http://ontario.rims.org

PULSE

orims
ONTARIO RISK AND INSURANCE MANAGEMENT SOCIETY

THE HEARTBEAT OF RISK MANAGEMENT, APRIL 2016

# President's Message

By:**Tina Gardiner,** ORIMS President - Regional Municipality of York

Recently I was using Google to look for an easy and delicious dessert recipe to take to a potluck dinner with friends. A recipe is defined as a set of instructions for preparing a particular dish, including a list of the ingredients required or something that is likely to lead to a particular outcome or means/way of achieving, a prescription, formula, or blueprint.

People often coin the phrase "recipe for success" and this had me thinking about ORIMS membership. (Dah Dah! ….. there you have my "degrees of separation" thought process!)

What is the "recipe for success" for ORIMS….for growing and retaining membership and providing good service to our members? Currently ORIMS is the seventh largest chapter of RIMS and we have over 315 RIMS members. Membership has declined slightly in the past five years.

As a Board we are conscious of our duty to provide good value for all members. And we have several categories of membership to consider. Are there different needs for each? What are the common needs? How can we improve our services?

The second piece of the membership pie (see how I came back to food….?) is how do we increase our membership base. I have been a member for over 25 years and have found this organization to be one of the best networking and training sources I have ever experienced. How do we get that message out there to newer folks to the industry? And how do we keep experienced people engaged?

We would love your feedback ….drop a quick email to any Board member to tell us what you need, suggest ideas, tell us the good, the bad and the ugly. You can reach me at tina.gardiner @york.ca

This is your organization so we want your ideas…..so we can formulate or fine tune an ORIMS recipe for success!

In this edition of the Pulse you will find articles about what is happening across Canada in terms of the RIMS Canada Council (RCC), recaps of a few chapter events that have recently occurred (thanks to our curlers!) and information about the emerging risk of Cyber Liability and how to have a successful global risk management program. We provided you with a few "save the dates" for upcoming events. We hope to see you there! Remember this is your organization and you get back what you put in. No matter what services the Board provides we need you to be successful. You are definitely an important ingredient in our recipe! (and there it is again!) We hope you enjoy this edition of the PULSE and as a special treat for our members, you will be receiving a PDF copy of the book "Navigating The Cybersecurity Storm" generously donated by the author Paul Ferrillo. Happy reading!

In case you were wondering I ended up making a double chocolate, SKOR and fruit trifle for the potluck. It was pretty to look at as a whole, messy to serve requiring multiple serving utensils and absolutely delicious by all accounts. …a bit like ORIMS!

INSIDE THIS ISSUE

1 President's Message – Recipe for Success

2 CYBERSECURITY AND PRIVACY – Diligence in a Post-Breach World

4 Spencer Educational Foundation
Six Dimensions of a Global Risk Management Program

6 Upcoming Industry Events – Captives & CI Strategies Summit – Training Workshops

7 Rims Canada Council Winter Planning Meeting

8 Professional Development Webinar – Professional Development Day and Spring Fling

9 Chapter Events – 2016 ORIMS Curling Bonspiel

# Cybersecurity and Privacy Diligence in a Post-Breach World

By:Paul Ferrillo, Weil, Gotshal & Manges LLP,

"By the time you hear thunder, it's too late to build the ark."

— Unknown

In November 2014—just two weeks after Admiral Michael Rogers, director of the National Security Agency, testified to the House Intelligence Committee that certain nation-state actors had the capability of "infiltrating the networks of industrial- control systems, the electronic brains behind infrastructure like the electrical grid, nuclear power plants, air traffic control and subway systems"—Sony Pictures announced it had experienced a major cyber-attack, one many sources believe was likely perpetrated by or on behalf of a nation-state. This destructive cyber-attack was a game-changer for corporate America because it became clear that hackers are not simply focused on credit card numbers or personal information. Indeed, the attack on Sony was designed to steal the Company's intellectual property, disseminate personal emails of high-ranking executives, and destroy Sony servers and hard drives, rendering them useless.

What the events of 2014 proved to corporate America is that there are no foolproof methods for detecting and preventing a devastating cyber-attack. As FBI Director James Comey eloquently put it, "There are two kinds of big companies in the United States. There are those who've been hacked…and those who don't know they've been hacked."

