AUGUST 2013 | VOLUME 23 | ISSUE 5

Risk Management *newsletter*

IN THIS ISSUE...

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 likely, however, that the CURIE staff, through dealing with the other 61 CURIE subscribers, have encountered issues like yours. If not, we're highly experienced in finding answers though 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.

Cyber Attack: It's Only a Matter of Time

BY JOE OZORIO, CBCP, CBCA, MBCI

"There are only two types of companies: those that have been hacked and those that will be" ~ FBI Director Robert Mueller, March 1, 2012

A neighbour of mine, a small business owner, was telling me about an incident he experienced recently. His only computer server, used for e-commerce and data storage, was hacked. The cyber criminal not only denied him access to his server, but also encrypted his files and demanded US$5,000 to release the server and provide him with the encryption key. My neighbour was adamant that he was not going to be "held for ransom"; especially after I told him it was likely he would have to continue paying the cyber criminal one file at a time. He was a victim of what in the cyber security world is known as "Encryption Ransomware". What did he do? More on that later.

Does this sound familiar? How about this? How many times have you seen an e-mail from a friend's Yahoo or Hotmail email address containing a strange sounding message asking you to click on an embedded link? Perhaps you've recognized this as suspicious and deleted the email (and been nice enough to tell your friend about it), but perhaps out of curiosity you've clicked on the link, and before you know it you've loaded malware onto your own computer, and your own email account is now hacked.

These are simple examples of a growing multi-billion dollar "industry".

CYBER CRIME ON THE RISE

It is impossible for most of us to imagine a world without computers, the Internet or smart phones. Technology continues to advance rapidly; creating endless new possibilities, but along with them a whole new world of risks. In the wake of a number of highly visible data breaches, litigation, and hacking attacks, awareness of cyber and privacy risks and costs continue to grow. Information Technology security experts believe it is now impossible to prevent violations of online data confidentiality. In 2008, the total value of intellectual property stolen from businesses around the world was estimated at one

trillion dollars. Today, it is almost impossible to calculate this amount due to the pervasiveness of cyber crime and the reluctance of organizations to report such breaches. In the past, political and terrorist activities were the primary drivers of cyber attacks; today the primary motivator for cyber crime is economic gain.

Perhaps even more daunting is the fact that unplanned IT outages/cyber attacks are the second most prevalent cause of supply chain disruptions, accounting for almost half (49%) according to the Business Continuity Institute.

I'm not a cyber security expert, but in my line of business – Business Continuity Management – I'm seeing more and more evidence of negative business impacts that in turn influence how organizations plan and prepare for business disruptions. The bottom line is that the impact cyber threats will eventually affect the majority of individuals and businesses. Hacktivists and cyber criminals are creative, determined, and often well funded and techno-savvy (but even that is not necessary today). It's only a matter of time before you, someone you know, or your institution fall victim to this growing condition of today's society.

YOUR ORGANIZATION COULD BE EXPOSED TO CYBER ATTACKS IF IT:

- Collects credit card data or processes online payments (e.g. student tuition or other fees payment)
- Stores data
- Houses research data on servers, laptops., tablets, etc.
- Publishes content
- Provides online content or media
- Uses cloud computing and outsourced computing
- Develops software for itself or others
- Performs system integration or software maintenance services
- Broadcasts or distributes content (whether or not you charge for it)

THE IMPACTS

Regardless of the nature or our vulnerability to cyber attacks, we need to first understand the impacts they can have. Here are just a few examples:

Third Party:

- Legal liability to others for computer/network security breaches
- Legal liability to others for privacy breaches

First Party:

- Regulatory actions and scrutiny for discovered breaches
  - Personal Information Protection and Electronic Documents Act (Federal)
  - Personal Information Protection Act (BC)
  - Personal Information Protection Act (Alberta)
  - An Act Respecting the Protection of Personal Information in the Private Sector (Quebec)
- Loss or damage to data/information/intellectual property
- Loss of revenue due to a computer/smart device attack (e.g. denial of service to student registration and payment services)
- Extra expense to recover from or respond to a computer/smart device attack
- Loss or damage to reputation could result in reduced enrolment, as confidence in the security of your college or university environment dwindles
- Loss or damage to reputation

A cyber attack is not a typical emergency situation. It is not a research experiment gone wrong or a fire, or a flood, or an act of violence on campus, but its impacts can be just as great, if not greater.

