PULSE

ORIMS
ONTARIO RISK AND INSURANCE
MANAGEMENT SOCIETY

THE HEARTBEAT OF RISK MANAGEMENT, Winter 2015

President's Message

■ **By: Julian Valeri,** ORIMS President

It's hard to believe that we are already into the year 2015! Perhaps even harder to believe is the fact that seven months have passed in my term as your President of ORIMS – and what a busy seven months it has been!

At the June, 2015 AGM (held jointly with the ORIMS Golf Tourney) the new Board embarked on an exciting journey together. What we lacked in long-term experience with ORIMS has been more than off-set by the enthusiasm, innovation and commitment to serving our members.

Some of our achievements to date have been:

A Blue Sky meeting was held last June to approve budgets and projects for the 2014-15 year;

Risk Management Wall and Desk Calendars were produced, printed and distributed to all members. ORIMS recently received recognition for the two resources from RIMS who have

recommended other Chapters consider these as "best practices" for engaging their membership;

We have welcomed 38 new members since the May AGM, bringing our total Corporate, Deputy and Associate Membership count to 339 members – by far the largest RIMS Chapter in Canada;

Last month, ORIMS hosted our annual Christmas Luncheon. Once again it was resounding success with over 700 registered in attendance on a snowy winter's day and $10,000 donated to the Daily Bread Food Bank!

The Don Stuart Award Committee selected Anne Chalmers, Teck Resources as the most recent Award winner;

Many members of your ORIMS Board are also members of the national RIMS Council of Canada and RIMS Committees, which continue to bring a wide perspective back to our Chapter;

Professional Development workshops have also seen a new look for this year. Starting last November, we introduced a new twist on the workshop format. It's an entirely NEW Program consisting of three workshops presented by 'Fail Forward'. Each workshop is a stand-alone learning session and can be attended individually. Participants completing ALL three sessions will achieve a Certificate of Completion in Fail Forward Resiliency Training. The first session was very successful, and the topics planned for the new year promise to build on the momentum we have started – don't miss out

I could certainly go on and on with the activities that are going on behind the scenes, but these are just a few examples of what we have achieved in the first half of our mandate – and we are only just getting started!

As we enter the second half of our mandate, I want to take this opportunity

to re-introduce the Board of Directors to you and give a warm thank-you to each of them for the great work that is being done on behalf of you, our ORIMS members.

These individuals have shown their dedication and tireless commitment to our Chapter to make all these things happen so effortlessly (at least on the surface!).

Our 2014/15 Board of Directors:

President –
Julian Valeri, *Region of Durham*

Vice President –
Paul Provis, *Ontario Government*

Treasurer –
Mark Cosgrove, *Ontario Power Generation*

Corporate Secretary –
Valerie McDonald, *Progressive Waste*

Public Relations/External Affairs-
Helen Trajanos, *TCHC*

Professional Development -
Tina Gardiner, *Region of York*

Education –
Agata Jamroz, *RBC.*

Communications –
Riaz Juma, *Bentall Kennedy*

Membership –
Joseph Costello, *HydroOne*

Social Programs –
James Eka, *CURIE*

Webmaster –
Glen Morato, *SunLife Financial*

Past President –
David Beal, *OSBIE*

On behalf of the ORIMS Board of Directors, I would like to take this opportunity to wish everyone a safe and Happy New Year.

Julian Valeri
President, ORIMS

2014–2015 ORIMS Board of Directors

TO PROMOTE AND ADVANCE EXCELLENCE IN RISK MANAGEMENT

EYES WIDE SHUT: The Best Defence is a Good Offence

■ **By: Catherine Korte,** Partner, McCague Borlack LLP

With the increasing interconnectivity of businesses to date, information is now exposed to a broad number of threats. Businesses need to ensure there is protection of information in order to prevent loss, unauthorized access or misuse. Businesses must have in place a process of assessing threats and risks to information and the procedures and controls to preserve the information. There are three guiding principles:

1. Confidentiality. Access to data must be limited to authorized parties.
2. Integrity. The data must be authentic and complete.
3. Availability. The data must be accessible, as needed, by those who are authorized to access it.

(Foundations of Information Privacy and Data Protection; A Survey of Global Concepts, Laws and Practices; Peter Swire, Kenesa Ahmad).

To minimize the risk to an information system, many factors need to be considered. One industry standard risk assessment formula is: Risk = Threat x Vulnerability x Expected Loss.

Security metrics help evaluate the effectiveness of security policies, processes and products as well as calculate the risk and determine the value of reducing or mitigating a risk. Some of the metrics that contribute to a risk/threat/vulnerability/loss matrix are the number of security breaches, the number of system outages and the number of lost information assets. Additional factors include the presence of software viruses and the use of investigation such as computer auditing and forensics.