Thus, it is absolutely critical to understand what kind of data a company collects, how the company uses, stores, shares, processes, protects, and disposes of information, and how to develop and evaluate a plan to respond to attacks that target these data. Proper planning can mean the difference between a news story that begins, "Sony has just announced that Sony Pictures Entertainment co-chairman Amy Pascal is stepping down from her post," and one that announces a major cyber-attack, but concludes, "Anthem said it doesn't expect the incident to affect its 2015 financial outlook, 'primarily as a result of normal contingency planning and preparation.'"

Proper planning includes incident response and information management business continuity planning, which are mission- critical. They are (or should be) part of a Board's enterprise risk management duties, and they are particularly vital for certain federally-regulated entities with an obligation to protect consumer and client information and to keep it private. We have written in-depth elsewhere about incident response plans and their elements. Here, we set forth a high-level summary designed to help evaluate a company's incident response and business continuity plans.

## Incident Response Planning—You Can't Defend What You Can't See

Given that 97 percent of the IT systems of companies surveyed globally have been breached, the question of how to protect a network from a breach is effectively a moot point. The better question is, how do you respond in the event of a breach when it occurs despite your best prevention efforts?

Incident response planning is exactly what it sounds like—a plan to detect and respond to indicators or actual evidence found on a network server or alert system that a malicious intrusion may be occurring.

In general, there are many indicators or precursors of a potential cyber-attack. Though there are far too many to list, potential triggers for a robust incident detection and response plan include:

- A network intrusion detection sensor alerts when a buffer overflow attempt occurs against a database server. Antivirus software alerts when it detects that a host is infected with malware.
- A system administrator sees a filename with unusual characters.
- An application logs multiple failed login attempts from an unfamiliar remote system.
- An email administrator sees a large number of bounced emails with suspicious content.
- A network administrator notices an unusual deviation from typical network traffic flows.

This non-inclusive list, based on the National Institute of Standards and Technology Computer Security Incident Handling Guide, illustrates one of the most basic challenges of working with advanced incident intrusion detection systems: they often generate thousands, if not tens of thousands of alerts of potential intrusions into a company's computer network every day. In fact, one

recent report notes that potentially actionable (i.e., "we better take a look at this") malware intrusions could number in the thousands per day.

Even in the largest companies, resources are not unlimited, particularly given the shortage of skilled IT professionals in the marketplace today, so each company's incident response plan will necessarily reflect certain compromises. However, recent events offer some basic principles as to how companies can and should lay out their incident detection and response plans from a "process perspective":

- Incident responders need to understand the "normal" behavior of their network. Logs kept by intrusion detections systems provide detailed reports from firewalls, intrusion detection devices, and network traffic flow activity meters.
- Incident response handlers need to fully understand what is "normal" behavior on any given day and time, so that they then can determine what is "not normal" based upon any one particular alert. Visibility is one of the key issues to emphasize because no security system in the world will mean much if you can't tell the difference between alerts to which you should respond and alerts to which you must respond. Often, breaches happen because critical alerts are overlooked amid the noise of numerous other alerts of lesser importance.
- Firewall, intrusion detection, and network activity logs need to be maintained and accessible, so efforts can be made to correlate potentially malicious current activity with network activity in the past. It may be necessary to keep these logs handy for months, since many attacks take that long to be "noticed" by an unsuspecting company.
- Cyber events need to be correlated quickly. Many times, this function can either be outsourced to a third party vendor, or it can be performed mechanically with an appropriate hardware solution that can analyze all of the alerts in real time.
- After reviewing evidence supplied by each of the above steps, incident response teams need objective criteria to determine which intrusions need to be escalated to a higher level and/or investigated further.
- Finally, when a breach and/or exfiltration of customer or protected data is confirmed, a plan should be in place to quickly minimize the damage to your network infrastructure, your brand, and your customers and employees.