Am I being paranoid? You bet! I think a little paranoia is healthy when it comes to understanding and being prepared for the impacts of a cyber attack. It may take days, weeks, months, or even possibly years for an attack to be discovered, during which time the impacts could spread insidiously. The time gap between compromise and detection can be quite long. At that point prevention is moot, but preparedness is paramount.

REPORTING BREACHES

The current regulations for reporting privacy breaches are not nearly as stringent in Canada as they are in the US. However, Bill C-12 puts forth proposed amendments to the Personal Information Protection and Electronic Documents Act (PIPEDA) that would require organizations to report to the Federal Privacy Commissioner any material breach of security safeguards involving personal information (think student records and credit card information) under its control. Bill C-12 is widely expected to pass this year.

BEING PREPARED

So what does all this mean? It doesn't mean giving in to the inevitable; don't make it easy for the cyber criminals to attack. It's all about being better prepared and in order to do that you need to understand a few basic principles:

1. Cyber criminals and hacktivists have some pretty sophisticated tools at their disposal. The average person can become a hacker by simply downloading and executing user-friendly, menu-driven software. Hacking is no longer the domain of the cyber geek.

2. Cyber criminals tend to follow the path of least resistance. As IT systems and infrastructures become more secure, they adapt. For instance, as Operating Systems from the major suppliers (Mac/OS, Windows) get better at breach prevention, the attention turns to the applications (e.g. Office Suite), and as these get better at breach prevention, the attention turns to the documents. Finally, documents become more secure; their focus shifts to what can be a very easy entry point: people. If a cyber criminal really wants to get into a system that is well protected, he or she could simply target an individual within that organization and engage in a little social engineering to get in a back door. For example, a cyber criminal may target a person within an organization and start to mine information about that individual available on Facebook or LinkedIn – it's amazing what type of personal information people post! Using that information the criminal could send the individual a compelling e-mail with information specific to them in a manner guaranteed to gain their interest. The victim thinks it's a legitimate message and clicks on the embedded link, or goes to the website advertised. In doing so, they create an opportunity for the cyber criminal to use a back door into the organization's system – bypassing the highly secure front door altogether.

3. Law enforcement's ability to assist is limited. Most law enforcement agencies do not have enough trained resources to deal with cyber investigations. Their focus is on monitoring, investigating and dealing with societal blights, like child pornography, or terrorist cyber attacks on public infrastructure systems (i.e., electrical grids, defense systems, etc.), or major banking institutions.

4. Some cyber crime is sponsored by organized crime or even governments. These are determined, well paid or funded individuals stealing anything that can create an advantage for them, or make them lots of money.

5. Understand that breaches are not only coming from external sources but could also come from within your organization, or could be the result of negligence, carelessness, ignorance, or the grand-daddy of them all: human error.

PREVENTATIVE MEASURES PLUS RESPONSE PLANNING REQUIRED

Preparedness begins at the top level of the organization. You need to ensure you have the attention, awareness and support of your executive management and board of directors (in a recent Oliver Wyman IT Governance Study with the National Association of Corporate Directors, 51% felt that the board was not provided with adequate information to provide IT risk oversight.).

Next, you need to look at cyber risks holistically:

1. Identify the true nature (sources, likelihood, impact) of the risk for your organization:
   a) Include representatives from legal, communications, corporate social responsibility, issues management, strategic planning, HR, and others.
   b) Understand that it's not simply an IT issue, and a disaster recovery or continuity plan is not enough. It's a very important component, but it's reactionary, not preventative.

2. Assess your institution's existing capabilities:
   a) Consider the broader impacts, consequences, and reputational risks.
   b) Look beyond knowing you can address technical aspects, i.e. getting your servers back up and running. Consider the reputational damage for example.

