

Managing business risk

What senior managers need to know about
business continuity

Information and Communications Technology (ICT) has become more vital than ever to the success and survival of many businesses. As such, eliminating the risk of business interruptions with respect to ICT infrastructure is becoming an ever more critical cornerstone to ensuring success.

In recent years, the perception of business risk has evolved well beyond typical disaster recovery scenarios. Today, business continuity planning requires a much broader focus that considers various risk factors that impact day-to-day business efficiency. In the case of ICT, this can include anything from network slowdowns and power outages to wholesale system failures.

This whitepaper will examine the role of business continuity and why it has become such a critical part of competitive strength in today's business world. It will also appraise how effective business continuity planning for ICT resources can play a key role in optimizing productivity, security and compliance.

More specifically, the role of business continuity will be examined in the context of three critical components:

- Business security
- High availability of business systems
- Business recovery

The information provided will help companies gain a better understanding of what these areas encompass; how to assess each in terms of business continuity requirements; and the steps to take to implement a plan that addresses their specific needs. In addition, we will outline how infrastructure and professional services can play a role initiating and enabling continuity planning processes and procedures – and be leveraged for success.

Business continuity is an issue that is top of mind for all types of businesses today. While the spotlight tends to be on major crises, the job of ensuring business continuity is much more than putting processes in place to respond to catastrophic events. In fact, catastrophic events represent only a small portion of risk in today's business environment.

According to the UK-based Business Continuity Institute, business continuity management “has emerged with a clear identity as a wide-ranging management discipline and is no longer synonymous with ‘Disaster Recovery’.” Its research also revealed that more companies have specific disaster recovery plans than general business continuity plans.

A point of interest in the same study states that all organizations with a business continuity plan also had a disaster recovery plan. This is because disaster recovery tends to be a more limited discipline. As such, it naturally falls into place within the broader context of a business continuity plan. Take care of the bigger picture and the smaller one falls into place.

A key part of business continuity planning is information and communications technology (ICT). Most businesses today rely on their ICT infrastructure to support the continued operation of their business. The more critical the data or application to business operations, the more important it becomes to maintain the supporting infrastructure.

Interruptions to ICT performance such as network slowdowns, viruses and power outages, can take on many forms and pose vastly different levels of risk to your business. For example, even a short interruption to systems that are integral to revenue streams – such as e-commerce – could have a large impact on your operation's bottom line. At the same time, bullet proofing an infrastructure from business interruptions is a complex, costly and challenging task. For many businesses it's a job that is often beyond available budgets and staffing.

There are many reasons why business continuity represents an added challenge:

- Few businesses have enough in-house resources or skill sets to effectively manage and monitor network and system performance. In addition, day-to-day back-up and reporting functions can be labour intensive and prone to human error.

- Infrastructure resiliency requires a dedicated data centre and all the necessary back-up processes. Often times the technology foundation needed for built-in redundancy and resiliency is too expensive and difficult for IT departments to maintain.
- There is a growing burden on companies to manage and follow the increasingly stringent regulatory requirements to ensure the secure collection, processing, storage, recovery and disposal of data.

In a survey of 130 Canadian firms, security was the #1 reason for upgrading their networks. Two-thirds of Canadian businesses reported security breaches within the last six months, and nearly 90% acknowledged that lost productivity was a result of these breaches.
– IDC

Rather than using a ‘patchwork’ approach, businesses need a cost-effective and flexible way to address these challenges. The cost of doing nothing is much too high.

Measuring the cost of risk

Leger Marketing reports that 72% of Canadian business executives have no plan in place to address disaster recovery and business continuity. At the same time, an IDC report shows that two-thirds of Canadian businesses had reported security breaches in the last six months, with 90% of those acknowledging lost productivity.

How that lost productivity affects revenue streams and profitability can differ depending on the type of business and level of in-house expertise. Essentially, the level of risk to the business is measured by the likelihood of an occurrence and the size of the impact that occurrence will have on operations.

Respondents in the Business Continuity Institute’s research study specified areas of consideration when engaged in assessing the cost of risk. These included: employee productivity, government regulatory requirements, the ability to retain and attract investment, protecting employees and new business development.

Choosing the right solutions to mitigate risks requires an understanding of areas and levels of risks that are

specific to the business. In other words, the greater the real or perceived risk, the greater the focus and need to prepare for predicted or unforeseen events in a timely manner.

What does business continuity for ICT really mean?

The role of a business continuity plan is more than simply establishing processes for rapid recovery if and when an IT infrastructure is compromised. Business continuity management is a broader-based discipline that looks beyond physical requirements to less tangible concerns such as staff productivity, supply chain efficiencies and overall reputation. All of these are inextricably linked with ICT integrity and performance.

To effectively support business continuity, ICT solutions must address and integrate aspects of:

- **business security** – making sure the infrastructure is secure and only authorized people have access
- **high availability for business systems** – ensuring critical infrastructure is always up and running
- **business recovery** – when all else fails, making sure that the systems and processes are in place for rapid recovery

Simply put, if a company can say with confidence that the infrastructure supporting its business model is secure, available and can recover quickly, it has a good business continuity plan.