As there is no silver bullet in a constantly-evolving environment where hackers are often several steps ahead of cybersecurity professionals (or at least adapt quickly to new security measures), a lawyer conducting due diligence on a company's incident response plan should evaluate the approach and process of the plan. Malware leaves signs or indicators of "bad behavior" on logs. Network traffic monitors may show spikes at unusual times, or even better, at regular intervals. A robust plan will have a process in place to correlate all of the indicators as quickly as possible and then escalate those more "suspicious" events for further review. In many cases, automated processes that correlate aggregated log data using "big data" analytics may be of particular benefit given the time-sensitive nature of event-response: any particular piece of malware could have devastating consequences if it is not quickly captured and eradicated.

## Business Continuity Planning

Information management business continuity planning requires implementing procedures to recover data and information from a backup source as quickly as possible in order to get systems back online. Business continuity planning was once the province of preparations for hurricanes, fires, and earthquakes, but in the wake of the devastating attack on Sony Pictures— as well as the companion announcement of the wiper malware attack on the Las Vegas Sands—it is incumbent upon a company (and its board) to plan for the consequences of a severe cyber-attack, which might involve the loss of data, the loss of servers, the loss of computer hard drives, and even the loss of VoIP-based phone systems. As many have noted, "The biggest risk a company faces in today's uncertainty of cyber-attacks is not being prepared."

Volumes can be (and have been) written about business continuity planning in general. Vendors abound in this area, many claiming to offer the "best" back-up and business continuity procedures. And of course, every company (whether it is U.S.- based or multi-national, or a financial institution, broker-dealer or "brick-and-mortar") is different when it comes to determining the most important elements of a business continuity plan, including which systems are critical to the organization, and how and when to bring them online. But in examining a company's continuity planning for a cyber-attack, at least the following issues should be addressed:

- Does the company have a written Business Continuity Plan?
- Has the company done a Business Impact Analysis that identifies the company's most critical systems and the maximum downtime that can be tolerated if they go down?
- What are the company's systems back-up procedures? How often is the full system backed up? Are back-ups maintained on the network? Has an "air gap" architecture been built into the company's back up-procedures so that a cyber-attacker cannot attack system back-ups because they are segregated and being held off of the network?
- Where are the back-ups held and how are they stored (network storage, external hard drives, or even in the cloud)?
- How long will the back-up media be maintained? How quickly can the company get to the back-up data when it is needed?
- Once the back-ups are accessible, what are the company's exact procedures for (A) obtaining whatever hardware is needed for the system restoration, (B) the restoration of the company's critical operating systems and applications, (C) restoring other data to their then-known back-up state, and (D) testing the restored system to make sure everything is working properly?
- Finally, as many telephone systems are internet-based, a telephone recovery strategy also needs to be in place.

Like an incident response plan, a business continuity plan needs to be tested, the personnel responsible for implementing it need to be trained, and it should be periodically rehearsed so that all involved (including third-party or outsourced vendors) know their roles in getting the organization's information management system back on line. Ideally, a plan should be put to the test through a full-scalefunctional exercise that includes a "full cut-over" and recovery to back-up data.

* * *

In many cases, the company that you are diligencing may be your own. It is indisputable that enterprise risk management is part of a director's fiduciary duty to the organization and its shareholders. And cybersecurity today is undoubtedly part of enterprise risk management, and thus within a board of director's oversight role:

> The control environment is the set of standards, processes, and structures that provide the basis for carrying out internal control across the organization. The board of directors and senior management establish the tone at the top regarding the importance of internal control and expected standards of conduct. Management and the board of directors have the authority and responsibility to set the top priorities of the company. If being secure, vigilant, and resilient is not defined as a priority and communicated within the organization, there is little hope that the organization will deploy sufficient resources to protect its information systems and to respond to cyber events appropriately.

Though the drafting of incident response plans and business continuity plans can be complex, the last 13 months of cyber-attacks have taught us both types of plans should be in writing, in place, practiced, tested, and ready to implement at any time. Taking the time to plan may well determine the fate of a company following a cyber-attack.

# Spencer Educational Foundation

## Risk Manager in Residence Program

■ **By Susan Meltzer,** Vice President, Risk, Aviva Canada

The Spencer Educational Foundation sponsors the Risk Manager in Residence (RMIR) program across the United States and Canada. This program matches up risk managers with universities for the purpose of visiting the campus, lecturing and meeting with students and faculty. A number of years ago, I was approached by the University of Calgary who encouraged me to put my name in for this program. Since then, I have visited eight university campuses from Calgary to California to Louisiana to Washington DC! This year, I had a very special placement sponsored by the Economics Department at York University.

