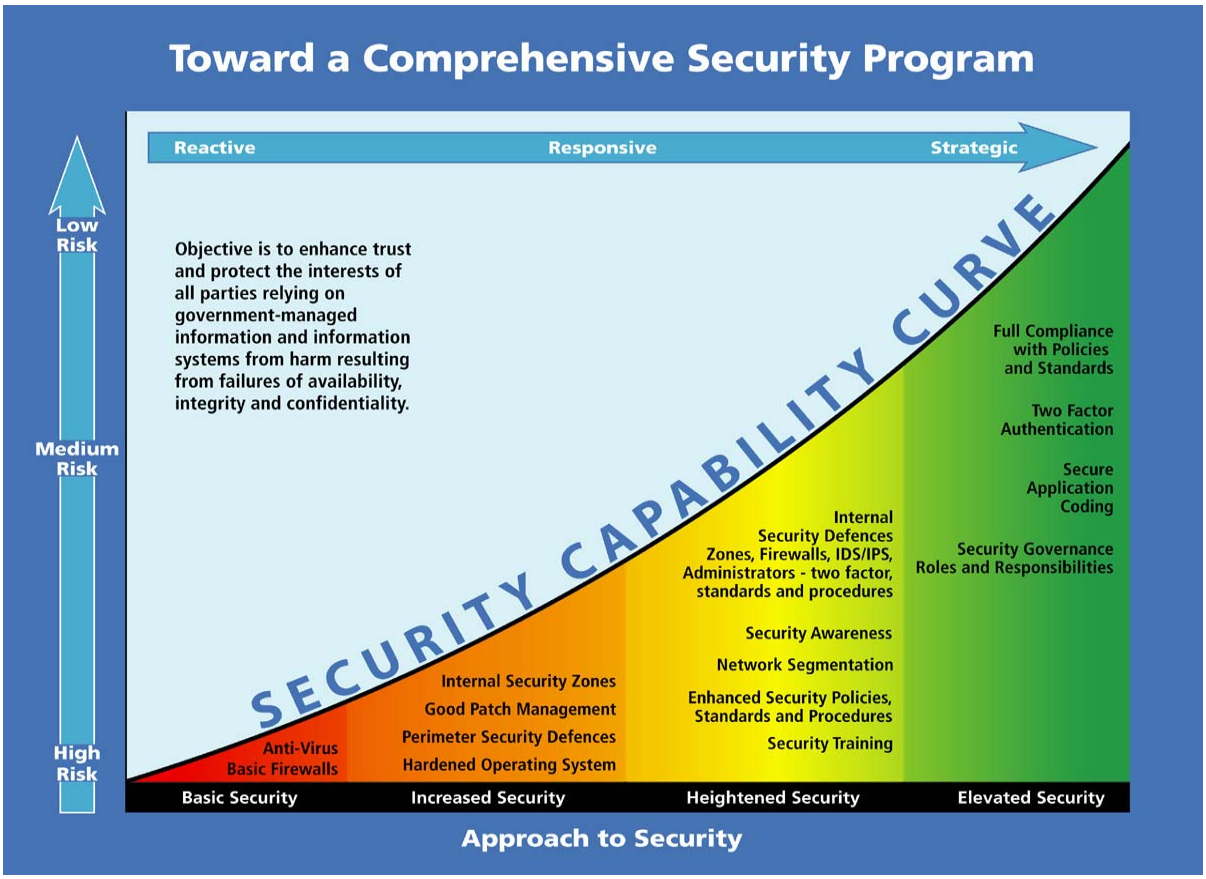
- Security Control Inventory document;
- Detailed Security Program Design document;
- Incremental Implementation Plan for new Security Program;
- Draft recommendations regarding security staffing levels and placement;
- Initiation of a security awareness and education practice;
- Enhanced detection and response capacity.

The Technical Design stream will continue to work on infrastructure upgrades and a plan for the integrated technical Implementations required to support the new Security Program model. This stream will achieve the following by the end of March 2006:

- Interim IDS/IPS by May 2004 with permanent solution designed and in place by Fall 2005;
- Detailed Technical Architecture to support the new Security Program;
- High priority central critical infrastructure housed within the security zone model;
- Standardized technical operating procedures implemented;
- Incremental Implementation plan for the supporting technical infrastructure rollout.

The current budget does not allow for the extension of the security zone model outside of the central core. Likewise, moving corporate and ministry business systems that reside in the core into zones is currently out of scope, but will be addressed in the 2006/07 fiscal year.

Improving enterprise information and technology security in the BC government will be accomplished in phased, incremental steps. Regardless of funding level, IM/IT security capacity and practice can be steadily improved by setting a course based on best practice and periodically assessing progress.



The graphic above shows the Security Capability Curve. As can be seen, the area at the far left of the graph depicts high risk and represents where the province was positioned in September, 2004. By April, 2005, vulnerability shifted into the Increased Security zone as the result of implementing higher security measures and moving from a reactive to responsive security posture. By March 31, 2006, the province will have moved into the Heightened Security zone through adopting more current security technologies and practice. It is recognized that it will take several years and a great deal of additional effort for the new Security Program to move the province to Elevated Security status.

The cumulative effect of achievements noted above will significantly increase government's capacity to defend its information and information systems. Other public sector agencies will benefit as well.

It should be noted that it is already evident that the funding required to deliver the full range of Security Program requirements is more than is allocated at the present time. Once program and technical architectures have been delivered in June, 2005, a more accurate assessment of the remaining vulnerabilities will be possible.

6. BUDGET ESTIMATE FOR FY 2005/2006

Budget Source

CITS	**$300,000**
CIO	**$500,000**
TB approved funding	**$3,000,000**

Total	***$3,800,000***
Capital	***$1,000,000***

Budget Plan	***As per Charter***	***Est. at Apr.1, 2005***
Project Office	**$590,000**	**$592,000**
Policies & Standards	**$400,000**	**$611,000**
Business Requirements & Security Program Design	**$300,000**	**$866,000**
Network Segmentation	**$1,150,000**	**$796,000**
Technical Enhancements	**$1,360,000**	**$935,000**
	----------	**----------**
Total Operating (including amortization)	***$3,800,000***	***$3,800,000***