Following is a more detailed outline of what each area entails.

Business security

This is the discipline of securing the technology infrastructure, data content and applications from external and internal threats in order to mitigate risks to the business, ranging from stolen information to system downtime.

Areas of consideration include:

- protecting networks from disruptions such as viruses, spam and other cyber threats
- expanding access to information while ensuring appropriate authorization for users

- ensuring compliance with data privacy and other regulatory requirements such as PIPEDA and Sarbanes-Oxley
- creating a proactive strategy to manage the total cost of security

80% of emails sent in December 2006 were spam.
 – Globe and Mail, January 2007

High availability of business systems

Ensuring 24/7 availability of ICT systems supporting business operations is all about minimizing the risk of downtimes as a result of hardware, software or telecommunications failures. An integral part of this process is assessing and understanding potential single points of failure throughout an integrated system.

Specific areas of focus to include in planning are:

- requirements for keeping mission critical hardware and applications running 24/7
- ensuring that customers, employees and partners can always communicate with the business
- maximizing employee productivity by reducing the risk of downtime for desktop PCs, applications and peripherals
- regulatory compliance

Business recovery

A key component of business continuity management is putting measures in place to minimize the risk and potential impact in the event of a business interruption. This is commonly known as Disaster Recovery Planning (DRP).

As highlighted earlier, interruptions to ICT performance can take on many forms and pose vastly different levels of risk. Catastrophic events, though rare, can have a considerable effect on the ability of a company to stay in business. Less “disastrous” but more frequent events, such as equipment failure and human error, can also affect business productivity, efficiency and profitability.

Businesses should therefore focus on strategies that allow them to recover and continue operations. These strategies can help to avoid productivity or revenue losses, as well as to adapt to changes as quickly and efficiently as possible.

Considerations include:

- continuing operations during repairs to damaged or failed equipment
- enabling recovery of damaged or lost business data or information
- minimizing timelines to resuming full operations
- developing and maintaining a recovery plan – this can encompass issues such as enabling network access from outside the office, as well as ensuring safe remote storage of redundant systems and applications

Most business disruptions are actually the direct result of soft failures. Recent studies have shown that as many as 80% of mission-critical application processing disruptions are directly caused by people or process errors. The other 20% percent are the result of technology failures, environmental failures or catastrophic disaster.
 – Gartner

How to assess business continuity needs

Business continuity requirements can vary dramatically depending on the business model and employee or customer requirements. A company that relies heavily on e-commerce as a source of revenue would have different priorities than one whose livelihood is not critically linked to on-line applications or real-time data.

It is challenging for businesses to be all things to all people at all times. Sometimes they don’t need to be. The resources needed to support 100% availability can be incredibly complex and costly. Many businesses simply don’t have the level of in-house expertise and resources to ensure ongoing network and system monitoring. Back-up resources for full recovery can also be beyond one’s budget or immediate requirements.

The greater the real or perceived risk the greater the focus and need to mitigate that risk. So it is important that businesses understand what those risks are, their potential impact on their specific business operations and their level of priority. For example, how much impact will a short-lived interruption to email services

have on operations? Does recovery of auditing and financial applications have a lower priority than mission critical VoIP or other communications services?

During the first half of 2006, there was an average of 6,110 Denial of Service (DoS) attacks per day.

– Symantec Threat Report 2006

Making the appropriate decisions is based on a thorough understanding of areas and levels of risks specific to the business. A critical first step is to perform a risk assessment.

This entails:

- identifying levels of risk by assessing areas of impact to business operations, factoring in both short and long-term business interruptions, and classifying them as high, medium or low based on their likelihood
- quantifying the cost of the risk by looking beyond the obvious system and support costs to include areas such as lost productivity, lost revenue and brand reputation
- prioritizing security, availability and recovery needs
- assessing available resources such as infrastructure, in-house expertise and budgets
- determining what is required to “fill the risk gaps” and invest accordingly

Where in-house resources are in short supply, businesses can engage professional services to help assess risk, examine and identify areas of exposure and develop an appropriate course of action.

Business continuity through hosting services

For many businesses building and maintaining a secure, fully redundant and easily recoverable data environment for ICT is something they may be unable to effectively manage on their own. Beyond the cost issue, the complexity involved is often well beyond the reach of available in-house expertise and facilities.

A viable option is infrastructure hosting services. Available in several variations, these services provide flexible, affordable solutions to help address key issues such as:

- managing IT complexities
- mitigating risk from system downtime
- increasing productivity
- reducing IT costs

By leveraging the leading edge resources of data centre facilities and technical experts, businesses can realize all the benefits of a secure and redundant, climate-controlled environment that includes round-the-clock availability and support, reliable power supply, network connectivity and back-up power generation.

Hosting services are typically offered as either colocation or managed services. The choice will depend on specific business continuity requirements, budgets, available in-house resources and expertise.

