CURIE Protecting Our Universities

Risk Management Newsletter

Canadian Universities Reciprocal Insurance Exchange

May 2008 Vol. 19 Issue 02

CURIE Celebrates Its 20th Anniversary

January 1, 2008, heralded a significant milestone in CURIE's history – the organization's 20th anniversary.

It's a milestone worth acknowledging: in the last 20 years, CURIE has grown to be the largest higher education property and liability insurer in Canada. Today, CURIE provides stable, cost-effective insurance and comprehensive risk management programs for 58 member universities, which represent almost 600,000 students from nine provinces.

A Desire for Cost Control and Stability Spurred CURIE's Creation

CURIE owes its genesis to a number of unexpected and costly mid-80s court decisions. These decisions prompted Canada's liability insurers to respond in ways that prevented universities from either obtaining insurance or affording to insure many programs and activities. These responses included withdrawing from writing liability insurance business, declining to renew policies, boosting premiums up to tenfold, and restricting or dropping coverage for essential programs and activities.

This difficult situation inspired Eric Fleming, risk manager at the University of Toronto; Ken Clements, executive director with the Canadian Association of University Business Officers (CAUBO); Al Simms, the University of Manitoba's legal advisor; and others to work with consulting actuaries The Wyatt Company to lay CURIE's groundwork. Thanks to their efforts, CURIE was formally launched on January 1, 1988, when 42 Canadian universities began pooling and collectively insuring their property, liability, and errors and omissions risks. By forming their own risk financing and insurance entity, these pioneering universities sought to better control their insurance costs, their financial health, and their programs.

In fact, CURIE's founders created the organization to stabilize insurance premiums, broaden liability exposure coverage, add catastrophe and earthquake coverage, offer higher and more flexible policy limit and deductible options, and focus on the unique risk management needs of universities—a mandate that remains largely unaltered to this day.

Focus on Subscribers Underpins CURIE's Success

During its early years, CURIE was managed by the Toronto office of Marsh Canada Limited (formerly Johnson & Higgins), a large international insurance broker. In 1992, CURIE opened its own office in Oakville, Ontario, with a staff of five. These dedicated professionals sought to serve CURIE's subscribers

Continued on page 2

In this issue…

- CURIE Celebrates Its 20th Anniversary
- Crisis Communication 101: Ensuring that key message gets out
- Questions and Answers
- Developing Information Technology Recovery Plans
- Year 2007 Financial Update
- CAUBO 65th Annual Conference
- CURIE University & College Risk Management Conference
- CURIE Launches New Web Site!

Serving Our Members

We understand that the increasingly broad and complex scope of university operations can present you and your colleagues with many, and sometimes unusual, risk and claim-related questions. It's most likely, however, that the CURIE staff, through its dealings with the other 58 CURIE subscribers, have encountered issues like yours. If not, we're highly experienced in finding answers through our network of contacts.

Don't hesitate to call or email us if you have a question. We are here to help you manage your risks and protect your university – and we are always looking for ways to serve you, our valued members, better.

Continued from page 1

exclusively while dealing with important organizations in CURIE's commercial insurance and regulatory environments.

This formula has proven exceptionally successful. Today, CURIE's subscribers enjoy a host of advantages:

- Insurance premiums substantially below market prices
- Group pricing based on actual loss experience
- Stable premiums (notwithstanding the cyclical nature of the insurance market, CURIE has been able to largely avoid the adverse impact of industry pricing hikes)
- Insurance tailored to their needs, including coverage typically unavailable in the market
- A wide breadth of risk management services
- Access to an experienced team of insurance experts
- Special tax advantages
- Fair and efficient claims processing
- Surplus retained by subscribers

For these reasons, universities now want to join CURIE because of its numerous benefits and international reputation, not just its insurance protection.

Solid Governance Keeps CURIE on Track

A board of directors oversees CURIE's insurance professionals, ensuring that CURIE both treats subscribers fairly and evolves each year to meet subscribers' changing needs. The Board includes three university representatives apiece from Ontario, the West, and the Atlantic provinces, plus the executive director of the Canadian Association of University Business Officers.

The Board meets quarterly to review all large claims and identify trends in losses and exposures. Highly familiar with campus issues and university culture, the Board also develops practical risk management initiatives, from safe lab practices to responsible hazardous waste disposal and athletics coaching.

Looking Forward to the Next 20 Years

"Even though CURIE has operated for 20 years," says Keith Shakespeare, chief operating officer with CURIE, "I feel as if we're now just hitting our stride. We're going to keep improving our insurance solutions and better tailoring services for our subscribers. This philosophy has guided CURIE since its inception, and we understand its importance better today than ever before."

