ARE YOU PENNY-PINCHING YOURSELF OUT OF BUSINESS?

FRAUD: EVERY BUSINESS IS AT RISK

WIN BY LOSING IN 2014

73rd ANNUAL CONVENTION REVIEW
The Crawford Solution℠

Comprehensive integrated claims services, business process outsourcing and consulting services for major product lines including:

- Property and casualty claims management,
- Workers compensation claims and medical management, and
- Legal settlement administration

Based in Atlanta, Georgia, Crawford & Company is the world’s largest independent provider of claims management solutions to the risk management and insurance industry as well as self-insured entities, with an expansive global network serving clients in more than 70 countries. The Company’s shares are traded on the NYSE under the symbols CRDA and CRDB. EOE
What’s Inside...

35 Widening Wealth Gap Is Biggest Global Risk, World Economic Forum Predicts
   Hilary Tuttle

36 Olympic Games Risk Management
   Katharine M. Nohr, J.D

41 Fraud: Every Business is at Risk
   Chuck Gallagher

42 The First Steps to Managing Cyber-Risk
   Thomas Dunbar

MANAGEMENT PERSPECTIVES
8 Are You Penny-Pinching Yourself Out of Business?
   Sean Castrina

NEW PERSPECTIVES
10 Personal Development
   Margaret Wildi

12 Win by Losing in 2014
   Geoffrey Tumlin

16 5 Risks You Must Take with Customers
   Tom Panaggio

18 Protecting Your “A” Factor: 16 Accountability Killers to Avoid
   Julie Miller and Brian Bedford

TECHNOLOGY TRENDS
22 Insurance and Cyber Security in a New Mobile Age
   Michael D. Croft

27 How Independent Insurance Professionals Can Help Their Clients Create Safer Workplaces
   Mark Hogle

28 Understanding Cyberterrorism
   Larisa Redins

30 Employees and Their Social Media
   Frank J. Saibert

ASSOCIATION NEWS
45 ISFA Insurance Scholarship Foundation of America

46 Welcome New Members

47 Congratulations New Designation Recipients

48 Meet the 2014-2015 Board of Directors

54 73rd Annual Convention Review

55 International Award Winners

58 The Last Line
Editor’s Note

Risky Business...

Risk is a part of our daily lives – there is no way to avoid it. We take risks each time we get in our cars, each time we board a plane – in truth, each time we leave our homes. But that doesn't prevent us from living our lives as normal. Although we strive to mitigate the risk in our lives and in the lives of those we love, the best we can do is to create an environment where we act responsibly and safely. In the same manner, as organizations endeavor to manage risk they seek to protect themselves without creating an interruption in business as usual.

In this issue of Today’s Insurance Professionals we learn about several examples of managing risk – not just directly as it applies to the insurance industry, but as it effects all of society in today’s world. We hear from the World Economic Forum and its predictions on societal, environmental, economic and technological risks. We take a look at the Olympic Games as a case study from the Risk Management professional’s approach, and focus on the power of Social Media and how it dramatically changes the risk dynamic. Fraud risk is a major risk that affects all organizations. In this issue we identify the key areas of focus for any company interested in identifying the warning signs of employees that are more likely to commit fraud.

As we advance technologically at an exponential rate, electronic data and the internet continue to evolve as an increasingly critical aspect of business activity. They can produce significant business efficiencies and growth opportunities, but also a range of particular risks that need to be understood and managed. We focus on the first steps to managing these specific risks that relate to the use of computers, information technology and virtual reality in our Cyber-Risk feature.

Included in the Association News of this issue are highlights from the successful and educational annual convention enjoyed by many in beautiful San Diego. Additionally, you will find updated profiles of the 2014-2015 Board of Directors, the International Award Winners, our new association members, and those who have successfully achieved the CLP, DAE and CIIP, CPIW, CPIM designations. Finally, don't forget to look for “The Last Line” – our newest addition to the magazine – for supplemental Association News submitted directly by our members.

We hope you enjoy this summer edition of Today’s Insurance Professionals magazine. And please don’t forget to stay connected with us on the IAIP Website; join the conversation on our LinkedIn and Facebook pages; and now you can also find us on our new Twitter account – just one more way we are...

…Connecting Members... Building Careers.