3. Develop or assess your current crisis management processes:
   a) Ensure that a well-aligned and integrated approach is possible with all aspects of your preparedness program.
   b) Align and integrate how IT, operations, communications, legal and senior management will all function together.
   c) Establish a sound management capability to address potential crisis events.
      i) Put mechanisms in place to guide escalation and expansion of the response management process.
      ii) Understand that perception is reality: who is at fault, how big or small the problem really is, and how vulnerable you and your students/faculty/staff/key suppliers/others are, may not be based on actual facts. Good crisis communications planning is the key to dealing with this disconnect.

In preparing for cyber attacks and potential breach, consider the following:

1. Trying to keep breaches or attacks quiet or worse trying to hide them has become more and more difficult, and in most cases is not advisable:
   a) Be prepared to manage these situations.
   b) Guard against those in the organization that would prefer to ignore the advice of the experts.
2. Regulators will respond far more negatively if you try to "hide" or minimize a problem, rather than quickly and overtly managing it.
3. Many notification and monitoring requirements associated with breaches vary by local authority and by country, and these regulations continue to change and emerge (e.g. Bill C-12). You require a clear plan for your local jurisdiction. Some organizations pre-identify an outside firm to assist with these requirements.
4. You need to go beyond simply identifying and understanding cyber risk to knowing what the plans are to manage cyber events if they do occur.

Think it through logically and take a step-by-step approach. Below is an example of Marsh's approach to cyber risk and privacy preparedness:

- Assessment – understand the threat and impact.
- Remediation – understand you current capability to prevent, respond and recover – and improve that capability where weaknesses exist.
- Prevention – make sure you have good protective technologies (i.e. ensure you are using the latest operating systems). Understand however, that relying on technology as some mythical "silver bullet" that will defend against all risks is to turn a blind eye to major risks facing every public or private entity.
- Education – inform your students, faculty and staff of the dangers, how they can inadvertently create exposures for your institution, and the potential impacts of their actions.
- Consider cyber insurance coverage, but be aware that placement of coverage is the last step in the process. Insurance is never a valid alternative to good risk management and preparedness. Understand what cyber insurance covers and what it doesn't:

This is a lot of information to consider, but the bottom line is that the growth in the frequency and number of cyber attacks should be prompting you to consider all of the issues I've outlined. However, you need to do your own research as well. It's never too late to get started.