The PC World Work Life Productivity recently published the 10 best practices to prevent data and privacy breaches as follows:

Data breach resulting from poor networking choices. Small and medium businesses often generally lack the budget necessary for equipment foregoing the use of routers and plugging directly into the Internet.

McCague Borlack LLP Cyber Risk Summit 6 of 104

1. Data breach resulting from improper shredding practices. The "dumpster diving" identity thieves target businesses that throw out paperwork without shredding it. All documents with sensitive information or personally identifiable data need to be thoroughly shredded before disposal.

2. Tax records theft around tax time. Businesses need to be focused on incoming and outgoing information related to taxes. Identity theft often steal tax returns from an outbox or mailbox.

3. Identity theft resulting from public databases. Businesses publish information about themselves in public databases. Business owners will want to maximize its exposure while still protecting individual privacy. Many individuals with Facebook profiles have their address and date of birth. Many identity thefts can use information searchable publicly to construct a complete identity.

4. Identity theft resulting from using a personal name. Sole proprietors that do not take the time to file a business as application are far higher risk of identity theft due to the personal name rather than the business names being published publicly.

5. Bank fraud due to gap in protection or monitoring. Business owners note that it is vital to balance their accounts every month to ensure cheques are not being written out of business funds. Businesses rarely, if ever, check what credit accounts have been opened under the business name. Monitoring services can alert business owners when new credit accounts are opened fraudulently.

6. Poor emailing standards. Many businesses use e-mail as if it is a secure means of communicating sensitive or confidential information. The reality is pretty much the exact opposite. Emails are available for a number of people other than the recipient, and there is generally ample opportunity for e-mail communications to be intercepted in transit. It is more appropriate to treat e-mails as postcards rather than sealed letters.

7. Failing to choose a secure password. Use secure passwords.

8. Not securing new computers or hard drives. Often businesses without a dedicated IT Department or security administrator should consider using outside consultants to lock down PCs and hardware. Larger businesses should insure IT Departments and their information security administrator secure all new computers and hard drives.

9. Social engineering. Social engineers are individuals that call and claim they are from another organization. Social networks like Facebook and Linked In. An attacker may even claim to be with a firm that the business owner does business with. If someone you do not know calls on the phone, or contacts you by email through a social network make sure it is the person you think it is before revealing passwords and confidential information.

McCague Borlack LLP Cyber Risk Summit 7 of 104

10. The Treasury Board of Canada has guidelines for privacy breach. The guidelines for privacy breach provide guidance to institutions on the management of privacy breaches. These deal with general requirements under the Act with respect to collection, retention, use, disclosure and disposition of personal information.

1. What is a privacy breach?

According to the Treasury Board of Canada website it involves the improper or unauthorized collection, use, disclosure, retention or disposal of personal information. A privacy breach may occur within an institution or off site and may be the result of inadvertent errors or malicious actions by employees, third parties, partners in information sharing agreements or intruders.

2. Potential causes of privacy breaches

According to the Treasury Board of Canada Secretariat's website, these include the following situations that could result in

the disclosure of, or access to, personal information by unauthorized parties:

- The theft, loss or disappearance of equipment or devices containing personal information;

- The sale or disposal of equipment or devices containing personal information without purging prior to sale or disposal;

- The transfer of equipment or devices without adequate security measures;

- The use of equipment or devices to transport or store personal information outside the office for telework or off-site work arrangements without adequate security measures;

- The inappropriate use of electronic devices to transmit personal information, including telecommunication devices;

- Intrusions that result in unauthorized access to personal information held in office buildings, file storage containers, computer applications, systems, or other equipment and devices;

- Low level of privacy awareness among employees, contractors or other third parties that handle personal information;

McCague Borlack LLP Cyber Risk Summit 8 of 104

- Inadequate security and access controls for information in print or electronic format, on site or off-site;

- The absence of provisions or inadequate provisions to protect privacy in contracts or in information-sharing agreements involving personal information;

- Insufficient measures to control access and editing rights to personal information, which may result in wrongful access to, and the possible tampering with, records containing personal information;

- Phishing or the use of deceptive tactics to trick an individual into providing their personal information either directly or by going to a fake website. For example, an individual pretending to perform system maintenance calls a government employee to obtain his or her security password; and

- Pharming or the use of a fake copy of an official Government of Canada website to redirect to a malicious web site in order to steal information without the user's knowledge. This method takes advantage of the weaknesses in the Data Network System (DNS). For example, an individual accesses what he or she believes is an official government website and submits personal information as requested by the site. The individual is unaware that he or she has been redirected to a fake copy of the official website.