Why was it special? Compared to sunny California and warm Louisiana in February? Getting there on the 401 during a freezing rain weather pattern? Quite honestly, it was special because it was a university close to home and where I could make a real difference with the students. I met formally with economics students at all levels - under-graduate as well as Masters and PhD candidates. I had sessions with the actuarial sciences students and talked about careers in risk management and insurance to a cross-functional group that included business and Corporate Finance. I discussed risk management, economics and politics with a variety of academics - gaining a totally different perspective. Oh, and I also got to have lunch with Steve Pottle!

I ran risk workshops where students role-played as the executives of an insurance company and a large telecommunications firm. The idea was to give them practice in risk identification. Their fresh outlook, anchored by their education, meant that they could identify a wide-ranging variety of risks and, in particular, those that are emerging in today's environment. I learned as much as they did. I spent a lot of time with them talking about their skills and education and how those could be of benefit to an employer in the future. When I got home, I accepted many LinkedIn invitations - as they were eager to begin their networking opportunities.

I also learned a lot about York, but in particular about their Experiential Education Strategy which connects students with employers to conduct unpaid research projects and paid internships. I am hoping to establish a relationship between Aviva and York going forward.

I would encourage you to consider volunteering for this program. I find that it has been not only beneficial to the students and their university, but it has been extremely rewarding for me.

# Six Dimensions of a Successful Global Risk Management Program

■ **By Nick Batten,** Vice President, Manager, Corporate Global Services, FM Global

**People buy insurance for two reasons:** either it is a requirement, or because they believe that, one day, they may have a loss and require compensation. Essentially, when clients receive a contract from the insurer in exchange for a premium, they receive a promise to pay that claim.

With supply chain networks growing vastly and the international presence of corporations reaching deeper into the four corners of the globe, the chances of a loss multiplies. And whether a loss occurs in a facility in Omaha, Nebraska, USA, or at a secondary site in Bangkok, Thailand, clients expect the same response—that the promise remains the same.

Providing seamless global coverage is not an easy undertaking. So what are the dimensions of a successful global risk management program?

**1. Global network with a worldwide reach**

One of the biggest decisions carriers face early in the course of building a global network is whether to 'plant a flag' in the form of an owned subsidiary in a territory or to depend on select partners to represent them in certain countries. Forming, capitalizing, staffing and maintaining local subsidiaries can be an expensive proposition and, in truth, no single carrier has the wherewithal to do so in every country. In many territories, local regulation may even preclude 'foreign' insurers from forming a fully-owned subsidiary even if they wanted to. So most global carriers' networks comprise a blend of owned licenses and partner facilities.

**2. Breadth and depth of a network**

If you asked 50 risk managers what qualities define a great global insurance network in their minds, somewhere along the line they'll point to network breadth and depth. They'll mention local presence and know-how. They'll want a consistent level of products and hands-on services delivered, as well as the ability to offer broad, compliant, on-the-ground coverages. They will need to settle claims locally and will want their carrier to offer consistent performance in terms of policy documentation and contract certainty. Odds are good that cost-effectiveness will feature prominently on the list, too.

**3. State-of-the-art global master form combined with broad 'standard' local underliers**

The ideal solution in structuring a global program is to have the local coverage and master coverage as closely matched, and as broad, as possible. This maximizes coverage in the local territory and therefore maximizes the local loss payment. When the underlyer policy is practically a mirror image of the master policy, the program structure ensures that maximum—not simply adequate—local coverage is in place. Should a loss occur, it can be paid with certainty at the local level.

*Continued on page 5 …*

## Six Dimensions of a Successful Global Risk Management Program

*… from page 4*

### 4. Balanced global and local service

Most risk managers value consistency when it comes to certain important aspects of their program, including capacity, coverage, claims and the level and quality of key services they choose. Yet keeping local constituencies and decision-makers engaged (and happy) can be an equally important element of a successful global program.

Because every client's needs are different, from a carrier's perspective, there is a need for a flexible service model that can be fine-tuned to ensure that centralized services and decision making authority are provided to the corporate client and that the agreed amount of localized, on-the-ground services are delivered to local subsidiaries and locations.

