


[Insurance News](#)
[The Press Room](#)
[Current Issue](#)
[Archived Issues](#)
[Email Newsletter](#)
[Insurance Links](#)
[Insurance Careers](#)
[Insurance Marketer](#)
[Publications/Directories](#)
[Classified Ads](#)
[My Events Calendar NEW](#)
[Submit Your Event](#)

## View Stories by Category

### Canadian Underwriter, June 2003

 [Printer friendly version](#)

## Wired World

### Facing Disaster

By *Stephen McWilliam*

When you read the headlines these days, there is a sense of susceptibility and unease amongst top executives when it comes to the security of their critical information systems - most often the lifeblood of their organization. Whether it is computer viruses running amok, the theft of vulnerable hard drives, or the growing threat of cyber terrorism, the concern is palpable.

Articles in related categories

[Technology](#)

The insurance industry, and financial services as a whole, with its wealth of highly confidential customer information, particularly financial records, is one of the industries most at-risk in terms of the fallout of such an incident. Gartner Group, a leading U.S. based research firm focused on trends in information technology, estimates that two out of every five enterprises that experience a disaster will go out of business within five years of the event. Ernst and Young suggest that more than 30% of companies believe that computer system failure is the most significant threat to their business, with nearly 60% believing the risk to be moderate to high.

### Up and running

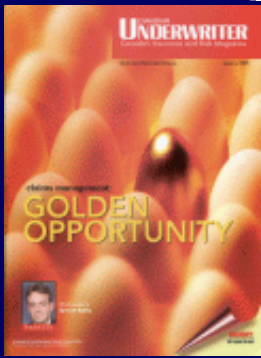
Ian James, Director of IT for B.C.-based Family Insurance Solutions Inc., has witnessed the effects of a critical system failure firsthand. And, he has learned from the experience.

As a provider of private auto and residential insurance in B.C. through more than 100 brokers, accounting for over \$50 million in annual business, Family Insurance distinguishes itself in the industry by bringing operational efficiencies to brokers through a "real-time point-of-sale system" that relies almost solely on workflow automation. While that brings a lot of value-add to the broker, for the insurer there is little in the way of manual workarounds to support policy issuance and maintenance in the event of a system failure.

"Therefore it's absolutely essential that we keep the systems up and running," says James. "Our system enables all of our underwriting decisions to be made in real time. If our system is down, it effectively halts the entire policy issuance process. Were we to go down for any extended period of time, it's not just the revenue that's lost - future revenue and market growth could also be impacted." Any disruption in service not only means lost revenue and opportunity, it also tarnishes a firm's image and credibility - all greatly affecting an organization's bottom-line if there is no proven plan in place to get systems and staff back up and running.

### System failure

Such a crisis hit Family Insurance in 1999 - which served as a "wakeup call" to the firm's senior executives. Ironically, it was only a simple component failure in a server that caused the failure across the system, but without sufficient backup processes available, the



December 2004

[Primary Insurer Strategies 2005](#)

company faced disaster. In hindsight, James acknowledges that if the company had a business continuity plan in place, systems could have been recovered within the hour. However, there had been no "plan", and under the pressure and duress of the moment, with call center brokers demanding to know why the system was down, mistakes were made, leading to a period of interruption that extended to the better part of a day. "When I think back to '99 I ask myself, 'why didn't we have a business continuity plan? Why wasn't appropriate business continuity addressed?'" says James. "Like all businesses we were focused on the day-to-day operational issues, putting out fires. That kind of planning was perpetually deferred since it involved a lot of people in the company, all of whom were very busy."

### Recovery strategy

After the incident, Family Insurance turned to Fusepoint to implement an off-site recovery strategy that now replicates all of the insurer's critical systems off-site. In addition to the reinsurance a business continuity plan offers from a technical perspective, James says, it also outlines a step-by-step procedure that allows staff to make very calm and rational decisions at a time that could potentially be one of duress.

"I believe for those operating within the financial services industry there has been an increasing amount of attention paid to business continuity," he adds. "One of the big drivers is emerging security issues. We look out in the community and we see increasing risk of business interruptions from many sources - for many of us 9/11 was the call to action."

The Wired World welcomes your feedback. Contact us, via E-mail at [vikki@canadianunderwriter.ca](mailto:vikki@canadianunderwriter.ca)

[Table of Contents](#)



[Contact Us](#)

Forward This Article  
to a Friend -

Comment On  
This Article -

Copyright © 2005 [Business Information Group](#). All rights reserved.  
A member of the [esourceNetwork](#)

[Business Information Group Privacy Policy](#)