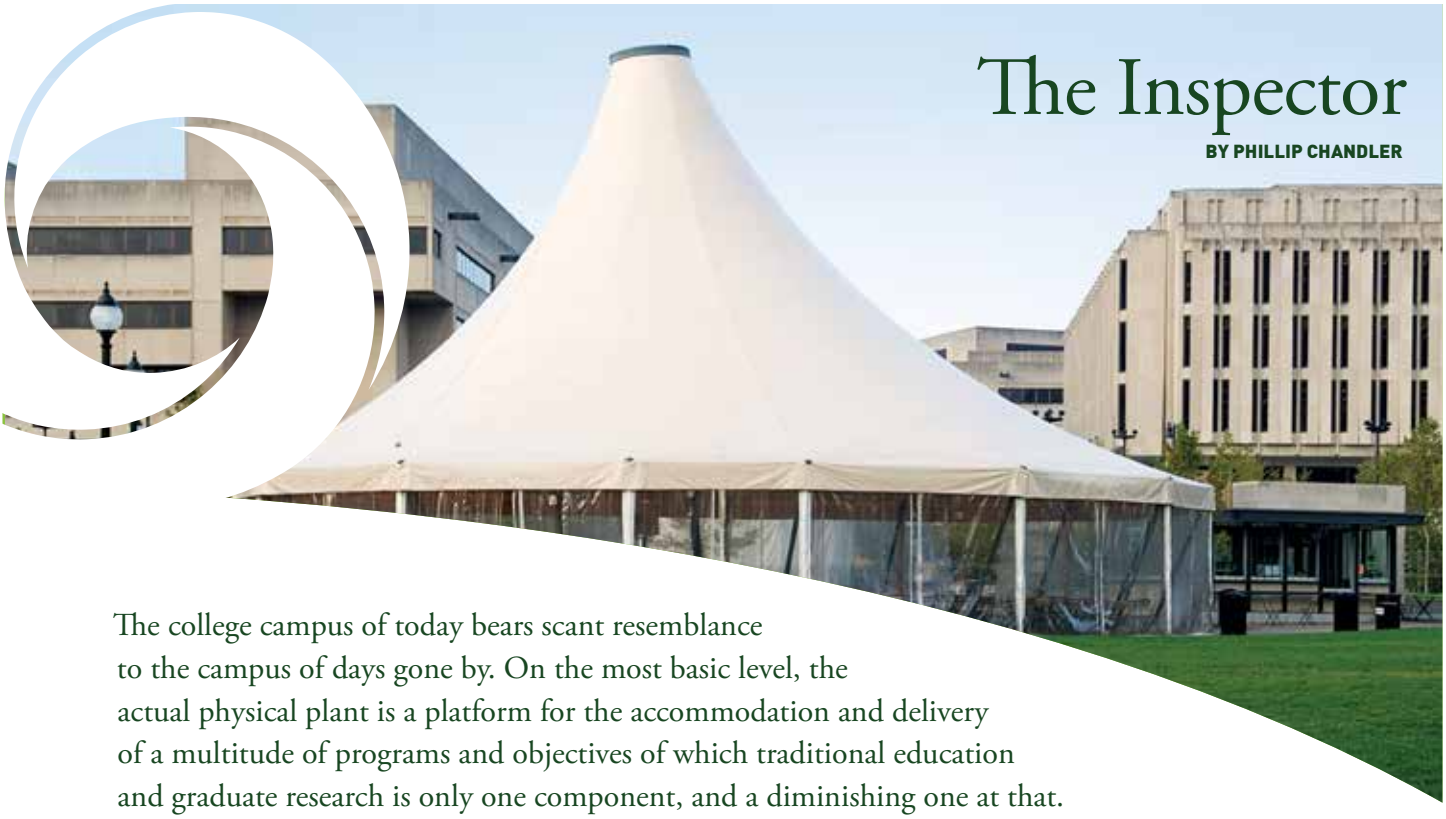
Oh, and my neighbour … he refused to be held for ransom. Most of his data was not that critical, nor did it contain information about his customers. His service provider was able to help him get past the denial of service. In the end, it cost him a bit more that the $5,000 ransom demand, but there was no guarantee that he would have gotten full access back if he paid the ransom. In the end, my neighbour was lucky.

But you can't count on luck. Being prepared (and a bit paranoid) is a safer bet.

JOE OZORIO is an Assistant Vice President and Senior Consultant within the BCM consulting practice in Marsh Risk Consulting.
With thanks to Gregory L. Eskins, Senior Vice President, Marsh Canada Limited for providing some content to this article.

Privacy & Cyber Perils	Property	General Liability	Traditional Fidelity Bond	Computer Crime	E&O (not purchased)	Special Risk	Board Privacy & Cyber Policy
Destruction, corruption or theft of your electronic information asset/data due to failure of computer or network	■			■		■	Information asset protection
Theft of your computer systems resources	■			■			Information asset protection
Business Interruption due to a material interruption in an element of your computer system due to failure of computer or network security (including extra expense and forensic expenses)	■					■	Network Business Interruption
Business interruption due to your service provider suffering an outage as a result of a failure of its computer or network security	■						Network Business Interruption (sub-limitted or expanded based upon risk profile)
Indemnification of your notification costs, including credit monitoring services							Privacy Liability (sub- Limited)
Defense of regulatory action due to a breach of privacy regulation							Privacy Liability (sub- Limited)
Defense of regulatory action due to a breach of privacy regulation							Privacy Liability
Threats or extortion relating to release of confidential information or breach of computer security							Cyber Extorsion
Liability resulting from disclosure of electronic information & electronic information assets					■		Network Operations Security
Liability from disclosure confidential commercial &/ or personal information (i.e. breach of privacy)					■		Privacy Liability
Liability for economic harmed suffered by others from a failure of your computer or network security (including written policies & procedures designed to prevent such occurrences)					■		Network Operations Security

Not Covered | Covered | See notes | Dependant upon specifications of claims, may not be covered



The Inspector

BY PHILLIP CHANDLER

The college campus of today bears scant resemblance to the campus of days gone by. On the most basic level, the actual physical plant is a platform for the accommodation and delivery of a multitude of programs and objectives of which traditional education and graduate research is only one component, and a diminishing one at that.