3. Preventing privacy breaches

To prevent a privacy breach the Treasury Board of Canada has recommended institutions should:

- Follow the requirements of the Policy on Government Security (PGS) and other security direction issued by the Treasury Board of Canada Secretariat (TBS). The Royal Canadian Mounted Police (RCMP) and the Communications Security Establishment Canada (CSEC) also issue direction on physical and information technology security, respectively;

- Conduct Privacy Impact Assessments (PIAs) and Threat and Risk Assessments (TRAs) in accordance with the Directive on Privacy Impact Assessment;

- Take privacy into account before making contracting decisions or entering into information-sharing agreements. Government institutions should include adequate privacy protection provisions, such as a requirement to immediately notify the government institution of a privacy breach. For more information, consult the TBS Guidance Document: Taking Privacy into Account Before Making Contracting Decisions;

McCague Borlack LLP Cyber Risk Summit 9 of 104

- Provide regular and ongoing training to employees, managers and executives to ensure that they are aware of the requirements of the Code of Fair Information Practices, Privacy Act, related TBS policies, and departmental or agency security and privacy practices and procedures;

- Ensure that personnel working off-site are aware of their privacy and security responsibilities. This means ensuring that appropriate measures are taken to safeguard the personal information they handle off-site. Government institutions should consider keeping personal information in-house when telework or similar arrangements would involve considerable privacy risks (e.g., a large volume of personal information or sensitive personal data);

- Establish clear administrative controls that restrict access and editing rights to records containing personal information to only those employees who have a legitimate need to know, and for institutions to put in place appropriate audit trails to ensure that these administrative controls are functioning as intended;

- Use cryptography (encryption) to protect sensitive personal information stored in a computer or a portable storage device or being transmitted through e-mail, on a government network, a wireless network, or across the Internet. The PGS provides further direction on encryption;

- Purge all equipment and other electronic devices containing personal information before selling, disposing of, or transferring such equipment or devices;

- Empty security containers such as file cabinets, safes or mobile shelving units and ensure that no classified or protected material is left inside before selling or transferring them to other responsibility centres or outside the government;

- Take precautions against "phishing" and "pharming":

  – Ensure that requests for personal information are valid and that individuals asking for personal information are who they claim to be;

  – Refuse to provide personal information in response to an unsolicited telephone call, fax, letter, email attachment or Internet advertisement;

  – Be on the lookout for clues indicating that a website may be fraudulent (e.g., spelling errors, unusual advertisements, or portions of the site that do not work properly);

  – Check the lock icon at the bottom of your browser to ensure that you are sending personal information over a secure connection; and

  McCague Borlack LLP Cyber Risk Summit 10 of 104

  – Verify the phone number and call the organization to determine validity if you have any concerns.
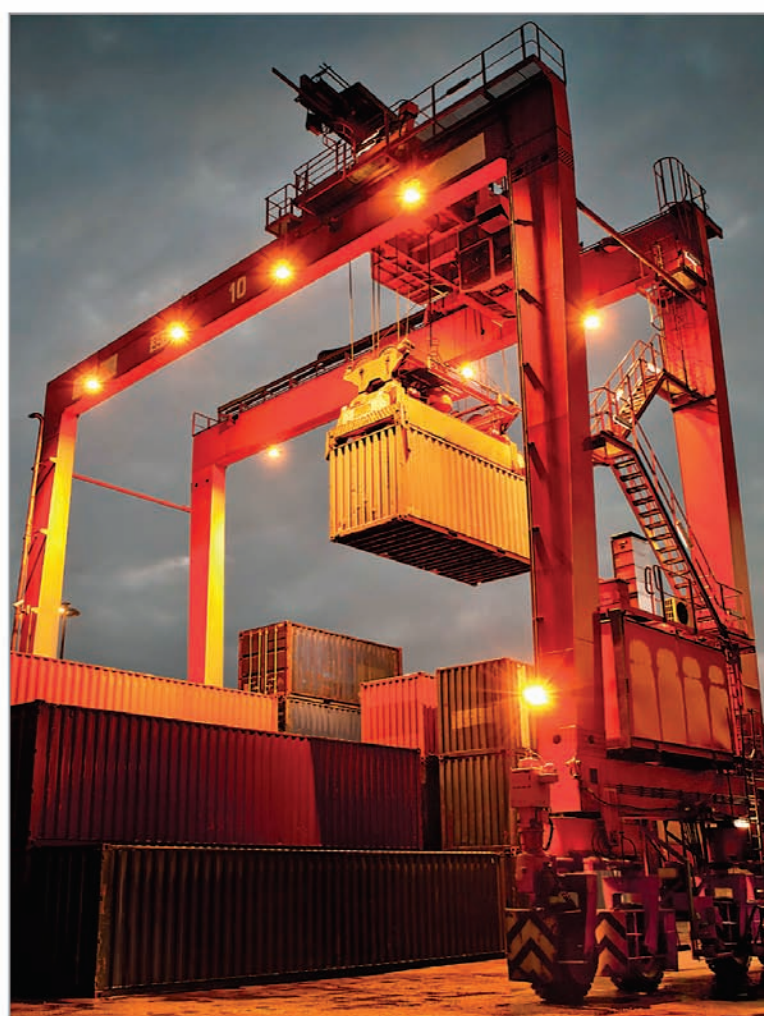
4. Privacy Breach Management Process

Institutions should consult the Privacy Breach Management Toolkit for effective privacy practices, plans and procedures to address privacy breaches.

