Background

Information and technology services have become ever more critical to the daily operations of the University of British Columbia. The challenge of securing these services in our complex, decentralized environment has become ever more difficult, particularly when coupled with the rising frequency and sophistication of attacks against information systems. A growing range of federal and provincial legislation has also highlighted the need to safeguard our valuable student and research data across the institution.

Over the last few years, there have been a number of individual initiatives within a range faculties and units to address the IT security challenge. These initiatives have tended to focus on specific issues and have rarely had a campus-wide impact, but should be leveraged as building blocks for a broader IT security framework for UBC.

In 2003, ITServices formed an Information Security Office with a mandate to address IT security issues both within the IT department and beyond. While successful in launching a number of campus-wide initiatives, including anti-spam and anti-virus services, departmental firewall services, and security awareness campaigns, since the departure of the Information Security Officer in 2006, much of the attention of the Office has been focused internally within UBC IT.

In 2005, responding to the requirements of the payment card industry (PCI) to safeguard credit card data, Enrolment Services and UBC IT launched a PCI compliance effort to secure ES' Consolidated Billing service. While initially successful, strict new requirements and a firm deadline for all UBC units to be fully compliant by October 2010 have required a new approach to achieving compliance.

Launched by the Faculty of Medicine in 2007, the COMPAS program is an ambitious effort to address the security and protection of information technology resources across the Faculty. Beginning with a vulnerability assessment and a risk analysis, the program soon established the need for common data security standards across the institution, not just within the Faculty of Medicine.

In 2008, the Office of the University Counsel chaired a broadly representative committee to draft a comprehensive Privacy policy for UBC. After multiple revisions, the policy was ultimately not approved, due in part to concerns about the resources required for units to achieve compliance with the policy.

Rather than continuing to address these key challenges in a piecemeal fashion, an integrated and coordinated institutional response involving broad representation from academic and administrative units is required.

Goal

The IT Security Working Group will define a model for delivering, funding, and governing a comprehensive IT Security framework for UBC. The model will be presented to the IT Steering Committee for their review, before being recommended to the UBC Executive for approval in time for the 2010/11 budget cycle.

The model will:

- Define an overall governance structure for IT Security at UBC
- Outline the roles and responsibilities of the UBC community
- Benchmark and compare security practices and services at other higher-education institutions
- Identify necessary campus-wide security services, standards, and best practices
- Estimate the resources required and cost of providing those services
- Identify appropriate funding sources
- Provide a high level implementation roadmap, including a timeline, critical success factors, and security metrics

Representation

There are a number of critical actors on campus with responsibilities in the area of IT Security. Units that need to be engaged in crafting the model for the IT Security Framework include:

- UBC IT
- Office of the University Council
- Internal Audit
- Comptroller, Finance
- Representative Faculties (2 or 3)
- Additional Administrative Units (1 or 2)

Members of the Working Group will be appointed by their Dean or Administrative head.

Meeting Details

In order to deliver the model for a comprehensive IT security framework in time for the 2010/11 budget cycle, the Working Group will meet on a bi-weekly basis over the next 9 months.

In addition to a Chair and the Members, the Working Group will require part time support from a business analyst for assistance with benchmarking, preparing the financial model, and recording meetings.