Two Decades of Growth

Here's a look at how CURIE has grown over the past 20 years:

	1988	2008
Number of subscribers	42	58
Property insurable values	$8 billion	$65 billion
Property coverage	$250 million	$1 billion
Liability coverage	$5 million	$30 million
Surplus	$0	$16.8 million (and $14 million has been returned to subscribers)
Number of CURIE staff	0 (all activities were outsourced initially)	6
Services	Insurance only	Insurance plus loss control and risk management consulting

Crisis Communication 101: Ensuring that key message gets out

By Lorne Honickman, McCague Peacock Borlack McInnis & Lloyd LLP.

Crisis communication is a strategic component of an organization's overall operational response to a crisis. The significance of the communication plan, in the over all crisis management model, is many times under estimated. During a crisis, effective messaging to shareholders, stakeholders and the public, can be determinative as to how an organization's reputation, ie. it's brand and image, will be maintained. In addition, any crisis represents the potential for findings of liability down the road. As such, it is crucial to ensure that the messages of today never become the evidence of tomorrow, which will be used against the organization at a trial in the future.

Effective communication is most important in the first few days that a crisis has hit. Let us take an example. An explosion occurs on a university campus. Fifteen students and teachers die and numerous others are injured. The first news reports suggest that a maintenance worker may have triggered a gas leak, which led to the explosion. At that particular time, there should only be one message from the university:

"Our main concern at this moment in time is for the families of the victims of this tragedy. We are doing everything we can now for those family members. A full investigation has begun in order for us to be able to find out how and why this occurred, and we are co-operating with all involved."

It is easy to see what would happen if the particular spokesperson responded to questions about an alleged error made by a maintenance worker by stating, *"it's obvious that this worker was doing something that he/she should not have been doing at that time. We are going to have to wait to see what the investigation shows."*

The university, by putting out that particular message, would be making a fatal mistake, ie. it would arguably be accepting blame and NOT just accepting responsibility. There is a very fine line which distinguishes the two but it is extremely crucial in the early stages of crisis communication, that no one cross that line. Taking responsibility is messaging to all what the company is doing at that particular point in time. Accepting blame, however, will of course, have enormous legal and public relations ramifications. Thus, determining the correct message is always the most important and most difficult aspect of crisis communication. Those messages should be developed in advance of any potential crisis or catastrophe. A proactive crisis management strategy will include a full communication plan. The organization should catalogue all the potential crisis it could be facing and develop specific and concise messages with respect to those particular situations.

Lorne will be leading an interactive workshop at this year's CURIE Risk Management Meeting… Further details in the next CURIE newsletter.

Once it is determined what the proper message is, it is imperative to ensure that particular message gets out. To begin with, the organization must be accessible. The words and perception of "no comment" should never appear to be attached to the company at any time. As part of the crisis communication plan, a spokesperson(s), will be in place and fully trained and ready to go. The first component is fully understanding the audience to whom the company will be messaging to, ie. shareholders, stakeholders, clients, employees, or the public through the media, and then utilizing some well established messaging techniques. For example, understanding how to bridge back to the essential message, is a technique that can be learned very quickly. It involves taking a question you are being asked and then bridging it back to the message you want to ensure gets out. Going back to our hypothetical news conference with the disaster at the university, when the spokesperson is asked a specific question about the allegations that a university employee caused the explosion, the only answer can be: *"right now everything is under investigation and we, of course, are co-operating with all levels of investigation, but as I stated, our prime concern right now is with respect to the families of the victims of this tragedy and that is where our focus is at this point in time."*

Continued on page 4

Questions & Answers

Question:
What are the benefits of FM Global's ***MyRisk***

Answer:
MyRisk Helps You Understand Your Risk

MyRisk is FM Global's private and secure Web site for clients and advisors working on their behalf. It provides up-to-date information about their global property risks and access to essential risk management information and decision-making tools, 24 hours a day, seven days a week.

With a flexible big-picture view of the overall risk quality of a client's location(s). ***MyRisk*** provides the details needed to set priorities and made the right risk management decisions. Its comprehensive, real-time information offers the following.