Examples of best practices in managing privacy breaches include:

- Preliminary assessment and containment;

- Full assessment;

- Notification (to affected individuals and internal management where required);

- Mitigation and prevention;

- Notification of the Office of the Privacy Commissioner of Canada (OPC) and the TBS; and

- Sharing of lessons learned.

In summary, the best defence is using a good offence to prevent privacy breaches from occurring in the first place.

Professional Development
Workshops 2014-15
November 18, 2014, January 19, 2015 and April 23, 2015.

ORIMS has partnered with Ashley Goode of the *FAIL FORWARD ORGANIZATION* to bring you a three (3) session programme that examines the concept of "Intelligent Failure" and how this can reshape our approach to complex problems and business risks while pushing the boundaries of creativity in our workplaces. ORIMS is hosting three workshops with *FAIL FORWARD*, leading to a **Certificate of Completion in Fail Forward Resiliency Training for those that complete all three workshops.** (For those that missed the first session in November we may rerun Workshop#1 if there is high demand, to allow for certification for those that missed the original Workshop #1 date.)

These workshops move beyond the rhetoric and focus on how to fail intelligently in practice. This means understanding failure and risk in a whole new way and harnessing the productive potential of our failures. They are hands-on, interactive sessions that use tools and activities developed by Fail Forward to transform the experience of failure. Participants will walk away with tangible skills, insights and actions that help them, and their organizations, fail better.

Before launching *FAIL FORWARD*, Ashley worked in Cairo with the United Nations Environment Programme and as a management consultant in Vancouver, Canada. In both lines of work, Ashley saw a fear of failure inhibit innovation, adaptation, and performance. In response, she launched both *AdmittingFailure.com* and the consulting firm, *FAIL FORWARD*, to spark a shift in how we perceive and talk about failure, and to help organizations learn, innovate and build resilience.

Since early 2011 Ashley has worked with organizations – from grantmakers and non-profits to government and private sector companies – to use failure as a learning tool and culture driver to support and foster innovation. She is well known for building the Organizational Learning Team at *Engineers Without Borders Canada*, and she continues to lead their annual *Failure Report*.

Her work on failure has received coverage in a wide range of media and news outlets, including: *The Globe and Mail*, Report on Business, Leadership Lab, *CBC Radio* in interview with Arlene Dickinson and Matt Galloway, Public Sector Digest, *Toronto Star*, *National Post*, and most recently on *CBC's* Lang & O'Leary Exchange. Ashley was also the 2013 recipient of the prestigious Harvard Business Review and McKinsey Innovating Innovation Award.

….so what is intelligent failure? Ashley blogged about this on her website (https://failforward.org)….and here is a copy of that blog from February 26, 2014…..

What does it mean to fail intelligently and what is an intelligent failure? I use the concept in verb and noun form as a catch-all to succinctly describe an ideal way of interacting with failure.

The concept comes from the recognition that to solve our most complex problems requires a different relationship with failure. Generally speaking, there are two sides to the concept of intelligent failure: There is the learning, adaptation and resilience side; and there is the Innovation, creativity and agility side. The sides seem disparate at first – the learning happens after a failure, the innovation happens because you made room for failure at the start – but I've found the pursuit and practice of one side often leads to improvements at both.

Intelligent failure is NOT about celebrating failure or even embracing it. I have spent too much time around people in the midst of failure to use those terms. Failure sucks. But it's also largely inevitable. So considering it's going to happen, someone who fails intelligently is able to get beyond the negative experience and realize the best thing we can do with a failure is to maximize our learning from it.

Intelligent failure is the intentional practice of reacting to failures more productively. Since we are not taught how to fail, our instinctive reactions to failure are usually defensive, dysfunction and generally don't serve us very well. But intelligent failure is a skill that can be practiced.

The gap between where we are, and where we want to be, is often filled with learning, innovation, and change. The practice of intelligent failure is both about maximizing productive learning post-failure, and about understanding your personal and organizational tolerance for failure and opening it up effectively, where possible.

Personally, this practice might mean reacting with appreciation and curiosity for what was learned when we or those around us fail.

It could also be communicating failures to ourselves and others in a way that focuses on the learning.

Organizationally, the practice of intelligent failure might be a creating a safe place for innovation to thrive because effort and smart risk-taking is rewarded, not just outcomes and successes. It might also mean using failures as opportunities to see ways to become more resilient.