Betsey Blimline
Editor, Today’s Insurance Professionals Magazine
According to Wikipedia - Risk is ubiquitous in all areas of life and risk management is something that we all must do, whether we are managing a major organization or simply crossing the road. The ISO 31000 (2009) definition of risk is the ‘effect of uncertainty on objectives’. There are several strategies to manage risk including insurance.

As a member of Insurance Professionals you’ll find this issue of the magazine interesting on two levels:

• Articles discussing risk management
• Highlights of the 73rd IAIP Convention

Many of the articles featured in this issue correlate to topics presented at the convention, fraud, customer service, personal development and professional skill growth.

Life is constantly changing which brings new challenges and opportunities daily in everyone’s professional and personal life. Risk changes as well so it’s imperative that all involved in risk management continually strengthen their approach to the demands of their responsibilities. Learn everything you can from the articles in this issue to support your professional objectives.

Those attending the convention have tools to better “manage the risk” associated with their employment in the insurance industry. Career growth and association management highlighted the learning sessions at the convention along with industry trends and leadership enhancement. As keynotes at the convention pointed out - (Judson Laipply) Life is Change and (Jean Gatz) STANDOUT Leadership.

Congratulations to all of the IAIP award winners! See them on page 55!

As I come to the end of my term as IAIP President I want to thank each member for giving me the opportunity to lead this great association and for supporting the entire leadership in the direction we’re taking. We are definitely on the course to BIGGER - BROADER - BETTER as we continue...

Jane Densch
CPCU, AIC, ARE, ARP, AIS, CPIW
IAIP President 2013-2014
Hello to our 2014-2015 team members

Every one of you will be a member of our team. Without each of you this coming year we will not be a success. I consider our glass to be “half full”. Can you tell I am an optimist? Transition is on the horizon. We are moving forward to bigger, better and bolder things which will help to “Connect Members and Build Careers” for the future.

I am appointing each of you as a member of the Insurance Professional’s Growth Team. We need your help, input and expertise to accomplish some of our transition objectives for the future. Believe me when I say these are not short term fixes, they are long term goals. And, the majority of these will be geared toward our local association’s growth and retention. In order to thrive as an International Association we must build a culture, at the grass roots level, of encouragement and support for our locals. As a member of our team each of you are charged with participating in providing these elements for success wherever needed.

There will be more communication, at all levels, on a consistent basis so we all know who is doing what, and when. We must provide ideas and feedback on an ongoing basis in order to achieve our goals. Remember it has taken us 74 years to get to this point in our association. By working “smarter” not “harder” we will be able to continue on our path of providing the best education and networking in the insurance industry.

A Lakota Native American Proverb states “we shall be known by the tracks we leave.” Let’s make sure our tracks are progressive in nature but easy to follow for those members who shall come later. Show them the way to continue making great strides in an association where “belonging is good business” for our employers as well as our members.

I am so excited and looking forward to working with each and every one of you in the coming term.
Are You Penny Pinching Yourself Out of Business?

Five Expenses You Should Never, Ever Skimp On

If you’re a small business owner, it’s probably a vast understatement to say that you don’t have money to burn. But according to Sean C. Castrina, there are some areas in which it doesn’t pay to cut costs. Here, he outlines five areas in which you should never be cheap.

If you’re bootstrapping your own business, you know all about doing more with less. The ability to stretch a budget is a survival skill, especially in those cash-strapped early days. And because you know you’re never much more than a bad quarter or an unexpected expense away from closing your doors, you’re always looking for new ways to save money. But here’s the real question, says Sean C. Castrina: Are you being cheap about the wrong things?

If your goal is to cut costs at any cost, you’re heading into dangerous territory,” says Castrina, “And too many entrepreneurs don’t just wander into Cheapskateville—they set up shop there.

“Avoiding unnecessary expenses is one thing; becoming a fear-driven perpetual penny-pincher is another,” he adds. “Too many people can’t see the difference. And that’s too bad, because ‘cheapness’ can hurt the value of your product or service, or the efficiency of your business, both of which will drive customers away.”

Having started more than 15 companies in industries including direct mail, home services, property management, retail, and more, Castrina knows just how tough it is to write checks to employees, vendors, landlords, banks, etc. when your hopes, dreams, credit, and livelihood are at stake. Yet making those checks too skimpy can cost you big down the road.