- Secure online access to your location-specific data
- Individually customized levels of access
- Ability to create reports based on location-specific data
- Faster, more efficient delivery of FM Global Risk Reports
- Global warnings of severe weather-related events
- Instantaneous access to a variety of property loss prevention resources
- Values assessment and reporting tools to ensure accurate valuation

For information or to register for MyRisk please contact John Breen, at jbreen@curie.org

Continued from page 3

The particular spokesperson responded to the reporter's questions, but in essence said "no comment", without of course, ever using those words and then bridged back to the important message, i.e. the concern for the families. Most importantly, the answer given in that hypothetical interview, will never come back to haunt the university in the event that there is litigation down the road. Most certainly, by "staying on message", the university is ensuring that it appears to betaking responsibility without ever admitting liability.

There is no doubt that this communication skill can be easily mastered by anyone, through a comprehensive message training session. Indeed, if one can learn to message to the public through the media, one will have what can be referred to at the black belt of messaging. As such, the most effective way of learning the technique is sitting in the "hot seat". A good message training session will put the potential spokesperson in a one and one interview, answering questions with respect to a mock crisis scenario. The spokesperson is under fire, if you will, for 3 – 5 minutes. The line of questioning produces a real world experience with an opportunity to make mistakes, and lessons on how to correct them. Most importantly, it allows the organization to begin to develop the important crisis communication messages as well as having the chosen spokesperson(s) ready, if and when the need arises.

One final note, while one of the messages of this particular article is the importance of "staying on message", one must never forget that if the technique is not done properly, it can lead to a different type of messaging disaster. Back in 2001, former Toronto Mayor, Mel Lastman, got himself into a difficult situation during Toronto's bid for the 2008 Olympics. The former mayor, made some questionable and disparaging remarks about Kenya and he met the media to publicly apologize. His message was clear at the beginning, (ie. "I'm sorry and I want to apologize for what I said".) However, when he was asked questions such as, "Are you a racist? Will you resign? How could this have happened? What do you plan to do now?" Mr. Lastman responded over and over again with only the words "I'm sorry for what I did, it was wrong". In other words, by "staying on message" and not even responding to a specific question, embarrassing results ensued. Every news story that followed in the paper and on TV, focused on the fact that the mayor said "I'm sorry" more than 20 times and not on the essence of the apology itself.

The message from all the above is that effective crisis communication is the equivalent to effective reputation management. Theorganizations that are successful at this, invariably are those that have been proactive, and have taken the time to plan for it accordingly.

Lorne Honickman, McCague Peacock Borlack McInnis & Lloyd LLP.
Combining his experience as a veteran television journalist and practising lawyer, Lorne provides crisis communication strategies and training sessions to organizations across Canada.

Developing Information Technology Recovery Plans

by Gayle Mitcham, Marsh Canada

In the last newsletter we reviewed the process for developing Business Continuity Plans using a project approach and 5 phases as shown here.

The development of Information Technology Recovery Plans can be done in tandem with the Business Continuity Plan project. Both plans can be developed using the same basic approach as they use the same basic information as their starting point. One additional consideration is that the recovery objectives for the business and the technology need to be linked together.

BUSINESS CONTINUITY PROJECT PHASES

Phase 1 – Preparedness Review

As in the Business Continuity Project, the first phase is planning and preparedness. This is a review of what you currently have in place from an IT recovery perspective and what the scope and objectives for the project will be including which departments and locations need to be involved.

Phase 2 – Business Impact Analysis - Linking Business Recovery Time Objectives to Technology Recovery Time Objectives

As outlined in the earlier newsletter, business recovery time objectives for each process are determined by the Business Impact Analysis. However, system recovery objectives are defined by the method and time required to recover the system. Business and system recovery times may be very different. Therefore it is important the business recovery time objectives (RTO) that are gathered in the BIA, be compared with the systems recovery time objectives (RTO), in order to identify any gaps.

As you know, a complex business process may utilize multiple computer systems and platforms, and each business process may have a different unacceptable period of downtime. The focus of the IT Recovery Plan must be on keeping the business running – not keeping the systems running. The key question then becomes – are recovery objectives in sync between the business process and the multiple systems and platforms that support the process.

This reinforces the idea that the business requirements need to be defined through the BIA before addressing computer requirements. It is the business owner who needs to determine what an acceptable risk for the business is and what systems RTO is appropriate. They also have to agree to the resulting cost of the systems implementation necessary to meet that recovery time.

