

Title

Develop Business Continuity Plans and Address ICT Security Risks

University Themes Supported

- Enhance the Student Experience
- Accelerate Research Momentum
- Build a High-performance and Environmentally Sustainable Organization

Description of Initiative

Context

The University relies upon ICT for its teaching, learning, research and business activities. As doing academic or administrative work becomes synonymous with using ICT, students, instructors, researchers and staff expect service availability that approaches 24x7¹. A recent survey of several administrative departments indicated that the maximum tolerable downtime, for the ICT services upon which they rely, is one day.

In reality, system failures may cause ICT services to be unavailable for days (component failures), weeks (major server failures) or even several months (fire or vandalism of a computer or network centre such as those located in the Administration or University Services buildings). Likewise, Internet attacks can also disrupt services for periods of days or weeks (until the compromised servers or desktops are “repaired”). The affected services may include student registration, grade entry, payroll, purchasing, accounting, donor processing, e-mail, online course content delivery (e.g., Blackboard), PAWS, the campus website, the Library, the campus network, and Internet and phone services.

It should be noted that in addition to disrupting services, ICT security breaches increase the University’s risk of litigation and liability, and potentially damage its reputation due to inappropriate or illegal use of University ICT assets. Such usage includes but is not limited to the distribution of illegal or copyright-protected material and the disclosure of confidential or personal information.

The Initiative

This initiative will close the gap between the expectations for ICT service availability and the University’s current ability to meet those expectations. It will reduce the likelihood of significant disruptions to key academic and business processes due to system failures or security breaches as well as improve our ability to restore services following those failures. It will also help protect institutional data from unauthorized disclosure.

The initiative has three components.

- Develop the University’s business continuity and resiliency plan related to significant failures of institutional ICT systems.

¹ While no individual student, faculty or staff member requires all services to be available at all times, the needs of the institution as a whole combine to produce an expectation approaching 24x7, with little tolerance for service disruption.

The plan will be developed in consultation with colleges and administrative units as well as with senior University management. In order to develop the plan, the University must identify the impact of system failures of varying durations as well as the strategies, with the associated costs, that can be undertaken to reduce the risk of failure, to reduce the recovery time from system failure, and to continue University operations in the event of a failure. The plan will contain only the strategies that cost-effectively address the institution's tolerance for risk.

- Implement the business continuity and resiliency plan.
- Improve the security of University ICT assets and improve the University's response in the remediation of ICT security breaches.

Objectives/Outcomes

The following is a partial list of objectives that will be undertaken using ITS operating funds:

- Implement and support firewall services for computers used in research.
- Increase the level of security between the campus network and the Internet (e.g. by using network address translation, firewalls and additional port blocking).
- Develop business continuity plans for the business processes supported by major institutional systems.

New funding will be required to implement the following objectives:

- Conduct a community education program and provide training relating to ICT security.
- Consult with and assist colleges, departments and researchers to make University computers and application systems more secure.
- Develop an ICT security architecture and practices that will reduce the risk of ICT security breaches.
- Assist in the detection and remediation of security breaches both to contain/limit their extent and to restore normal services as quickly as possible.

Outcomes:

- Improved ICT services to students, instructors, researchers and staff. The risk of service failures and the recovery time from service failures will be reduced offering a higher level of service.
- Increased student, faculty and staff productivity resulting from a reduced number of service disruptions.
- Reduced University risk of litigation and liability due to inappropriate or illegal use of the University ICT assets.
- Increased protection of the University's reputation from harm due to inappropriate or illegal use of University ICT assets.
- Reduced risk of data loss (e.g. research, administrative) or the accidental disclosure of confidential information.

- University units will have a business continuity plan for continuing operations in the event of a failure. The plan will be cost-justified (considers both cost of service disruption and cost of reducing the risk of a service disruption).

Revenues/Costs

Costs

ITS contingency will be used to develop the business continuity plan related to ICT system failures. The cost to develop this plan is estimated at up to \$100,000 (estimated external consulting cost) plus University staff to participate in its development.

It is expected that new funding will be required to implement the business continuity plan. New funding will also be required to improve the security of our ICT systems and to improve our response to security breaches. The table below contains an estimate of those costs.

		Annual Funding Required
Business Continuity	<p>Implement the business continuity and resiliency plan approved by senior University management.</p> <p>The requested budget is for staff costs. Capital funding will likely also be required for hardware and software and is included in the appendix, ICT Capital Projects.</p> <p>The actual cost to implement the plan will depend upon the system availability required by the University.</p>	Estimated on the order of \$500,000 per year
Improve the Security of University ICT Assets and Our Remediation of Security Breaches	Community education and training – 1 FTE (ASPA phase 2) plus materials and ongoing training.	\$90,000
	ICT consultation services for colleges, departments, and researchers – 1 FTE (ASPA phase 3) plus materials and ongoing training	\$110,000
	Development of ICT security architecture and practices to reduce the risk of ICT security breaches (related to the network, servers, applications, databases or desktop computers) as well as assistance in the detection and remediation of security breaches. 4 FTE plus materials and ongoing training	\$400,000

Revenues

This initiative is like insurance; it will not directly generate revenue. It will save the University cost in restoring services in the event of major ICT system failures or security breaches.

The university provides other value to the University. However, it is difficult to put a dollar value to this value: preserving the delivery of academic and administrative online services to students; improved ICT service to, and increased productivity of, the University community due to fewer service disruptions; reduced University risk of legal or financial liability; reduced risk of a loss in University reputation due to the avoidance of some service failures and security breaches; protecting research systems and data thereby reducing the risk of loss of research results.

Performance Measures and Metrics

- Number of business services or processes with a current continuity plan.
- Percentage of computers with ‘sufficient’ security (patches, antivirus, etc.).
- Number of security complaints of University computers attacking other computers.
- Count of incidents (e.g. disclosed data on missing computers; compromised systems; data lost).
- Value of data lost.
- Average recovery time, time lost, and cost caused by a system failure or security event.

Responsibility

- Ed Pokraka, Director, Information Technology Services
- ITS management

Timeline

The business continuity plan relating to the ICT systems used by two administrative units (likely SESD and HRD) will be developed by the end of January 2008.

A timeline for developing plans relating to the other major ICT systems will be created in early 2008 after we better understand the process and effort required. A goal is to develop plans for several more systems (business processes) by May/June 2008.

The implementation of the business continuity plans and ICT security improvements will depend on executive approval and availability of funding.

Comments

Because of the pervasive presence of information technology at the University, this initiative speaks directly to two of the trends identified in the “themes” document for this planning cycle.

- Security: Our world is increasingly a more dangerous place. This was most recently brought home by the tragic events at Dawson College in Montreal in September 2006. Over the next Planning Cycle, emergency preparedness, whether for pandemics, natural disasters, or human attack, will be a persistent preoccupation.
- Systems: Most aspects of the University’s activities are increasingly reliant on technology in general and major systems in particular. System failure, encroachments from external sources, and escalating operating costs for upgrades and replacements are all foreseeable challenges.

It should be noted that the business continuity plans developed by this initiative will only address ICT system failures. Business units may want to develop plans for other risks.