The campus increasingly supports the partnership of academia and private enterprise, hosting for-profit research and development activities. Likewise it frequently becomes an entertainment venue, hosting many diverse public performances of mass-appeal, including traditional team sporting events. In support of all of the above, the campus also becomes a gigantic lodging facility, housing athletes, campers, trade emissaries and senior adult learners. Talk about an identity crisis! Today's college or university is a veritable Disney Land.

It should therefor come as no surprise that the fire safety professional on the campus is challenged as never before. Protecting students and faculty, never an easy task, pales in comparison to the challenges posed by the multi-various activities we now find (some schools already have aviation facilities on campus). These days, there really isn't a chapter of any of our model codes that doesn't have some direct bearing on college operations. Consequently, the fire official, the environmental health and safety professional, regardless of the hat he or she wears, needs to be fully conversant in all area of fire protection.

Of course education is indispensable in assuring that we are all up to the fire safety challenges of the modern campus, but there is more. We all must recognize that the need for fire inspection and code enforcement activities far exceeds the limited scope of practice established for us in a different era. Classically, the campus fire gal or guy's job was to protect vulnerable young adults asleep in their dorm rooms. Following this model inures us from dealing with the multitude of true fire hazards on the campus. Expressions such as "that's not our job," while providing a convenient dodge, is disheartening to hear from any professional, let alone from one that by virtue of training, experience and personal conviction, is committed to the preservation of life, limb and property.

One sure telltale sign of a changing campus, of a campus infrastructure pushed to the max in accommodating every purpose under the sun, is the proliferation of tents and membrane structures. Some of us are experienced with the use of air-inflated structures to economically house burgeoning sports programs. Here we usually have enough early notification to adequately prepare others and ourselves for this new fire safety challenge. But there are also those tents that seem to materialize suddenly out of thin air. Campus entities not regularly on our limited horizon suddenly think it a grand idea to invite a circus to town, right in our own back yard. Or maybe the office of institutional advancement has decided to host a mini-Woodstock extravaganza for graying alumni, replete with field dining and kitchen tents that would have made General George Patton proud.

At the expense of stating what might be obvious to most readers, tents represent a huge public safety risk. They are made of combustible materials. They contain combustible materials. They host large crowds and they feature events involving open flames. They are susceptible to sudden structural failure. Sadly, we are reminded of the Hartford circus fire of July 6, 1944, in which 163 people, most of them children, perished in a fast moving fire. While we have learned from that tragedy and as a result, tent materials are safer now, we are in no way immune from a future catastrophe.

While it is true that the Hartford tent canvas had been treated with paraffin cut with gasoline – may that never be the case again; many of the factors contributing to the loss of life are just as likely to be present today. The tent was located without regard for firefighting water supply. There was no fire evacuation plan – the bandleader struck up "Stars and Stripes Forever," a universal alarm of danger in the circus world – but this alert was not recognized as such by the audience. There were numerous blocked exits, some impaired by the support cables. And perhaps most significantly from our perspective, the Hartford fire marshal had chosen not to inspect the tent before the performance. Had he done so, the outcome may have been entirely different.

For the campus fire safety specialist, there are a number of basic recommendations for assuring the safety of tents.

1. Familiarize yourself with the **code** in effect in your jurisdiction. For some that may be Chapter 24 of the International Fire Code. As the saying goes: "Ignorance of the law is no excuse."

2. If required by law, obtain necessary **permits** from outside authorities having jurisdiction. Hopefully, this will trigger an inspection; an extra set of eyes is always welcome.

3. Determine the **combustibility** of tent materials along with decorative hanging decorations, bunting and sawdust used on the floor. Demand documentation that the above materials meet the flame propagation requirements of NFPA 701.

4. Assure safe **location** of tents, providing appropriate separation between other tents and buildings. Also situate tents so as to provide Rapid emergency responder access and when possible, close to hydrants.