“Subject every prospective cost-saving measure to this litmus test: What are the possible short- and long-term effects of this decision?” he advises. “Will it save my business money without negatively affecting profits? Sometimes, the answer is ‘no.'” Here, he takes a look at five penny-pinching sins that are costing your business:
PENNY-PINCHING SIN #1: Paying employees the bare minimum. Excessive tightfistedness on payday sends a very clear message to your employees: “I place a low value on you and what you do for my company. I don’t see you as a person with talents and unique abilities, but as a debit on my monthly expense report.” And that, Castrina points out, is the kind of message that sends skilled employees running for the hills, costing you money in lost productivity, turnover, and customer dissatisfaction.

“Yes, some low-skill positions can be filled by just about anyone and shouldn’t come with a high salary,” he comments. “But if you have experienced, efficient employees with a high level of expertise, you need to compensate them fairly. Quality employees can make or break your company. Ask yourself: Would I want this person working for the competition? If not, pay them well and keep them on your team indefinitely.”

PENNY-PINCHING SIN #2: Using an in-house bookkeeper. According to Castrina, too many small business owners do bookkeeping in-house. Why is that a problem? First, he says, many boss-designated bookkeepers don’t completely know what they’re doing. For instance, they may use unnecessarily broad headings or classify items incorrectly. Sooner or later, your accountant (or worse, the IRS) will charge you to correct these mistakes, saving you nothing.

“The larger problem, I’m sad to say, is that it’s easy for an in-house bookkeeper to steal from you,” Castrina says. “It’s happened to me and to many other small business owners. Now, I’m adamant about hiring a third-party bookkeeper who reports to me directly. I ask my staff to leave this contractor alone, just as they would an IRS auditor.”

PENNY-PINCHING SIN #3: Skimping on legal services. Castrina recalls going through a touchy legal matter several years ago. When he described the matter to an older business colleague, his colleague had this to say: “Your attorney is a nice guy, and he’s good with general matters, but for this situation you need a killer. You need someone whose name strikes fear into the heart of opposing counsel!”

“I took my colleague’s advice because I knew he’d been in my shoes,” Castrina says. “And I’m so glad I did! The matter went away quickly and was some of the best money I ever spent on higher-priced billable hours. For general matters, I like hiring young, new-to-their-firms attorneys whose rates are low and who are really trying to earn my business. But for matters in which your company’s survival is at stake, hire the best lawyer you possibly can.”

PENNY-PINCHING SIN #4: DIYing branded materials. “You have one chance to make a good first impression.” We’ve all heard this advice our entire lives, but too often, business owners forget it… often, to their detriment.

“We’ve all encountered a business that made a poor impression because their employees weren’t wearing uniforms or because their signage wasn’t professionally created…and don’t even get me started on forms, business cards, stationery, and websites made with ‘do it yourself’ kits!” Castrina says. “The fact is, customers are always going to judge businesses by their covers. So if you want to be paid like a great company, you need to look like one.”

PENNY-PINCHING SIN #5: Relying on word-of-mouth marketing. Have you ever heard of Budweiser? This, of course, is a ridiculous question. Everyone has heard of Budweiser. Among (many) other things, the company produces an endless stream of expensive, Hollywood-quality commercials just to remind consumers of the well-established fact that it sells beer. The point is, no matter how successful they are, great companies are always trying to communicate with and attract potential customers.

“If I hear one more small business owner tell me that he or she believes in ‘word-of-mouth marketing,’ I may scream!” Castrina comments. “Don’t get me wrong; customer referrals are very powerful and can really help drive your business. But I’ve never owned or worked with a company—even those with A+ BBB ratings—that owed more than a third of sales to word-of-mouth business. The fact of the matter is, if you try to save money by not budgeting for marketing, you’ll save your way right out of business. You simply must spend money to attract customers.”

“Here’s the bottom line: In business, you get what you pay for,” concludes Castrina. “If you try to skimp on something that affects the experience your company offers consumers or that compromises its ability to run efficiently, your efforts will probably backfire. As an entrepreneur, it’s good to be frugal…but it really doesn’t pay to be cheap.”