But meeting this corporate need for consistency, while allowing for a judicious degree of localized contact, service and decision-making, can be a delicate balancing act.

### 5. Consistent loss prevention engineering service, protocols and deliverables

As more companies expand their footprints overseas, they often find that the challenges they face in understanding hazards and managing risks grow proportionately.

Why? As companies establish themselves in places where they can produce more cost effectively, they often discover that the prevailing standards of protection and construction differ significantly from what they may be used to at home. Local codes may be lax or non-existent, often in regions that may be more prone to natural hazards. Also, local attitudes toward loss prevention can vary widely. So, unless companies go in with their eyes open and take prudent steps to manage those risks, what they seek to gain in productivity may be offset by the increased cost of risk.

### 6. Claims control and settlement via in-house claims adjustment network

One way of ensuring prompt claims service anywhere in the world, is by having insurers recruit, train and retain well-qualified claims professionals with on-the-spot authority, and who are located around the globe. Additionally, the role of an adjuster should begin long before a loss ever occurs, that is, by helping clients, both local and corporate, feel educated and prepared for a loss and developing shared expectations.

### Success in the global arena

Developing, communicating and executing a risk management plan can be a formidable hurdle for any enterprise. Even in the simplest organization, there are organizational boundaries to cross, decision-making structures to penetrate, and relationships with key decision-makers to cultivate. Of course, risk managers always have to think well beyond their own organizations. A successful risk management plan depends on a concerted effort from numerous parties, including underwriters, engineers, brokers, contractors and countless others who are integral to its success. Taking that same simple plan "global" means that extended communication lines, cultural differences, language barriers and time zones must be added to the list of challenges.

While daunting, these hurdles are not insurmountable. The key is to get all of the parts moving in the right direction at the right time. Experienced risk managers know that the answer lies in an agreed plan that has been communicated to all parties—such that individual assignments are fully understood in the context of the overall plan and all actions support that plan.

# Upcoming Industry Events

## 12th Annual Canadian Captives & Corporate Insurance Strategies Summit

**May 25-26, 2016 Sheraton Centre, Toronto ON**

This is the only Canadian conference dedicated to Captive Insurance and a must-attend event for current & prospective captive owners, captive managers and corporate insurance professionals. In an interactive and insightful environment, thought-leaders in risk management will come together to discuss best practices for using captives in risk mitigation strategy.

Make sure your Captives strategy is performing at its best. Be up-to-date with regulatory changes, tax updates and innovative investment strategies. The 2016 Summit features discussions on: Forming a Captive | Selecting a Domicile | Maximizing Captive ROI | Navigating Tax Law + MORE

**ORIMS Members receive 20% OFF Registration using VIP Code: ORIMS20**

**Visit: www.captivesinsurance.com for more information.**

RIMS-CRMP
RIMS-Certified Risk Management Professional

## Become a RIMS-Certified Risk Management Professional

**The RIMS-Certified Risk Management Professional (RIMS-CRMP)** establishes you as a recognized expert and leader in the risk management discipline—and a valuable asset to your organization. This professional distinction sets you apart from your colleagues and demonstrates your high level of knowledge, skills and experience. Stay competitive in today's economy with the RIMS-CRMP certification.

**Upcoming Exam**

**Testing Window:** October 15–December 15, 2016

**Fee:** RIMS Members US $350 | Non-Members US $500 (includes application fee)

*All eligible risk professionals may take the computer-based exam at Pearson VUE test centers during the exam window.*

**Learn more at www.RIMS.org/Certification.**

RIMS the risk management society

## Upcoming RIMS Workshops

Stay up to date on current risk management trends and developments. Advance your risk knowledge by attending an in-person workshop. These valuable educational offerings are designed to fit your evolving business needs.

| | |
|---|---|
| **Enterprise Risk Management** | **June 8-10** / Vancouver, BC<br>**August 17-19** / Winnipeg, MB<br>**October 19-21** / Toronto, ON |
| **Applying ERM Theory** | **September 15-16** / Calgary, AB<br>**November 3-4** / Vancouver, BC |
| **Integrating ERM & Strategic Planning** | **May 19-20** / Ottawa, ON |

## DRIE-SWO SPRING SYMPOSIUM

MONDAY, MAY $9^{TH}$, 2016
25 Water Street,
Kitchener, Ontario

The South Western Ontario Chapter of the Disaster Recovery Information Exchange (aka "DRIE-SWO") is having their Spring symposium on Monday, May 9th, 2016.