Finally, the ability to fail intelligently, whether personally or organizationally, is increasingly an essential skill in an ever-changing world. Eddie Obeng talks about how the pace of change of our world has surpassed our ability to learn and have the knowledge needed to solve our most important challenges so we have to create space to experiment, figure out what does and doesn't work, learn and adapt.

On Tuesday, November 18, 2014, 50 Risk Managers and Insurance Professionals took part in workshop #1. This workshop started by encouraging participants to consider the tension between keeping our organizations safe and free from harm by managing risk versus keeping our organizations innovative and experimental by accepting risk as two opposing but valid approaches to managing complexity and uncertainty. Using *Fail Forward's* Innovation and Risk Appetite Assessment tool, participants then assessed their organization's risk tolerance. This was not your typical risk assessment! It gave us the toll tool to examine an organization from the perspective of how much risk should be accepted to see innovation and bring your organization into the future as opposed to how much risk needs to be managed to avoid loss. A great discussion and sharing session followed the exercise.

The fee for each workshop is $150 for members and $180 for non-members plus applicable taxes.

WORKSHOP #2 – FAIL FORWARD

Monday, 19th January 2015 – The Toronto Board of Trade, First Canadian Place   100 King St. W., Toronto, ON

This workshop started with a crash course in Intelligent Failure. We dove into the Intelligent Failure Learning and Innovation Loop which explored the many different types of failures, started to talk about these failures more productively and subsequently learned how to react to the different types of failures appropriately.

This set the stage to work toward single and double loop learning where the former involved "identifying and correcting errors in the external environment" and the later asked participants to "also look inward. They needed to reflect critically on their own behavior, identify the ways they often inadvertently contributed to the organization's problems, and then changed how they acted."[1] Closing out this workshop was a fun exercise which asked participants to reflect on a failure that they had in the past and practiced sharing it in a way that maximized learning. ([1] Argyris, Chris (1991). Teaching Smart People How to Learn)

WORKSHOP #3 – ORGANIZATIONAL LEARNING

Thursday, 23rd April 2015 – The Toronto Board of Trade, First Canadian Place 100 King St. W., Toronto, ON

The final workshop in the series will be kicked off by examining some of our neurobiological and otherwise instinctive reactions to failure and what we can do - in spite of our often dysfunctional reactions - to build a more productive relationship with failure.

We then present a metric for participants to assess the learning and innovation competencies of their organizations. This metric recognizes our instinctive reactions to failure often prevent us from maximizing what we can learn so sets out competencies that allow us to protect against our instincts. It is a useful tool to identify where improvements can be made to allow learning and innovation to thrive.

Finally, we'll look at the various approaches for visualizing failure in order to detect failures early and deal with them appropriately. We will explore how this scenario-based exploration ties into after action reviews and the continuous learning that happens along the way.

Be sure to watch for the registration form blast email or check the ORIMS website for the registration form …..and register for the final Workshop #3. Request a repeat of Workshop #1 if you missed it the first time…so we can measure the demand. Come out and network with your colleagues and learn new skills. Don't miss out!

Understanding Your Risks with Analytics

■ **By: Patrick Bossey** Manager, Business Intelligence Unit Crawford & Company (Canada) Inc.

In today's business world, there is a lot of buzz and discussion around data and analytics. While the concepts themselves are relatively straightforward, the business applications become as broad and diverse as the organizations that leverage them. This is where it can become overwhelming.

In 2012 Crawford & Company (Canada) Inc. created a Business Intelligence Unit to provide performance management analytics and intelligence in support of internal business decisions as well as consultative analytics and stewardship for our clients in support of their business decisions. As a result, we have established a fairly strong sense for how analytics are being leveraged both on the risk management and claims management side.

So, what are the keys to transforming noisy data into meaningful information? As we will explore, it is about starting small, staying focused and leveraging the business' knowledge and experience.

Start Small, Stay Focused

Some of the Business Intelligence Unit's most successful initiatives have started with little more than a client or business leader having a hunch and some anecdotal evidence. From there, the team can isolate the necessary data and focus the analysis on answering the question. For example:

– A property management client was concerned that allowing walking groups to use the malls for exercise before stores opened was resulting in high frequencies of claims, and was considering revising their policies regarding the practice. We worked with that client to analyze several years' worth of claims data and confirmed that there was a high frequency of claims occurring related to those walking groups. However, further analysis showed that the total incurred costs associated with those incidents was lower than expected since very few of the individuals would actually pursue a claim against the property manager. The client was able to evaluate the costs of claims and the potential negative impacts on goodwill that a policy change would have. The client concluded leaving the current policies as they were would be worth the risk.

In this situation, we looked at answering very specific business questions and focused on the data that was relevant to

the particular business question. However, as we worked through the analysis, other pieces of data and information arose that created tempting tangents; this is where our focus became so critical – otherwise we could have succumb to scope creep and not delivered in a timely or effective manner.