About the Author:
Sean C. Castrina is the author of 8 Unbreakable Rules for Business Start-Up Success and the soon-to-be-released 8 Unbreakable Rules for Small Business Dominance. He is also founder of newbizcoach.org. A successful business coach and a true entrepreneur, he has started over 15 successful companies over the last 18 years. His companies have ranged from retail, direct mail marketing, and advertising to real estate development and home services. Sean is a sought-after speaker and can speak with authority on what it takes to start, sustain, and grow a business.

About the Book:
Personal Development

While the 2014 Sochi Olympics are just a memory, think about the athletes, past and present, and the years of training, the successes and failures along the way and the drive they must have to achieve their dream of a gold medal. While Olympians are an elite group and many of us won’t achieve a Gold, Silver or Bronze Medal, we can still have dreams of being the “best” at whatever we do. While life really isn’t about gold medals, it is about knowing what you want in life and going after it. Mark Twain once said – “Twenty years from now you will be more disappointed by the things that you didn’t do than by the ones you did do.”

What is “personal development”? Some define it as both individual self-development and the development of others through various relationships that utilize courses, tools and other methods in the process. For others, personal development is about pursuing personal growth opportunities in all aspects of life – both at work and in their personal life. Personal development is just that – personal; and, each one of us will view it differently.

It’s important to take control of your personal development knowing that it’s not “once and done;” it’s a life-long process. Personal development is your responsibility; you have to own it. You must look for teachable moments every day. What can you learn and what can you take away and use immediately? What can you use in the future?

The next step is to create a plan for what it is you want to do or become. This is an individual process and your plan will not look like any others. Your plan will take time to develop so be patient with the process. Your plan can be as formal or informal as you like; and, it can be as broad as your vision for the future or focused on a specific skill you want to learn. Once you know what success means to you, it’s time to establish goals to achieve that success.

When setting goals, make them SMART goals – ones that are Specific – simplistically written and clearly define what you want to accomplish, Measurable – having tangible evidence that you have accomplished the goal, Attainable – a stretch so you feel challenged but defined well enough so that you can achieve them, Realistic – aligned with your key responsibilities or objectives, and Timely – including one or more target dates for completion. Achieving goals requires patience and persistence. Some may be achieved in a short period of time and others may take a lifetime.

If your goal is to become a more effective leader, what are you doing to achieve that goal? Are you reading articles about effective leaders? Is there a workshop or seminar you can attend that will give you new insights into leadership behaviors? What about courses at the local college or through IAIP? The Certified Leadership Program is an excellent resource for anyone who wants to hone their leadership skills. Remember that personal development goals are extremely important in leadership and management. Being an effective leader is not just about the skills you possess but the person you are and how you interact with your team, your peers, your family and business contacts.

If your goal involves increasing your level of professionalism and efficiency, have you reached out to a mentor who could provide guidance and support? Perhaps you want to teach others and help them improve their skills, earnings potential, or, self-esteem. Remember, we learn so much more about ourselves when we help others grow and learn.

Once you establish your goals, the next step is to put them in motion through your actions. Enroll in that class, sign up for that seminar, read that article or reach out to that mentor. Taking the first step is always difficult and can be scary at times. Remember that you own your personal development, and time spent working on your plan is critical to your success. Be patient and never give up. If your goal is to become an entrepreneur, then talk with other entrepreneurs. If you want to earn a college degree, take that first step and make an appointment with the college registrar. If you think you can’t do it, what’s standing in the way? Is someone or something keeping you from achieving your dream? Are you getting in your own way and making excuses for not achieving your dream?

“Twenty years from now you will be more disappointed by the things that you didn’t do than by the ones you did do.”

by: Margaret Wildi
IAIP Member and
Past International President

To begin, you need to conduct a self-evaluation, past and present, and identify your strengths and weaknesses. Benchmark your skills and determine if they’re relevant in today’s work environment. What skills or knowledge do you need to acquire or upgrade? You also need to review your priorities, values and ethics and determine if changes need to be made. Next, define success for yourself and then prepare your personal development plan.
We are always looking to others for inspiration and examples of who we want to become. Enlisting the help of peers, family members and friends can be critical to your success. However, don’t compete with others; compete with yourself. What can you do differently or better? Is there a course or seminar you can take that will help you be more successful in the future?

Your personal development can also help foster healthy relationships. As you grow and develop, your attitude changes for the better and your self-confidence is improved, which then leads to additional growth and development. Who doesn’t want to be around others who have positive attitudes and self-confidence? Employers notice those workers who have great attitudes and get things done. They reward those employees with additional, higher level responsibility, compensation and promotions. Even if you have no aspirations for a higher position, it’s important that you continue to learn and grow within your current position.