This year's theme is "Declarations – Lessons learned before, during and after a Disaster".

For more information visit: http://www.drie-swo.org/

# RIMS Canada Council Winter Planning Meeting

The RIMS Canada Council (RCC) met in Toronto on January 28-30th for their Annual Winter Planning meeting. As our ORIMS delegate was out of the country, I had the opportunity to participate as a substitute delegate.

The RCC is a passionate and dedicated group of people who present an amazing representation of the risk management profession from across our country. The importance and value of the RCC was clearly illustrated by the high level of representatives from RIMS; Gordon Adams, RIMS Board Liaison, Annette Homan, COO RIMS and Seamus Gearin, RIMS Canadian Consultant all took an active role throughout the 2½ day weekend meeting.

Gord and Annette provided an update on recent changes to the RIMS Board structure, the revised mission statement and other general updates. The new Mission Statement, "To educate, engage and advocate for the global Risk Management communities", reflects the "global" nature of the RIMS organization. They highlighted the excellent new resource of the OPIS platform and encouraged all RIMS members to visit and promote the use of this valuable communication tool.

An important topic of discussion was the new RIMS-Certified Risk Management Professional, ("CRMP") program, a credential that is foundational in elevating and recognizing expertise in the risk management discipline. Details about the CRMP are available on the RIMS website and as referenced in the latest edition of the RIMS Risk Management Magazine, including a call for participation in the pilot exam during the upcoming RIMS Conference in San Diego in April.

In addition to the customary RCC Agenda items, the meeting included a comprehensive Strategic Planning session, facilitated by consultant, Meredith Low. The goal was to articulate the purpose and mission of the RCC as well as to identify focus areas for the coming year. These include education, the RIMS Canada Conference and the opportunity to bring Canadian Chapter board members together to communicate what Canadians are interested in and to share best practices. The RCC will continue to enhance communications across Canada, and by providing a unified voice to RIMS, can also help expedite assistance more quickly than if the communication comes from separate Chapters. All Canadian Chapters are encouraged to share their issues, trends and accomplishments, as well as to provide articles to be included in the RCC newsletter for the benefit of all members.

An extremely valuable portion of the RCC meetings is a Roundtable sharing of experiences from each of the Chapters. We all came away with new ideas to bring to our Chapters to enhance networking and professional development opportunities and to improve efficiencies and cost savings in our operations.

I am grateful for the opportunity to have experienced this RCC meeting and look forward to continuing conversations with this talented group of people, who are committed to supporting and promoting the Risk Management profession in Canada.

*Valerie Fox,*
*Corporate Director, Risk Management*
*Progressive Waste Solutions, ORIMS Secretary*

## ANNUAL SPONSORED EVENTS

Curling Bonspiel - **February**
Spring Fling - **May**
Golf Tournament - **June**
Christmas Luncheon - **December**

ORIMS has launched its new sponsorship program! The 4 new sponsorship levels are designed to provide our sponsors with benefits throughout the year with all Platinum sponsors having the special benefit of a table for 10 at the annual Christmas Luncheon. The earlier a sponsor signs up, the more benefits a sponsor receives.

Visit the Sponsorship & Donations section on our website for more information and see the many benefits we are offering our supporters. Please consider becoming a sponsor of ORIMS for 2016!

LIVE WEBINAR

## Professional Development Webinar

Wednesday, April 20, 2016

10:00 a.m. – 11:00 a.m.

***Topic:***
*"Understanding Influences on an Electrician's Decision Making to Work Live"*

***Presenter:***
*Sarah Thorne, Cofounder and Principal, Decision Partners*

Sarah will discuss her findings of recent research undertaken for the Electrical Safety Association using Decision Partner's state-of-the-science method called Mental Modeling Technology™. The research demonstrated that there are many influences on electricians' decisions to work live. This insight is being used to guide ESA's policies, strategies and communications to significantly reduce serious injuries and deaths in the industry.

