

I D C E X E C U T I V E B R I E F

Business Resilience and Disaster Recovery: Challenging Misconceptions

June 2006

Dave Marks, Joe Greene, David Sent

Sponsored by: TELUS

An interruption to the continuous operations of business comes at any time, takes a range of forms and has varying degrees of impact. Yet, Canadian organizations are lax when it comes to ensuring that revenue, productivity and reputation are properly protected. This Executive Brief is the first of a three-part series which together explore good planning, future direction and options available to businesses in preparing their business resilience, IT security and disaster recovery plans:

1. This, part one, presents a high-level overview of business resilience. Read the next two papers in the series for a deeper dive.
2. Part two offers guidance and actions that an organization can take to build an effective business continuity plan with the least possible investment required.
3. Part three explores the benefits of using a managed security service provider in building business resilience.

INTRODUCTION

Businesses use technology to create competitive advantage, improving their ability to respond faster to changing market conditions and new business requirements. The same is true with business resilience and disaster recovery – technology is the enabler.

IDC Canada's 2006 *Top Executive Survey* revealed that the top area of IT focus for executives is implementing new strategic applications for competitive advantage. Another question in the same survey showed that their top concerns with IT's ability to support their business is both reliability and uptime. As will be discussed, these two top areas of focus both being given the same importance and

priority is not coincidental: strategic investments can take the form of ensuring reliability as reliability is itself strategic.

Effective planning in business continuity – to prepare for and recover from disasters, large or small – requires a delicate blend of sound business operations and flexible technology deployment. Unfortunately when organizations consider business continuity, disaster recovery and risk management, they often equate it too closely with shoring up weakness in technology. Although extremely important, technology investment is the result of proper planning. And where technology investment is required, it needs to support established policies and processes, while at the same time being flexible and scalable enough to support ongoing business changes.

Consider IT security, generally thought of either in a broad context such as firewalls or end-user context such as antivirus and anti-spyware. These point products are limited to addressing specific types of attacks and protecting large assets, whereas increasingly, security practitioners consider a far more holistic approach to protection. Business today exists in an information economy and data is the single most valuable asset. Like a firewall protecting a PC (or any other device or application for that matter) point technologies only go so far. To improve your Information Security position, you must understand the various attack vectors by, for example, keeping up with analysis of your log files (if you even look at them at all), and ensuring that data is protected from multiple angles. It is also prudent to have data storage policies in place to make certain that data is available when needed.

Putting in place the best technology defenses, by themselves, will not guarantee continuous operations for a business. There must be a proactive process including business leaders and employees to develop practices, policies and procedures that identify (even if at a high-level) appropriate protective measures through the lens of business context. In Canada, 41% of large organizations currently consider their IT security strategies and policies major issues.

As IDC explores in the second paper, reducing risk through business continuity planning doesn't need to be painful. The more granular and specific your efforts get, the better. By taking stock of critical assets, identifying vulnerabilities with these assets and matching vulnerabilities with threats that can harm the assets, an organization can then formulate what action to take when an interruption occurs.

BUSINESS RESILIENCE AND BRAND PROTECTION

In addition to preserving revenue opportunities and productivity, maintaining business continuity protects and even enhances brand image. It is at this point that the agenda of both the CIO and CEO converge. This is the crossroads of technology enablement, value creation and corporate branding.

Consider the following examples within the context of good planning and the relevance to positive brand image:

- During the 2003 blackout in eastern North America, a prominent multi-billion dollar private pension fund continued its operations the very next day at the command centre of its service provider ensuring no loss of transactions and minimal inconvenience for its staff and stakeholders.
- During the SARS outbreak in Toronto, some financial companies had established rotating teams to manage core operations in separate locations preventing physical contact thus making transmission of the disease unlikely. The only permitted forms of communication between the various teams were telephone and email; even the use of physical mail was prohibited.
- Only days after the catastrophic damage of Hurricane Katrina, Home Depot powered up some of its operations in a store a few miles from downtown New Orleans and opened for business. In an area without electricity and running water, Home Depot stood as a testament to business resilience and provided not only much needed supplies, but also hope. The ability of Home Depot to resume so quickly is partly based on its own core competence of offering products and services to help its own customers renovate and rebuild their homes and partly based on its excellent business resumption planning. With the help of service providers restoring communications, responding and rebuilding the store was almost second nature to the company.

In the examples above, these companies resumed operations from total technological failure, biological epidemic and a natural disaster by having plans in place to protect their business processes. These businesses built in the necessary resilience that allowed them to continue operations.