What can you do right now? Take a few minutes to perform that self-evaluation and determine your strengths and weaknesses and be very honest with yourself. Then, create a personal development plan including personal and professional goals. Seek the support and guidance of others to help you successfully reach your goals. Finally, keep your personal development plan front and center and review it often. Les Brown sums it up very nicely: “If you take responsibility for yourself you will develop a hunger to accomplish your dream.”

So, look for those teachable moments that are all around you. Don’t sit back and expect things to change because you want them to. You have to take an active role in your personal development, each and every day of your life. Remember – Do it for YOU!
WIN by Losing:

SHED BAD COMMUNICATION HABITS

The fastest and the best way to improve your communication is to stop doing things that repeatedly cause you trouble. Communication expert Geoffrey Tumlin identifies seven bad communication habits that are at the top of the quit list.

One or two bad communication habits can cause a lifetime of trouble. And with today’s quick and easy methods of communication, it’s all too easy for bad habits to work their way in. You overreact to an email—not for the first time—and send off a furious and damaging reply. Your spouse accuses you of not listening (again) and you have to sheepishly admit (again) that she’s right. You offend your “friends” or followers on a social media platform with yet another ill-advised attempt at humor. Or you can’t resist a snarky comeback to a difficult customer’s provocation, even though you immediately regret your words. When bad communication habits take over, the reputation you worked so hard to cultivate takes a beating.

“Bad communication habits are the punishment that keeps on giving,” says Tumlin, author of the new book Stop Talking, Start Communicating: Counterintuitive Secrets to Success in Business and in Life. “Even if you suffer from only one bad habit, it can recur in dozens of conversations and cause damage each time. But the good news is that by eliminating a single bad habit you can prevent many future problems. In fact, nothing else you can do gives you as much bang for your buck as eliminating a bad communication habit.”

That’s where Stop Talking, Start Communicating comes in. Full of counterintuitive yet concrete advice, it draws on Tumlin’s extensive experience as a communication consultant to show readers how to unload bad habits, improve conversations, and use today’s powerful digital devices, not to fragment attention and dilute relationships, but to achieve more of their most important goals and aspirations.

“This is the best time in human history to be a competent communicator,” Tumlin asserts. “It’s true that it can be incredibly difficult to break free of the bad habits associated with the distraction, expediency, self-expression, and excess that characterize so much of our digital-age communication. Yet if we are willing to cast off some of our bad communication habits, we can optimize opportunities to connect productively and meaningfully with other people.”

Here Tumlin shares seven of the most common bad communication habits. If any of the habits hit dangerously close to home, resolve to improve or eliminate them:

**Bad Habit #1:** Letting the Neanderthal pick your words. When we’re agitated, irritated, or frustrated, a battle plays out between our primitive, impulse-driven Neanderthal brain and our more modern, thoughtful, and deliberative brain. And while the Neanderthal parts of our brain are indispensable when we’re in physical danger, our Neanderthal brain is terrible at picking our words. Word selection is better left to our more analytical modern brain, because the Neanderthal prefers to club first and ask questions later.

The problem is that although words can build relationships only slowly, they can cause damage with lightning speed. A blurted retort, a thoughtless tweet, or a hasty remark can—and does—land people in hot water all the time. When the Neanderthal chooses our words, it never ends well.

“A simple but powerful way to improve your communication is to stop talking and think for a minute whenever you’re frustrated or upset,” Tumlin asserts.

“Don’t need to take a vow of silence, but you do need to pause long enough to keep your more thoughtful and deliberative brain in charge of selecting the words you’re going to express. Even a few seconds can help you to steer clear of the Neanderthal’s exhortations to club someone, can allow you to get in front of ill-advised words, and can provide you with the space you need to self-correct when you’re angry or upset.”

**Bad Habit #2:** Using authenticity as an excuse for bad behavior. “I was just being myself” sounds harmless, but it’s often an excuse to indulge in destructive behavior,” points out Tumlin. “Smart communicators realize that by focusing on what they want to accomplish instead of what they want to say, they keep their conversational goals in their rightful place—above their feelings in terms of priority.