Join us for what is sure to be a very enlightening hour!

Registration information to follow shortly.

*SAVE THE DATE!*

orims
ONTARIO RISK AND INSURANCE MANAGEMENT SOCIETY

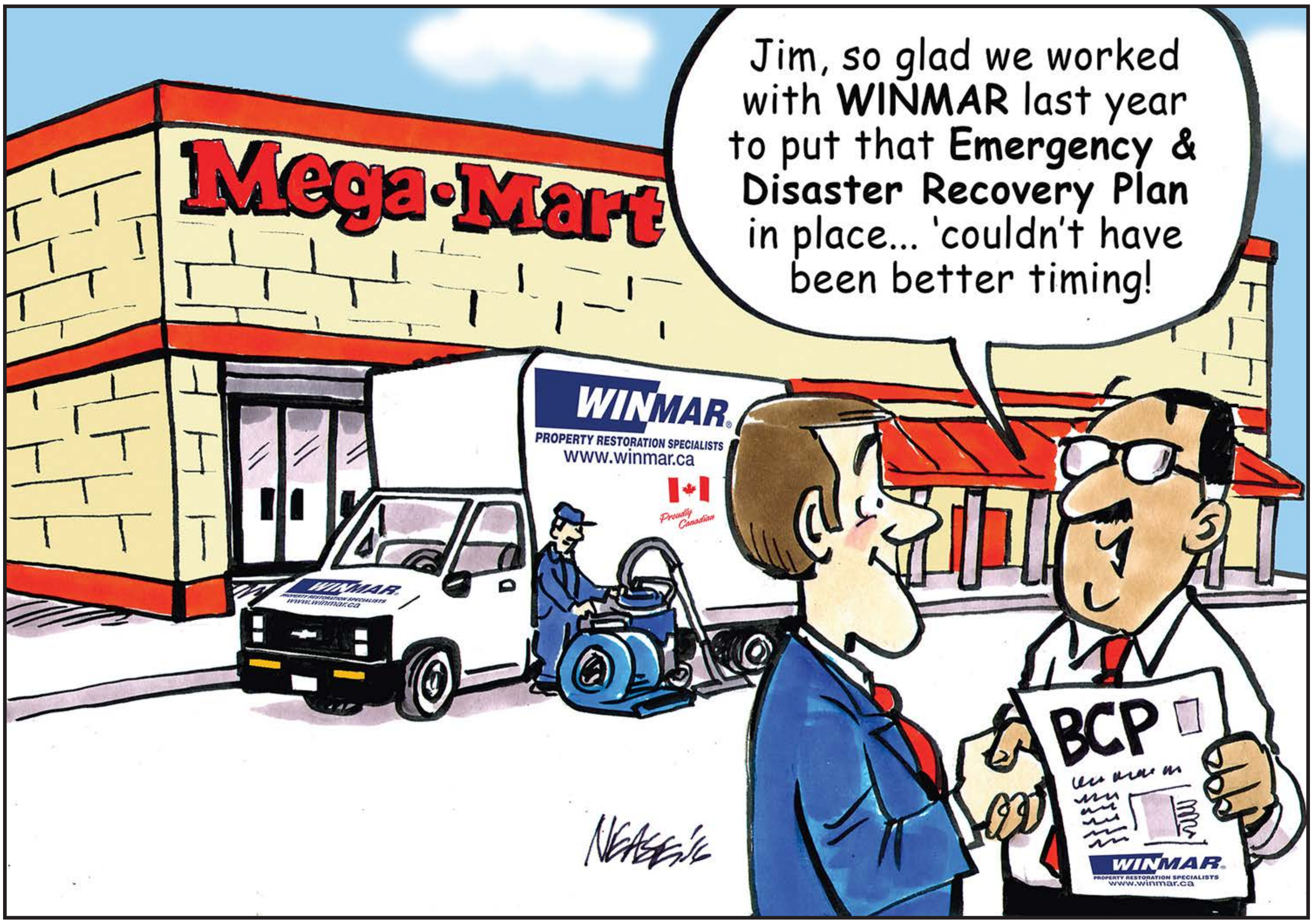
## Professional Development Day & Annual Spring Fling

Professional Development Sessions

*Wednesday, May 4, 2016*
*1:00 pm – 4:00 pm*

McCague Borlack Learning Centre,
Toronto Head Office, The Exchange Tower
130 King Street West, 27th Floor, Toronto, Ontario
(Speakers and topics to be announced soon!)