Brand is a valuable and intangible asset that itself can't be locked down as a server or network can. A fundamental way to nurture brand value is by continually and consistently delivering service/product to customers, partners and suppliers. This extends beyond backing up data and beyond recovery of lost files. Brand resilience is about the proactive process of building a brand that persists, *especially* during a time of instability.

Those who expect products or services to arrive in a timely manner will likely forgive a short period of downtime if it occurs infrequently; however in this patience-thin, on-demand world, customer expectations are only getting tougher.

CONSIDERATIONS

As Canadian companies increasingly serve and are served by global markets, they face more risks through a broader attack surface. These threats range from directed and undirected security attacks to

downtime occurring anywhere within customer or suppliers environments. As a result, Canadian businesses are forced to rethink some traditional methods. This is especially true given the increase in regulatory controls and expected transparency for business operations.

Whether building a resilience plan for the sake of being compliant with legislation, to protect your brand or to protect revenue, organizations need a robust checklist of internal capabilities. In the example of the private pension fund, it would not have been advisable for the financial services organization to build redundant power systems for the rare occurrence of a province-wide blackout. However, outsourcing mission critical systems to a third-party hosting service proved to be a sound business decision and enabled the organization to mitigate specific risks.

In building a business resilience plan to prepare for disruptive changes, both natural and human, IDC provides the following points:

- **Consider a CRO.** Given the size of an organization it is prudent to create the position of a Chief Risk Officer whose mandate is to ensure an organization's preparedness for risk. The responsibilities of the CRO may also be to broker CEO and CIO common interests. This position will amalgamate the often distributed responsibilities of risk and response into a coherent framework.
- **Know your limits.** Any organization must ask itself how risk tolerant it is; another item to be handled by the Chief Risk Officer. Limits should at first be considered outside of any cost model. This will provide a clear and true understanding of the organization's risk profile, and a solid overall context within which to consider areas such as IT security.
- **Assess resource/capability availability.** Poll internal resources to identify if the organization has competent and available resources to build in-house capabilities. (*Subject of part two of this series.*)
- **Triage based on strengths.** Decide what can be done internally, what needs to get developed in-house and what you'll need to draw from external providers to help manage. An organization doesn't need to categorically hand-over all parts of its functions to an outside firm; rather it should be a gradual transfer of risk management responsibilities within a partnership of those areas where an organization doesn't have the resource internally to create the competency. Ultimately, the ownership of the risk remains in the hands of the organization. (*Subject of part three of this series.*)
- **Carry-out due diligence on providers.** Pick a service provider that has a strong track record, strong technical expertise and aligns with the goals of the organization.

- **Take your pulse, at least annually.** Periodically, conduct a health check with internal stakeholders and external consultants or auditors.
- **Test.** Test your preparedness plans. A recent survey of large enterprises in Canada reveals that of the 67% who have a disaster recovery plan in place, 25% have not tested it.
- **No one-size fits all.** There are many ways to analyze risk, with some more appropriate to business and IT than others, and some better suited to organizations of a given size. However, one consistency is that business continuity needs to be conducted across organization functions bringing all stakeholders together at the same time – or at least to get buy-in and plan review by the stakeholder (including business, IT and security professionals).

A typical question raised on this topic is: How do you put plans in place to prepare for an unfortunate eventuality when you don't even know what it is or where it might come from? Fact is, it is impossible to know at all times the type and direction of a risk to business. Until recently, there were no browser drive-by attacks. There were no large-scale distributed denial of service (DDoS) attacks launched from the combined power of many hijacked PCs (known as a botnet). And there will undoubtedly be more surprises in the future. But preparation should begin by asking: How prepared is my organization to handle known threats? And what are the assets the organization needs to defend?

CONCLUSION

While brand and reputation is arguably the most valuable asset to an organization, complacency is arguably the most detrimental of all characteristics when it comes to business continuity.

Business executives must be cognizant that in preparing against and recovering from disasters, technology is simply one domain they must consider. Sound business vision, leadership and the recognition of corporate competencies as well as risks are an essential part of building a business resilience plan.

Central to this activity is the mindset that the process of planning is the best approach to business resilience, not the arrival of a plan. The former is an adaptive activity that considers the unending changes in the market place; the latter is an activity that creates a static state.

COPYRIGHT NOTICE

The analyst opinion, analysis, and research results presented in this IDC Executive Brief are drawn directly from the more detailed studies published in IDC Continuous Intelligence Services. Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from IDC. Contact IDC Go-to-Market Services at gms@idc.com or the GMS information line at 508-988-7610 to request permission to quote or source IDC or for more information on IDC Executive Briefs. Visit www.idc.com to learn more about IDC subscription and consulting services or www.idc.com/gms to learn more about IDC Go-to-Market Services.

Copyright 2006 IDC. Reproduction is forbidden unless authorized.