“Authenticity sounds good in theory, but in practice it often torpedoes our goals,” says Tumlin. “I’m not suggesting that you become a fake, just that you don’t cloak momentarily gratifying, but counterproductive, communication in the fabric of ‘being yourself.’ Poor communication—when your words hijack your goals—isn’t a trait; it’s a choice.”

**Bad Habit #3:** Multitasking when we should be listening. The digital revolution facilitated hypercommunication and instant self-expression, but, ironically, made it harder for anyone to listen. There’s just too much communication junk getting in the way. (Just consider the frenetic activity happening on Twitter at any given moment!) Our thoughts are scattered, our minds wander, and ever-present distractions make it difficult for us to focus on the person right in front of us. Most of us need to make a concerted effort to reinvigorate our listening skills.

“Intentional listening will make you more present in conversations and will decisively improve your communication,” promises Tumlin. “The funny thing is that people are telling us all the time about what they want, what they fear, and what’s important to them, but we’re often too busy thinking about what’s in our inbox or who just texted us to absorb much of what they’re saying. The ‘old school’ behavior of listening will help you become a much better communicator and will enable you to become far more knowledgeable about the people in your life.”
Bad Habit #4: Asking faulty questions. Questions aren’t always neutral. They make some of your conversations better, but as you’ve probably noticed, many questions make a surprisingly large number of your conversations worse. Even “simple” inquiries can go awry. “Is your mother coming over for dinner again?” or “Did you call Jim in accounting about this?” can cause trouble if the other person thinks there’s a criticism behind the query.

“Some of your relationship problems probably reflect your undeveloped questioning skills,” says Tumlin. “Faulty questions contribute to many conversational failures and can add anxiety, defensiveness, and ill will to interactions. In general, the more you query simply to indulge your personal cravings to get an answer, to hammer home a point, or to satisfy a narrow personal interest, the more your questions are likely to stifle dialogue. It’s better to focus on what you can learn from or about another person and to ask questions that reflect a broad curiosity about the person or topic you’re discussing.”

Bad Habit #5: Meddling. Our quick, cheap, and easy digital devices allow us to have far too many unnecessary conversations, engage in way too much unnecessary collaboration, and get our hands (and thumbs) on too many irrelevant issues. That’s why smart communicators, like smart doctors, have a good triage system—its categories are Now, Delay, and Avoid—to focus on the most pressing issues, while delaying or ignoring less important matters.

“Problems in the Now category require an immediate, solution-based conversation,” explains Tumlin. “Don’t automatically assign too many issues to this category—this is the fundamental miscalculation your triage system is trying to correct. Delay is your default category. Many issues may disappear completely or resolve themselves without your intervention. Finally, avoid issues that reflect highly emotional, incredibly complicated, and other volatile feelings that reside deep inside another person unless they are impairing the accomplishment of critical work.”

Bad Habit #6: Fighting with difficult people. Jane talks too much. Jim is incredibly stubborn. Uncle Billy loves to argue. Your client is moody. Whether they’re controlling, critical, or cranky, the behaviors that make someone a difficult person tend to spark frequent confrontations—even though we’re unlikely to influence these people. For example, we wrestle with Jane to get a word in edgewise. We struggle to change Jim’s mind. We fire a barrage of points and counterpoints into Uncle Billy’s arguments. We try to offset our client’s mood swings. It’s time to quit trying, insists Tumlin.

“At the end of a conversation, the difficult person remains the same, but often you are in a weaker position,” Tumlin points out. “But giving up your desire to ‘win’ by imposing your will on the other person can realistically and consistently improve your communication with difficult people. When you find yourself with no choice but to interact with a difficult person, have modest expectations, avoid tangents, and stay focused on your end goal. It’s really all you can do.”

Bad Habit #7: Overreacting. We often use more force than needed to accomplish our objectives. We yell when a measured response would have worked better, send a blistering e-mail when a more restrained reply would have sufficed, and issue an ultimatum when a firm but gentle statement of convictions would have done the trick. But excessive force frequently causes a destructive cycle—attack, retaliation, escalated attack, and escalated retaliation, etc. No matter how justified we may feel, the bottom line is that using excessive force isn’t usually a winning strategy.