**Spring Fling Reception**
**4:30 pm – 8:00 pm**
(Location details to be confirmed.)


Jim, so glad we worked with WINMAR last year to put that Emergency & Disaster Recovery Plan in place... 'couldn't have been better timing!
Mega-Mart
WINMAR
PROPERTY RESTORATION SPECIALISTS
www.winmar.ca
Proudly Canadian
BCP
WINMAR
PROPERTY RESTORATION SPECIALISTS
www.winmar.ca
NEASE

# Chapter Events

## 2016 ORIMS Curling Bonspiel

On Monday February 29th, 2016 ORIMS hosted the Annual Edward C. Ricketts Memorial Curling Bonspiel, held at St. George's Golf & Country Club. It's always a busy time of year and despite the continued fight through flu season and the bitter winter elements, the event was well attended and a good time was had by all. A big thanks to everyone in attendance, as we managed to raise $1,000 for Second Harvest.

For the 2nd year in a row Chubb Insurance took home the championship at the tournament this year. Congratulations to:

Skip – Lilia Fernandes
Vice – Cameron Brady
Second – Wayne Briggs
Lead – Aaron Weinstock

This event could not have been the success it was without the support of our sponsors: SCM Insurance Services, AON Canada, McCague Borlack and Chubb Insurance. Your generosity and faith in our organization is greatly appreciated. Lastly, a special thank you goes out to Deborah Robinson from Canadian Litigation Counsel for her tireless efforts in support of this event. Thank you all so very much.

James Eka
Director of Social Programs

# Chapter Events Cont'd.

# ORIMS 1ST WEBINAR!

ORIMS held their first hour long webinar on January 20, 2016. The topic was LEVERAGING DATA TO QUANTIFY RISK presented by Ryan Durrell of Axxima, Actuarial & Insurance Management Advisors. Ryan spoke about the importance of collecting good data and how to use it to help quantify risk. He was an entertaining presenter and offered relatable and useful ideas to get us thinking.

The webinar was well attended with approximately 50 people registering for the event. We received a lot of positive feedback and over 50% of attendees thought it would be a great idea to do it again.

We would like to thank Ryan for being ORIMS' first Webinar presenter and James Eka, our Director of Social Programs, for all of his hard work on making this first webinar happen. Not only did he do a great job hosting, he was also the "behind the scenes" tech expert pulling it together to ensure members enjoyed a smooth webcast. Thanks Ryan and James!

Stay tuned for our upcoming webinar on April 20th. The topic for April will be Understanding Influences on an Electrician's Decision Making to Work Live which is based on state-of-the-science method called Mental Modeling Technology™ presented by Sarah Thorne of Decision Partners.

**Webinars are free to all members!**

## 2015-2016 ORIMS Board of Directors

**Tina Gardiner**
President

**Vacant**
Vice-President

**Mark Cosgrove**
Treasurer

**Valerie Fox**
Corporate Secretary

**Vacant**
Public Relations
& External Affairs

**Helen Trajanos**
Professional
Development

**Colleen Bryan**
Communications

**Glenn Morato**
Membership

**James Eka**
Social Programs

**Terry Lampropoulas**
Social Media

**Cindy Chan**
Education

**Roman Parzei**
Board Advisor

**Julian Valeri**
Past President

## Editorial Policy

The PULSE is a publication of the Ontario Risk and Insurance Management Society and is published periodically throughout the calendar year.

The opinions expressed are those of the writers and the volunteer members of the PULSE Editorial Committee. Articles submitted to the PULSE for publication are subject to the approval of the PULSE Editorial Committee. Approval of such articles is based upon newsworthiness, and perceived benefit to the readership. All decisions of the PULSE are not subject to appeal. Individuals submitting articles to the PULSE hereby acknowledge their acceptance of the PULSE Editorial Policy.

## Editorial Committee

*PULSE is produced on behalf of ORIMS by,*
PAPPLE GRAPHICS.