Leverage Businesses Knowledge and Experience

This is by far the most important component of a successful analytics initiative. This is how you effectively interpret what the data and statistical results actually mean to the business. In the particular example that follows, that business knowledge was the key to unlocking the story the data was trying to tell.

– Crawford was approached by a retail client to validate the assumption that higher frequencies of losses were occurring on the weekends than on weekdays. Analyzing several years' worth of claims data confirmed that Saturday would typically see the highest claim volume of any day during the week – consistent with sales volumes and store traffic on that day. However, further analysis revealed the day with the second highest frequency of losses was a particular weekday but we could not explain why. It was the client's business knowledge and expertise that revealed that staffing levels were different on that weekday, which likely contributed to the frequency of claims.

An analyst can identify that a particular day of the week has higher frequencies of losses than others or that certain provinces or cities will see higher rates of litigation stemming from slip and fall, and trip and fall claims. But sometimes, the analyst cannot answer why that is the case. That is where leveraging the appropriate business knowledge and expertise becomes so valuable to the quality of the output.

The key to successfully and effectively analyzing and interpreting risk and claims data is collaboration between business stakeholders and analysts, and here is why: when a business stakeholder is the one asking the business question and analyzing and interpreting the data, there is a potential for confirmation bias. The data is often subconsciously interpreted to support the business stakeholder's initial preferences or feelings towards the business decision in question. Interpreting what a result of 50% means then becomes no different than the old idiom "is the glass half empty or half full?" In other words, it is just the person's view on it.

Conversely, an analyst is able to perform a series of tests establishing correlation and causation with a high degree of confidence and a very neutral statistical interpretation of what the data means. However, the analyst may not apply the right context, framework and nuisances of the business. This could ultimately lead to a misinterpretation of what the results actually mean when applied to the business question at hand or an inability to simply answer "why?" without them layering in their business knowledge and expertise.

By working together, you can get very different perspectives and points of reference on the data and that usually results in a more robust and holistic interpretation of what the numbers actually mean.

New Perspective on Hoarding

■ **By: Rory MacKinnon,**
  Director of Commercial and Large Loss Division at Paul Davis Systems of Toronto, York and Durham Region

Let me come clean from the start. I'm not an authority or expert on hoarding behaviour, although I have been involved in numerous fire and flood restoration projects which involved large quantities of possessions belonging to residents believed to be afflicted with hoarding disorder. Much of the information that follows I've gleaned from research and from interaction with Fire Prevention officers and Mental Health professionals.

My goal in the next 1700 words or so is to describe, from a restoration contractor's point of view, how mental health professionals view hoarding disorder, and how we as building owners, property managers or contractors might need to reconsider our approach in dealing with situations that involve hoarding behaviour. There's a little bit of good news in that we're seeing the startup of Hoarding Task Forces in certain districts of Ontario, but more on that later.

Much of the specific information I've included below about common characteristics of hoarders, criteria for diagnosis and methodologies used to help individuals suffering from hoarding disorder comes from Integrated Hoarder Response's (IHR) website

(ihrhelp.com). IHR provides therapy for hoarders and helps them systematically remove excessive items from their home. Their website states that recovery from hoarding disorder requires between 12 and 16 sessions. I've highlighted some of the main points below, but more comprehensive information can be found on their site.

In 2013, Hoarding Disorder was designated a distinct mental disorder in the DSM-5 (Diagnostic and Statistical Manual of Mental Disorders). Prior to this, hoarding behaviour was thought to be an Obsessive Compulsion Disorder (OCD), but therapies generally used to treat OCD had little effect on hoarding behaviour.

Hoarders often live alone, have few social contacts and are usually isolated from family and friends as a result of their home environment. IHR finds that 90% of their clients have serious medical conditions and health issues; many of them suffer from depression and/or anxiety. Criteria for diagnosis consider the volume of clutter in living areas, the extent that normal activities are precluded because of limited access to rooms and the level of dis-

tress or impairment in functioning for the resident due to the hoarding behaviour.

Some hoarders acquire vast piles of valuable items. Often these items are not properly cared for, become damaged and eventually become valueless. The bulk of things generally hoarded are free including used newspapers, furniture, clothing, toys, curbside materials, dumpsters, trash and donation boxes. Animal hoarding is also common. In Durham Region, Ontario there are several new cases reported every month.

Typical signs that might indicate a hoarding problem include clutter outside a home, unpleasant smells coming from a residence, presence of flies or maggots, unpaid bills when finances are not an issue or when heating, plumbing and electrical systems are not repaired. In severe cases, sinks, stoves, beds and tubs are filled with clutter to the point that residents cannot use these facilities. Only ap-

propriate professionals should be consulted for a proper assessment.

