

AT&T Global Services Canada - Whitepaper

Keys to Improving Security and Business Continuity

For Canadian multinationals, the ubiquitous rise of communication technologies such as the Internet, e-commerce, globalization and the convergence of voice and data applications revolutionize the way they conduct business. However, all of this can be rendered ineffective, or worse yet, catastrophic, if any one of these technologies experiences a disruption.

And it appears that this issue of security and business continuity is keeping Canadian IT executives up late at night; according to the 2007 AT&T Business Continuity Study of 100 business executives in the Toronto region regarding business continuity and disaster recovery planning, 66 per cent of Canadian IT executives say business continuity is a priority, with 30 per cent indicating that it has moved up on the priority list due to recent natural disasters or terrorist threats. The report also notes that 77 per cent of executives indicate their companies have established some sort of business continuity plan. Twenty-one per cent indicate their firm does not have a plan in place, with two per cent unsure if the company has a plan or not.

Why Business Continuity is Important

Unfortunately, many companies are still in the dark about the importance of implementing business continuity solutions before disaster strikes – putting the future of their business at great risk.

Survey respondents cited blackouts (29 per cent) and cyber attacks (11 per cent) as the most frequently experienced disasters. Perceived threats to cyber security include internal sabotage (31 per cent), internal accidents (28 per cent), spam (25 per cent) and denial of service attacks (24 per cent), yet only 12 per cent of respondents said worrying about man-made disasters was most likely to keep them up at night. Seventy per cent of IT executives surveyed have already implemented Internet security measures and 59 per cent have established redundant servers or back up sites as part of their business continuity activities.

Indeed, to survive in today's business environment, Canadian multinationals need to achieve a state of business continuity – where critical business processes, work centres, systems and networks are secure and always available to support customers. Business continuity planning involves ensuring that a business is sustainable through a period of significant business interruption caused by a disaster or any other unforeseen disruptive event.

While planning and preparation are essential to ensuring companies can deal with disaster or other disruptive events, actually implementing the tools and technologies that keep business going presents another set of challenges. Shortage of staff, tight budgets and other constraints can sometimes prevent even the best intentioned companies from putting the appropriate pieces in place. All companies, regardless of size, need to identify their critical business components and effectively manage the risk around them, whether from a pandemic, hurricane, earthquake, or any other kind of crisis. Taking a proactive approach to business continuity is essential for being prepared to respond when disaster strikes.

Plans should specify redundant systems, back-up sites, employee communications, and alternative work sites. This also should include a process for maintaining customer communications immediately following the crisis, and proceeding until things return to normal.

Six Steps for Effective Business Continuity

The more accurate a company can be in their planning, the more prepared they will be in the long run. The following outlines six key steps in preparing for any type of business continuity process:

Identify Critical Business Processes and Impacts

The initial step is in identifying the functions are critical to the firm and how diverse disaster scenarios could impact the firm's continuity of those operations. For instance, how could demand for products and services be affected, will demand for products and services grow or decline, will there be different types of impacts,

and what does that mean to the firm's operation? The answers to these types of questions could change the criticality of a given function. This step is vital so that attention and resources can efficiently focus on the most important items.

Perform Risk Assessment, Mitigation, and Management

To ensure a company is equipped to maintain critical business functions during a crisis situation, it is essential to complete a functional Risk Assessment to ensure that it is addressing the critical functions first and making the appropriate investments, both in time and money. The Risk Assessment identifies the critical functions, processes, resources and suppliers/vendors which have the greatest impact on a company's ability to serve its customers.

It also involves the identification and assessment of any potential threats, the existing vulnerabilities, and the probability that a threat will exploit the identified vulnerabilities. This aids in the identification of relative risk exposure from different components of the business, so that fact based decision making on mitigation plans can occur.

Deliver Cost Effective Recovery Strategies

The next step is to define the firm's business continuity strategies. For example, how does the firm want the business to perform and what options are available, does the firm keep the same service level agreements, or does it prioritize work? The results of the Risk Assessment and the identification of Recovery Strategies are instrumental in the development of Contingency Plans to address specific threats. It is also critical that these activities be accomplished in a methodical and consistent way across organizations, so that all parts of the corporation are preparing for the same scenarios, using the same information, and ensuring that the end-to-end plan is functional.

