



**a higher level of
managed IT services**

Practicing Safe Computing in the 21st Century

Business Continuity Solutions for Real Business Issues

Face the Facts:

The current reality is that corporate Canada must ensure that their data and employees are protected in the event of a disaster, whether man made or natural. Not only do executives have to make a promise to their board, investors, employees and customers, but they must also meet compliance and regulatory requirements, which in turn hold them accountable for taking the proper steps to mitigate the impact of a disaster.

Organizations today are facing an exponential rise in threats from viruses, worms and attacks that put their mission-critical applications and data at risk. Now we are also seeing an increase in threats from terrorists, hurricanes and a potential pandemic which would pose a threat to an organization's most precious resource, its employees. Business leaders need to take the steps to protect their systems and ensure their critical staff has a safe and secure alternative work environment should they not be able or willing to enter a disaster zone.

Ask Yourself the Tough Questions:

- Do you feel your organization is prepared to deal with a major disaster?
- Are customers concerned about your disaster preparedness?
- How would a major power or network outage affect your business?
- Did you change your disaster preparedness practices after a major disaster such as power outage, virus, worm, SARS, fire, floods, terrorists, or the threat of a major pandemic?
- What in your opinion is the greatest threat facing your organization?
- How much do you spend on disaster preparedness?
- What's the best course of action to avoid a major systems outage or disaster?

"By outsourcing to Fusepoint, we can replicate our site on a minute-by-minute basis and have the infrastructure in place to access our documents in case of an unforeseen event occurring whether that is a flood, fire or pandemic. Our clients never have to worry about losing documents."

Mark Bonner
IT Director
Goodman and Carr LLP

Seven Keys to Unlock the Secrets of Success:

1. Focus on mission-critical applications:

Identify the critical systems that are driving your business and complete a threat and risk assessment. What are all of the possible points of vulnerability and what is the impact to your business?

2. Measure your cost of downtime:

When the critical systems you have identified above are down, what is the impact to your bottom line and company brand? This should drive your budget conversation with your CFO. Your goal is to create a hundred thousand dollar solution to a million dollar problem, not the other way around.

3. Security is not just about technology.

It is about the integration of people, processes, and technology where malicious activity is quickly identified, escalated, and terminated when required.

4. Identify secondary locations for

critical staff to work, ensuring access to technology and hardware is on hand and available to them. For example, Hot-seats in secure facilities with laptops accessing remote databases.

5. Consider geographic disparity of systems.

In the event that one facility is down you have complete and immediate fail over capability through Global Load Balancing.

6. Monitoring, educating, and reporting:

Create an external monitoring process for notification from key governmental agencies and industry publications, educate your employees on the latest information, and report impact back to executives.

7. Create a program, not a one-time event.

Keep your disaster recovery plan evergreen, test it, document changes and test it again for continuous improvement. You're only as safe as your weakest link and if you don't test, you won't know what you're missing until it is too late.

Being proactive and prepared is the key. Monitoring threats – no matter what form – and implementing and testing policies and processes should occur on a regular basis.

If a positive can be found from recent events, it's a growing awareness among executives that information systems represent the lifeline of their organizations – but many still require more than a gentle reminder. Protecting corporate assets and reputation is everyone's responsibility – not simply the IT department – and steps need to be taken to ensure proper infrastructure, services and resources are in place long before an organization faces costly, business-altering decisions in the wake of a crisis.

Practicing Safe Computing in the 21st Century

*Business Continuity
Solutions for Real
Business Issues*

**To find out more, please visit our Web site at:
www.fusepoint.com or call 1.877.387.3764**