Megan Phillips, program coordinator for IHR confirmed with me that her 'participants' report intense pleasure when they acquire things. The pleasure sensation reinforces the hoarding behaviour so

that the 'rush' becomes similar to a chemical dependency. Phillips contends that she often sees two thought processes that simultaneously exist for hoarders: the Pleasure Principle and Avoidance of Pain. When the driving mental force that seeks to obtain gratification is not met, the result is a state of intense anxiety. The removal of possessions is generally connected with the emotions that sit at the root of hoarding behaviour. Hoarding behaviour is reinforced in two ways: the intense pleasure experienced from acquiring and the anxiety experienced when their items are discarded. Although it is natural for people to project some meaning on their material possessions, hoarders ascribe intense value to all of the items in their home.

I recently spoke with an insurance adjuster who had settled a claim with an insured who was a hoarder. When the adjuster arrived to inspect water damage at a condominium apartment, she admits that neither she nor the restoration contractor who accompanied her, fully appreciated the value the insured put on her possessions.

Throughout the condominium were towering stacks of clothing, luggage and miscellaneous items. Heaps of contents filled the kitchen, bathroom (including tub and shower area), living room and the bedroom. The bed itself was filled with items and it was obvious that the insured

habitually slept on a living room couch and had no access to her kitchen or bathroom facilities due to the extensive clutter. The insurance adjuster eventually learned that the insured showered daily at her gym and ate all of her meals at restaurants. The insured was financially well off and

was a well respected professional within the legal community.

The contractor assessed that his crew would need to pack and remove a large quantity of contents to his warehouse so that he could extract water from the affected floor area, remove any unsalvageable material and start the drying process. As the contractor's crew began to pack the insured's contents, the insured began to display signs of growing agitation. In a flash of emotion the insured lashed out at him and his team accusing them of stealing some of her prized possessions. She ordered them to stop and threatened to call the police. All packing ceased and the insurance adjuster returned along with the building superintendent. The superintendent suggested the insured look through all her belongings before calling police. The contractor and adjuster waited outside of the condominium unit in the hall while the insured looked for the missing items. Over two hours later, the insured erupted in joy that she found the missing items. The insurance adjuster decided to negotiate a final settlement with the insured rather than cause any further complications on her file. The insurance adjuster did hear later that the superintendent tried to help her reduce the volume of her items along with some of her neighbours. The gains were short lived and she ended up filling her unit again with heaps of contents. As far as the adjuster knows, the unit was never properly dried or cleaned as a result of the water loss.

The contractor mentioned above, was simply acting on his technical training. Dry down a building and contents as fast as possible in order to reduce the opportunity for further damage and to ensure there is no onset of mould. He had no understanding of the implications of hoarding behaviour and simply carried out the procedures described for drying jobs.

Not only do restoration contractors need to adjust their protocols to effectively deal with hoarding issues. A fire prevention inspector advised me that he 'has learned to deal with the person and not just their stuff.' What does this mean? He must still do his job per the Ontario Fire Code. He told me that when inspecting a suspected hoarder's house or apartment he is careful to maintain a respectful tone with the resident. His first priority is

Community Service Bulletin

Daily Bread: More than just a food bank.

For many people coming to a food bank for the first time, it's because of an unexpected crisis – a disability, sudden illness or a job loss. It's a single mom who can't make ends meet. It's your neighbours who are working multiple part-time jobs but still can't get enough hours to make ends meet. It's parents who are struggling to pay the rent and put food on the table; waiting years on Ontario's affordable housing list along with over 165,000 other households.

A registered charity, Daily Bread is a distribution hub that provides food and support to 200 food programs across Toronto. Daily Bread's Holiday Drive started November 27 and ran until December 31 with goals of $2.5 million and a million pounds of food. The money and food that was raised during the Holiday Drive helped provide food for over 200 programs and to thousands of people who were struggling with hunger over the winter months.

Daily Bread also works towards long-term solutions to hunger and runs innovative programs to support people on low incomes including a community garden, food services training program for people experiencing barriers to employment.

Daily Bread also has an information and referral services program that trains member agencies to support food bank clients by connecting them to community resources. These are all critical issues that lead to empty cupboards, where intervention and support can mean someone gets back on their feet and out of the food bank.

From food banks and community food centres to women's shelters, drop-in programs or hostels, many of our member agencies are also doing far more than providing food. Most are multi-service agencies that run innovative programs supporting and empowering people on low incomes all while advocating for long-term solutions to poverty. But people can't wait for those solutions on an empty stomach, which is why in addition to working towards solutions, Daily Bread continues to collect and distribute millions of pounds of food for over 58,000 food hampers every month.

Most needed food items include: pasta, dried/canned beans or lentils, rice, canned fruit and vegetables, pasta and pasta sauce, peanut butter, canned fish/meat, oatmeal, baby formula/cereal and food as well as high fibre/low sugar cereal. Food donations can be dropped off at any local fire hall or participating grocery store.