Colocation hosting services allow businesses to leverage a data centre facility for housing all or part of their own IT infrastructure. These services are ideal for housing either primary IT or back-up systems.

With managed hosting services, businesses can contract a specialist to supply and implement the dedicated servers and software necessary for business operations. The provider is responsible for managing the performance of the IT infrastructure, including server hardware, bandwidth, back-up, security, databases, operating systems and other software applications.

Hosted services can help businesses to:

- access a highly sophisticated IT infrastructure at a fraction of the cost to build and manage an in-house data centre
- reduce operational risk by ensuring performance, security and 24/7 availability for business systems backed by service level agreements
- minimize the complexity and cost of compliance with government or industry regulations by leveraging standardized processes and technologies for security, storage and recoverability of data
- optimize business growth by re-focusing in-house infrastructure management resources on revenue generating initiatives
- prepare for future growth by enabling full and easy scalability of infrastructure

Businesses that want to maintain their infrastructure in-house but lack the IT support skills can also opt for remote managed services. In this model the service provider will offer remote 24/7 monitoring and system support for any or all components of a business' infrastructure, including servers, LANs, workstations, printers, security and back-up.

Finding the right resources

Business continuity planning is critical to survival in today's competitive environment. It is important to understand that it is not only major disasters that can have a serious impact on bottom line results and overall performance. Minor interruptions from internal errors, system misuse, viruses, infrastructure instability or delays in technical support can increase costs and reduce business productivity because they can consume extensive human and financial resources.

In order to avoid the trap of overspending and underachieving the desired results, the first step is to commit to developing a business continuity plan. This will provide the foundation needed to assess risk, determine its impact, prioritize needs and put the appropriate measures in place.

72% of Canadian business executives have no plan in place to address disaster recovery and business continuity.

– Leger Marketing

Where resources are limited, there are ample opportunities for businesses to leverage the offerings of industry specialists to provide the support needed. Available solutions can help reduce operational risk and costs and improve overall productivity and performance.

The key is finding suppliers that are well versed in risk assessment, business impact analysis and infrastructure and system support. After all, ensuring business continuity for ICT resources is a complicated and integrated discipline that requires considerable cross-functional expertise and world-class infrastructure capabilities. Given the growing reliance on ICT infrastructures, having the right services in place and the right long-term partnerships are integral to present and future survival.

Solutions for business continuity from Bell

A growing number of companies are successfully eliminating the risk of interruptions to their essential business operations by enlisting Bell to safeguard their ICT infrastructure.

Bell offers a comprehensive portfolio of professional assessment services and ICT infrastructure planning, procurement, implementation and management services to help businesses ensure:

- **business security** by securing infrastructure, data content, applications and corporate access
- **high availability of business systems and operations** by supporting 24/7 operation of ICT hardware and applications
- **business recovery** through enabling rapid business recovery with back-up resources and maintaining compliance with data privacy regulations

Bell solutions provide companies with a cost-effective and flexible alternative to managing and maintaining systems in-house, while reducing the level of daily strain on IT staff.

Following is a matrix that describes the Bell business continuity service model for ICT:

	Business security	High availability	Business recovery
Professional services	<ul style="list-style-type: none"> • Vulnerability assessment • Configuration and installation • IP Networking 	<ul style="list-style-type: none"> • Network assessment • Configuration and installation • IP Networking 	<ul style="list-style-type: none"> • Disaster recovery planning • Configuration and installation • IP Networking
Infrastructure solutions	<ul style="list-style-type: none"> • VPN solutions • Firewall solutions 	<ul style="list-style-type: none"> • Business communications systems • Virtualization solutions 	<ul style="list-style-type: none"> • Secure remote access solutions • Virtualization solutions
Co-managed and fully managed services	<ul style="list-style-type: none"> • Business internet security • Managed security solutions • ProConnect™ and Ethernet wide area network (WAN) services 	<ul style="list-style-type: none"> • Hosting infrastructure services • Managed move service • Managed storage solutions • ProConnect and Ethernet WAN services 	<ul style="list-style-type: none"> • Accelerated delivery service • Express servers from Bell • Hosting infrastructure services • Managed remote back-up and recovery • ProConnect and Ethernet WAN services with diversity • Megalink™ diversity for PBX • Toll-free emergency routing

The Bell advantage

Being one of the most experienced providers of ICT services in Canada, Bell offers:

Experience and reliability

Bell has been delivering reliable communications services to Canadians for over 125 years. Our ICT services have been built on significant investments in key infrastructures, including data centre facilities and a coast-to-coast IP network.

Proven expertise

Our experienced team of cross-functional professionals understands the evolution of technology and has a proven track record of successfully delivering business continuity solutions to businesses.

Creating value

Bell offers an unrivalled suite of solutions built around security, operational continuity, recovery and compliance. Leveraging extensive partnerships with industry leaders, Bell is your single source to assess, design, implement, integrate and manage your current and future ICT business needs.

For more information contact your Bell representative or Bell Certified Partner.

bell.ca/businesscontinuity