5. Require appropriate **egress** capacity and signage and emergency lighting as needed. Many tents qualify as places of assembly; insist on an evacuation plan including a pre-event announcement.

6. **Control** cooking. It needs to be done in tents dedicated for this purpose, separated from other tents by 6.1 m (20 ft.). Cooking equipment needs to be inspected safety and compliance with manufacturer's specifications. It needs to be kept 3.5 m (10 ft.) away from exits and combustible materials. Cooking equipment, along with all tent contents, need to be kept .91 m (3 ft.) away from the fabric envelope.

7. **Portable fire extinguishers** are essential. They must be inspected and appropriate for the hazard present. Type K is required for many cooking operations. Event staff needs to be familiar with their use.

8. **Propane** cylinders used for cooking and heating need to be secured against tipping. They need to be kept outside of the tent and at least 3.04 meters (10 ft.) away from the outer membrane.

9. **Fireworks** shall not be used with 30.5 m (100 ft.) of a tent. Additional requirements apply to pyrotechnic displays before a proximate audience and greater separation may be required for fireworks based on type and size.

10. Exhibit **common sense**. Most tent events are temporary. The code official is given some latitude, especially in regards to venting requirements of cooking appliances and proximity to patrons. A competent fire watch may alleviate many concerns.

By no means have we touched on all issues of tent fire safety, just the basics. Hit the books! Keep your eyes open! And know this: if we don't ask the tough questions on the campus, who will?

PHILLIP CHANDLER is a long time fire-fighter and a fulltime government fire marshal working extensively in the college environment – from large public university centers to small private colleges. His primary responsibilities include code enforcement and education.

CURIE Member Up Close: Nowell Seaman

Manager of Risk Management and Insurance Services at the University of Saskatchewan

Nowell Seaman has dedicated over 30 years of his career towards understanding the process of risk management, 18 of which have been dedicated to improving the approach, and establishing collaborative initiatives at the University of Saskatchewan. Having been involved in the arts in the early stages of his profession, Nowell never planned on a career in risk management. His interest in the arts led him into the theatre and popular music, including time as a professional guitar player in Nashville, but his curiosity about the business world soon steered him in a different direction.

Nowell worked as partner and director in a company that was involved in insurance brokerage, real estate and property management. Over the course of 12 years in that role, Nowell realized he was less interested in sales and marketing and more inclined towards the professional services side - risk management consulting for his commercial clients. After achieving his Chartered Insurance Professional (CIP) and Canadian Risk Management (CRM) designations and selling his shares in the brokerage business, Nowell moved on to become involved in a project funded by the Canadian International Development Agency in Moscow, Russia, where he and a small team of colleagues conducted risk management seminars for emerging businesses.

In 1995, Nowell joined the University of Saskatchewan where he became the school's first and only full-time risk management officer. Over time, Nowell developed the scope of Risk Management and Insurance Services, and in 2003, the University of Saskatchewan implemented a formal Enterprise Risk Management (ERM) program. Nowell displays a strong sense of pride in the program's success and an appreciation for his working environment, describing the university setting as "incredibly diverse, fast-paced, challenging and provides a lot of variety," all of which Nowell states, "keeps things interesting."

Nowell points out that his office doesn't manage all risk. He relies on many departments (e.g., health and safety, communications, security, facilities, IT, international and many others) to run their own risk management initiatives, while he and his staff act as coaches and facilitators for the process.

> "We ensure that they know how to approach risk, [and in doing so] we build capacity, reduce reliance, and help others develop risk management capability within their own areas of expertise."

The University of Saskatchewan has been a member of CURIE since 1998. "CURIE is more than an insurance company," claims Nowell, "We have the advantage of a strong network for sharing ideas and solutions." In support of this comment, Nowell offers the example of CURIE's SportRisk Program to show how members

Nowell in front of the CLS (Canadian Light Source) national synchrotron research facility at The University of Saskatchewan.

can benefit from highly experienced consulting services and best practices at peer universities. The University of Saskatchewan incorporated CURIE's SportRisk program into the operations in its College of Kinesiology, which in turn served as a tool for engaging and producing a great risk management team within the college.