Continued on page 6

Phase 1- Preparedness Review

- Establish Steering Committee
- Determine scope and objectives
- Define "criticality"
- Review existing documentation
- Conduct preparedness interviews
- Identify Planning Scenarios
- Develop Project Schedule and Plan

Phase 2- Business Impacts

- Customize BIA questionnaire
- Define Impact Criteria and Rating
- Conduct BIA workshops with Business Unit leaders
- Have BU Leaders complete questionnaire
- Review and challenge responses
- Identify critical services
- Review technology recovery capabilities
- Perform Gap Analysis

Phase 3 – Strategy Development

- Facilitate business strategy workshop
- Review technology and business recovery objectives
- Research solutions
- Perform cost benefit analysis
- Present recommended strategies

Phase 4 – Plan Development

- Develop Plan Template
- Pre-populate known data
- Develop recovery procedures and workaround workshops
- Business Unit Leaders to complete the plan
- Develop contact lists and call trees
- Walkthrough the plan with immediate stakeholders
- Obtain Plan sign off

Phase 5 – Exercise

- Develop a BC Plan Awareness Program
- Schedule and execute table top exercise
- Update plans with feedback from exercise
- Develop maintenance and testing schedule

Continued from page 5

In many cases defining RTO's will be an iterative process. It is basically a negotiation process between the business owner and the systems area to balance the risk with the cost. While there may be initial requirements for short RTO's, after weighing the cost of the solution, business owners may be willing to accept longer less costly solutions.

Phase 3 – Strategy Development - Evaluation of Disaster Recovery Solutions

Once the business RTO has been agreed upon, it is time to analyze the various recovery methods available and determine the most suitable recovery method for each application. This phase defines the resources required in recovering the application and the process that will be used to recover. In most cases there are more than one recovery alternatives that will meet the business RTO requirements. For example, in the case of data systems, the recovery strategy usually involves having the critical data systems replicated somewhere else and putting them online with the latest backed up data available. For less critical data systems, there may be an option to have spare server hardware located at an alternate location. When necessary these servers can than be configured with the required application.

Considering multiple options and various solutions makes it necessary to carefully evaluate the best suitable recovery solution for each application used by each department. The main factors that should be considered are:

- Cost of deployment, maintenance and operation
- Business recovery time requirements
- Ease of recovery activation and operation

Selected strategies for technology recovery are then presented to Executive Management for approval. A cost benefit analysis should accompany the strategy recommendations.

Phase 4 – Plan Development - Disaster Recovery Plan Development

Once the appropriate recovery solution has been identified and implemented you are ready to move on to developing the Disaster Recovery Plan.

The plan should include the following:

- Recovery Team(s)
- Notification Procedures
- process to alert recovery teams during business and non business hours
- notification to the IT damage assessment team
- general notification to IT staff
- IT Damage Assessment Process
- Process to evaluate the nature and degree of damage to the system
- Damage assessment should include; the origin of the emergency or disruption, potential for additional disruptions, status of physical infrastructure, inventory of equipment, type of damage to equipment, items to be replaced, estimated time to restore normal services
- Sequence of Recovery Activities
- Recovery Procedures - step by step task list of what needs to be done to recover the critical system
- System Linkages to other applications
- IT and Business Testing Required

Once the plan is completed it is important to ensure that a plan maintenance schedule is developed and implemented to ensure that it remains current and up to date.

Phase 5 – Exercise

Disaster Recovery Plans should be tested using a mock drill that actually executes the plan. This should be scheduled and carefully organized so that it does not impact production operations in any way. This usually requires that it be done outside of normal business hours. Recovery times should be closely tracked during these drills. This will allow you to ensure that you are meeting the business requirements. Plans are then updated to reflect the lessons learned from these exercises.

The best test of the plan is during an actual disaster. Lessons learned during this type of scenario are invaluable and need to be documented immediately following the recovery.

Plan tests or exercises should be held at least annually.

Completed Information Technology Recovery Plans

The completion of these project steps should ensure the development of an effective IT Recovery Plan for your organization. Going forward plan maintenance should include an annual review of RTO's from the BIA to ensure that gaps between business requirements and systems capabilities continue to be addressed.

...Watch for the next Newsletter where Crisis Management Response will be reviewed in detail.