Every dollar donated means Daily Bread can provide $5 worth of food. This holiday Daily Bread hopes to raise $2.5 million and 1 million pounds of food. The support of the community is crucial in allowing Daily Bread to continue to provide food to individuals all across Toronto so that they don't go to bed on an empty stomach.

In support of:

Daily Bread Food Bank

… from page 6

to be on the alert for anything that might be an immediate threat to life or risk of imminent fire. Once he's dealt with the more egregious issues, he then seeks help from other agencies and departments in order to encourage further harm reduction. He admits it takes time and patience, but gaining a suspected hoarder's trust is more effective in the long run.

Gaining a hoarder's trust does not mean turning a blind eye to serious hazards. Not only must property managers have a good understanding of the Fire Code, they must also understand limits of a resident's right to privacy as well as their duty to report safety threats. A six-alarm blaze at 200 Wellesley St E, Toronto on September 24, 2010 that required the evacuation of approximately 1700 tenants and injured 17 people, including 3 firemen, was linked to hoarding. A discarded cigarette ignited combustible materials on a cluttered balcony on the 24th floor and then proceeded to ignite heaps of combustible materials within the apartment. A class action suit resulted in Toronto Community Housing Corporation (TCHC) paying $4.85 million to more than 600 tenants who lost property and/or were injured in the fire. The class action suit alleged that TCHC and the building's former operator, Greenwin Property Management Inc, knew of the hoarding issues but had done nothing about them. The fire marshal's report also found that 19 units of the building were overcrowded with belongings.

In Canada, task forces dealing with hoarding are found in a number of provinces including Ontario, Alberta and British Columbia. There are more than 80 such hoarding coalitions in the US and communities in the United Kingdom and Australia are also taking proactive measures to deal with hoarding. How prevalent is hoarding? Although no definite statistics exist at this time, it is estimated that hoarding behaviour affects 3 to 6 % of the general population. A 2009 study in Australia found that hoarding was a factor in 24% of preventable fires in that country.

In Toronto, a program called SPIDER (Specialized Program for Interdivisional Enhanced Responsiveness) was launched last year in order to establish a coordinated effort to combat the dangerous effects of hoarding. In Durham Region, Ontario, the Durham Hoarding Project was officially launched in June 2013. This organization was spearheaded by fire services staff who were concerned about gaps in the region's ability to properly address the dangers of hoarding. It was felt that individually, agencies such as the SPCA, Durham Region Housing Services, Durham Regional Health Department, municipal law enforcement, and the Canadian Mental Health Association could not provide the full range of services needed to effectively deal with hoarding behaviours. It was believed that a coordinated plan that provides all appropriate services can better deal with the needs of people with the disorder and make communities in Durham safer and healthier.

A fire prevention officer confided in me that at the very least, property managers should develop relationships with fire prevention units in their area. Working together, the property manager will have more success in setting goals to make their properties safer. He confirmed to me that as far as effectively reducing the hazards associated with hoarding is concerned, 'It takes time, as well as a committed effort to develop a systematic approach to deal with these problems. Quick knee jerk reactions that include interventions to deal harshly with hoarders often only exacerbate problems. The property manager should make sure to seek professional help to deal with the hoarders mental state as well as the appropriate agencies to deal with physical risks.'

2014 ORIMS
Christmas Luncheon

I'd like to take this opportunity to thank everyone who attended our annual ORIMS Christmas Luncheon; the event was an incredible success! With your help we were able to donate $10,000 to the Daily Bread Food Bank, along with 200 pounds of non-perishable items. As Jackie Mutcheson once said, "It takes each of us to make a difference for all of us." What a great way to give back to the community.

We all know December can be a very busy time of the year. Despite the hustle and bustle of gearing up for the holidays, dealing the onset of flu season, and the fact that approximately 20 cm of snow fell overnight causing road closures and transit delays, we still managed a record attendance of over 700! On behalf of ORIMS, I would like to thank you for taking the time to spend the afternoon with us.

It was a great opportunity for me to organize this perennial event with many of today's industry leaders. I would like to thank our generous sponsors and companies who donated many amazing prizes for the raffle. Your continued support is greatly appreciated.

I would also like to thank all the members of the ORIMS Board of Directors, the staff at the Westin Harbour Hotel, all of the volunteers that helped make this event a great success and a special thanks to Nancy Lacroix for her assistance throughout everything. Follow this link to view video highlights of the afternoon.
http://youtu.be/5NotrEOM-2o

On behalf of the ORIMS Board, we wish you a happy, healthy and prosperous New Year!

James Eka, Director, Social Programs

Photos:
Courtesy of
Canadian
Underwriter
Magazine

Christmas Luncheon Contd.

ORIMS

ONTARIO RISK AND INSURANCE
MANAGEMENT SOCIETY

Have a Happy and Safe New Year!

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.