Develop Business Continuity/Disaster Recovery(BC/DR) Plans and Provision DR Capabilities

Contingency plans should be developed to ensure continuity of critical business operations as well as for key suppliers/ vendors. Every Business Unit officer should be responsible for supporting critical business functions appropriately. Contingency plans should identify not only incremental strategic or procedural changes from existing business continuity plans, but also any gaps in capabilities that need to be addressed. It is important to implement any new capabilities prior to the event occurring, to ensure that a business can successfully recover at time of disaster.

Test and Certify

Business continuity plans must be tested on a regular basis to ensure they will be effective at time of disaster. This involves developing a test plan for how a business will test capabilities. It also involves not only conducting table-top simulation exercises, but actual recovery implementations to ensure that the capabilities will operate effectively.

Monitor and Improve Performance

Situations evolve over time and are not static. A firm should consider how changes to a situation and the business environment

could affect a firm's preparedness. To ensure a plan works at time of disaster, business continuity plans should be considered an organizational priority and reviewed regularly. In addition, changes to a firm's business operations must also be reflected in their business continuity plans, whether they are systems upgrades, process changes, or resource restructuring.

Benefits of Managed Hosting Services

Largely due to the complexity of today's business applications and the nature of enterprise businesses, firms should look to the benefits of managed hosting services. Such hosting services range from fully managed solutions with a comprehensive range of applications management capabilities to robust disaster recovery and business continuity services. In the face of tight IT budgets, available resources and limited technical expertise, many organizations may wish to involve a third party in implementing a business continuity program.

By outsourcing the planning and development phases of business continuity, companies can better assess the needs of their IT environment. It can also free up resources, enabling employees to concentrate on the core business while experienced business continuity assessment professionals focus on risk management. A major benefit of outsourcing this planning process is that an objective third party can then effectively assess the organizational continuity requirements, and develop a tailor-made solution that meets the business' specific needs. Ensuring proper network security measures can be a difficult endeavor from a time and cost perspective, which is why many organizations choose to outsource this task to professionals. Investing in planning and working with a trusted partner can ensure that the business continuity best practices put in place are practical, comprehensive and cost effective.

Information is one of the most valuable assets of any company and regardless of company size, security breaches or other unexpected interruptions can happen at any time. Considering that a technology disruption can cost companies untold millions, being proactive about business continuity – before disaster strikes – represents good business sense.

Determining a Firm's Business Continuity Preparedness

Canadian companies can begin to assess their own level of preparedness by asking the following questions:

Mitigate Risk, Protect Mission Critical Data

- Has the business analyzed which business processes, applications and services are most critical?
- Has the business assessed the impact of a potential disruption?
- Has the business created a strategy to mitigate risk?
- What security measures are in place?
- Are key locations hardened and facilities conditioned?

Meet Regulatory Requirements

- Have customers or business partners mandated performance or availability service levels?

- Has the business complied with all current or emerging regulatory requirements?

Invest Wisely

- Has the business quantified the potential costs of downtime or total business failure?
- Has the business developed sound business cases to optimally invest in risk mitigation?

AT&T Managed Security Services

Safeguarding corporate data is a top priority for every company, but managing the right technologies and strategies is no easy task, especially when you consider the complexity of recent viruses and security breaches.

AT&T Managed Security Services provide peace of mind by offering robust protection, proactive monitoring, and around-the-clock maintenance of the gateway to your corporate network. Offering resilient and scalable network security, these services use industry-leading platforms and advanced security standards to provide you with access to the Internet while restricting others from accessing your corporate network.

Rest easy knowing your data is protected by AT&T Managed Security Services.

Dedicated Firewall Service

- Fully scalable to meet your changing needs
- Detailed monthly reports to keep you informed

On Premise Firewall Service

- Cost-effective managed security solution for customers that want the infrastructure located on site
- Available on market leading platforms and technologies

Bundled with AT&T Global Managed Internet service

- 24/7 management of all service components including required hardware and software upgrades by AT&T Security Operations Centre

For more information contact an AT&T Representative or visit www.att.com/canada

© 2007 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners.

11/07 ATT-WP-CA-02



at&t

Your world. Delivered.