Gayle Mitcham is an Assistant Vice President in the Business Continuity Practice for Marsh Consulting. If you have questions about this article or would like a quote from Marsh to provide assistance with your program, Gayle can be reached at 416-868-2748

CANADIAN UNIVERSITIES RECIPROCAL INSURANCE EXCHANGE

Balance Sheet

December 31, 2007 with comparative figures for 2006

	2007	2006
Assets		
Investments:		
Cash	$ 22,969,795	$ 27,490,208
Short-term investments	9,406	99,207
Bonds and debentures	46,408,767	34,742,336
	69,387,968	62,331,751
Investment income due and accrued	463,736	438,064
Due from subscribers	384,999	407,578
Recoverable from reinsurers on unpaid claims	2,414,000	2,383,000
Due from reinsurers on paid claims	1,127,361	2,643,659
Due from reinsurers on excess program	2,845,602	2,174,142
Prepaid expenses and other accounts receivable	141,274	117,915
Capital assets	48,700	37,500
	$ 76,813,640	$ 70,533,609
Liabilities and Subscribers' Equity		
Premiums received in advance	$ 11,991,197	$ 13,616,579
Unpaid claims and adjustment expenses	43,054,359	33,496,379
Payable to reinsurers on excess program	4,239,697	6,164,257
Accounts payable and accrued expenses	203,384	221,256
Premium taxes payable	500,145	527,647
	59,988,782	54,026,118
Subscribers' equity:		
Accumulated excess of income over expenses	16,571,816	16,507,491
Accumulated other comprehensive income	253,042	–
	16,824,858	16,507,491
	$ 76,813,640	$ 70,533,609

CURIE Risk Management Newsletter

CURIE Protecting Our Universities

Published and distributed by Canadian Universities Reciprocal Insurance Exchange (CURIE)

5500 North Service Road, 9th Floor, Burlington, Ontario
L7L 6W6
Telephone: (905) 336-3366
Fax: (905) 336-3373
Editor: Keith Shakespeare

www.curie.org

CAUB0 65th Annual Conference

Making Connections

University of Manitoba, Winnipeg
June 14 to 17, 2008

Please note that most CAUBO 2008 activities will take place at the Winnipeg Convention Centre

CURIE University & College Risk Management Conference

Toronto Marriott Downtown Eaton Centre Hotel
September 20 & 21, 2008

Watch for further details on our website and the next issue of the CURIE newsletter.

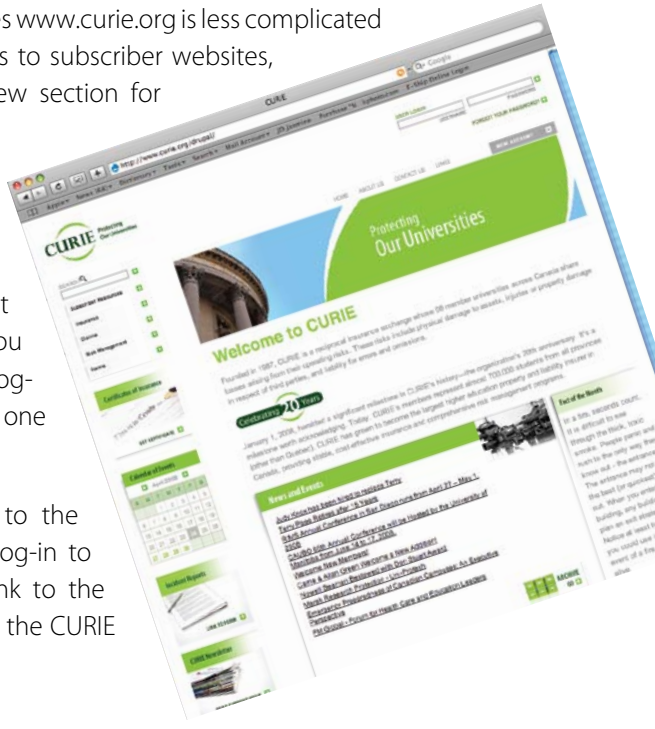
CURIE Launches New Web Site!

A new look and improved functionality.

On April 7th 2008, CURIE launched an updated and improved website – www.curie.org While maintaining much of the original information that members use on a regular basis, the site contains several new features.

"Our aim is to provide visitors with easy access to the latest information and to become the 'go to' source for up-to-date and current CURIE initiatives", says Keith Shakespeare, chief operating officer with CURIE. "We encourage members to return to the site often and see what's new. We're always looking for feedback and aim to be responsive to the on-line requirements and preferences of our members."

The website is designed to be easy to navigate and make work easier for subscribers and visitors. In addition to new features www.curie.org is less complicated to update. The website features links to subscriber websites, on-line incident reporting and a new section for Board Members.



To access these services a new *Username* and *Password* is required. Please contact either John Breen at jbreen@curie.org or Judy Knox at jknox@curie.org. They will register you on the new site, and after your initial log-on you can change the password to one of your choice.

Please note there will no change to the *Username* and *Passwords* used to log-in to the *CURIE Certificate Program*. A link to the Certificate Program can be found on the CURIE website home page.