In terms of what makes risk management at the University of Saskatchewan unique, Nowell cites the establishment of research facilities such as the Canadian Light Source national synchrotron. In 1998, Canada had no synchrotron facility; however, after a campaign by the Canadian scientific community to establish a synchrotron radiation facility in Canada and over a five-year construction period, the Canadian Light Source Synchrotron opened in 2004 on the University of Saskatchewan campus. The design and delivery of this leading edge project served as a great learning opportunity, stretching Nowell's limits in a new and rewarding way, as this project was one of the largest research facilities built in Canada during this century.

Nowell takes pride in the outstanding leadership at the university, as showcased by the school's Board of Governors and senior executives, who express a keen interest in managing key risks and ensuring that needs are met. "Every senior executive at the University of Saskatchewan can speak to risk management," says Nowell, elaborating that he advises them on progress or on developing risks with a quarterly report on key risks and a semi-annual report to the Board of Governors. Nowell emphasizes the importance of leadership when he says, "We understand that, in order to be successful, you have to take risks, but you need to manage them well."

Along with all the successes of his program, Nowell points out that the field of risk management comes with ongoing challenges as well. There has been an increased reliance on IT infrastructure in more recent years, as well as serious challenges in external landscape. Nowell brings up the current situation with unprecedented flooding in Alberta, pointing out that, in general, we are seeing an increase in severe storms, a situation that challenges the physical protection of universities. He points to the related issue of funding, commenting that

"it is a struggle to ensure we're covering all facets of risk management at a time when university funding is shrinking."

In addition, a specific challenge for CURIE lies in maintaining continuous exposure to different risks for every member across Canada.

In discussing the challenges for the future of risk management, Nowell emphasizes the importance of continuing to use an integrated approach. He consistently stresses the importance of communication, engagement and leadership within the risk management picture, highlighting his passion for his work and his drive to succeed on behalf of the University of Saskatchewan community.

Statement of Income & Expenses

For the second quarter ended June 30, 2013

	2013	2012
Written Premium	23,511,935	24,385,399
Earned Premium	11,755,967	12,168,598
Less Reinsurance Costs	598,283	611,379
Net Earned Premium	11,157,684	11,557,219
Net Incurred Claims	6,053,139	6,216,567
Net Loss Ratio	54.25%	53.79%
UNDERWRITING PROFIT (LOSS) BEFORE OPERATING EXPENSES	**5,104,545**	**5,340,652**
Operating Expenses	1,774,391	1,745,786
Net Operating Expense Ratio	15.90%	15.11%
Combined Ratio	70.15%	68.90%
UNDERWRITING PROFIT (LOSS)	**3,330,154**	**3,594,866**
Income from Investment	535,768	555,897
Other Income + Realized Gain (Loss) on Investments	293,239	(112,523)
* Other Comprehensive Income (Loss)	997,509	1,521,656
NET PROFIT (LOSS)	**5,156,670**	**5,559,896**
SUBSCRIBERS EQUITY (SURPLUS)	**61,054,495**	**50,486,585**

* Other Comprehensive Income (Loss) represents unrealized gains (losses) on available-for-sale securities.

Upcoming Events

SATURDAY – SUNDAY, OCTOBER 5-6, 2013

CURIE University & College Risk Management Meeting
The Hotel Grand Pacific, Victoria, B.C.

AGENDA

SATURDAY

CURIE Board Update

Recent Developments in Contractual Exclusion of Liability

Panel Social Media

CURIE Round Table (closed meeting, members only, bring your questions and/or issues to discuss with your peers)

Working with CURIE on Reputational Risk

Tsunami at University of Lethbridge

Data Security & Legal Update

SUNDAY

Claims Update

Certificate Management

Movie & Q & A

SUNDAY – WEDNESDAY, OCTOBER 6-9, 2013

The 2013 RIMS Canada Conference
The Victoria Conference Centre, Victoria B.C.

CURIE Protecting Universities. Sharing Knowledge.

Canadian Universities Reciprocal Insurance Exchange

Published & distributed by CURIE
5500 North Service Road, Suite 901
Burlington Ontario L7L 6W6

Telephone: 905-336-3366
Fax: 905-336-3373
Editor: Keith Shakespeare

www.curie.org