“Exercising restraint during a contentious interaction is challenging, but try to apply the least amount of interpersonal force and intensity necessary to accomplish your objective,” asserts Tumlin. “In other words, bring a stick to a knife fight in order to prevent a conversation from escalating dangerously. Try to stay serious and focused, don’t add any new emotional material, and keep the conversation as brief as possible. Be the calm, controlled, and stabilizing influence on a conversation that’s become heated so you can minimize the chance of permanent relational damage.”

“Let’s focus on shedding the bad communication habits that are coming between us and the most important people in our lives, because those bad habits prevent us from having the kinds of productive and meaningful interactions we desire,” concludes Tumlin. “Eliminating just one or two bad communication habits will dramatically improve your communication and strengthen your relationships.”

About the Author
Geoffrey Tumlin is the author of Stop Talking, Start Communicating: Counterintuitive Secrets to Success in Business and in Life. He is the founder and CEO of Mouthpeace Consulting LLC, a communication consulting company; president of On-Demand Leadership, a leadership development company; and founder and board chair of Critical Skills Nonprofit, a 501(c)(3) public charity dedicated to providing communication and leadership skills training to chronically underserved populations. Tumlin is a frequent guest on television and radio programs throughout North America, and his writing and ideas have been featured in hundreds of media outlets. You can learn more about Geoffrey Tumlin at www.tumlin.com, and you can reach him at geoff@tumlin.com.

About the Book
Imperial PFS, the leader in premium financing, continues to focus on the success of our agency partners.

We offer a broad range of services and programs provided through a nationwide network of local offices. Our experienced and long standing teams are focused on providing you the highest standards in customer service.
At State Auto we focus on our only means of distribution... the independent agent!

PaceSetter Program—exceptional training for your producers

Inner Circle—recognizing agency profitability and growth

Agency and CSR incentives—rewarding our best performers

Proud partner of the IAIP—If you’re interested in partnering with State Auto, please contact Terra Boroff at 614-917-5128 or email Terra.Boroff@StateAuto.com
Many business owners are risk-averse, and for good reason. However, if you want to be successful, Tom Panaggio says there are five risks you must take when it comes to building relationships with your customers.

Here’s one of business’s dirty little secrets: Many business owners prefer to keep their customers at arm’s length. They’re very careful to keep every interaction strictly professional, never getting overly personal or friendly. After all, if you get too chummy with customers—or even appear too interested in or sympathetic to their personal circumstances—they might start to want more from you: better pricing, extended credit, lengthier conversations, access to your services on nights and weekends, etc.

And then, of course, other business owners stay aloof from customers for a different, more instinctual reason: In a digital age dominated by email and computer screens, they simply don’t know how to interact with customers face-to-face and avoid doing so at all costs. “Both reasons for not getting close to customers can feel safe and self-preserving for business owners; however, they’re anything but,” says Tom Panaggio, author of the new book The Risk Advantage: Embracing the Entrepreneur’s Unexpected Edge. “Keeping customers at arm’s length inevitably erodes the connection between them and you, which, sooner or later, usually leads to the customer taking his or her business elsewhere. Nobody likes feeling unimportant, and with all of the choices out there today, customers don’t have to settle for it.”

Unless you’re running your business from underneath a rock, you know that losing a customer is a big deal because it has a significant impact on your organizational health. Besides the loss of potential future revenue, any sunk costs (costs you initially incur to gain the customer) are unrecoverable. Plus, there’s no telling how much damage negative word-of-mouth might do to your company’s future growth (or lack thereof).

“If you lose a customer due to price or other circumstances beyond your control, then fine,” Panaggio comments. “However, losing a customer because he or she felt unappreciated or underserved is inexcusable. It indicates serious flaws in your internal business processes that can lead to additional losses.”

Fortunately, Panaggio says, there are concrete things you can do to avoid “customer churn” — as long as you’re willing to face your unwillingness to invite them within arm’s length and accept the risk of getting closer to your customers. Here, he shares five specific risks you must take with your customers:

Risk getting personal. Many entrepreneurs use the phrase “It’s not personal; it’s business” to justify keeping their customers at arm’s length. But the truth is, especially if you’re at the head of a small business, every customer interaction is personal. If that makes you uncomfortable, relax. “Getting personal” doesn’t mean that you need to become your customers’ best friend—simply that you need to get engaged in their experience and show them that they matter, that you understand their needs. “When they work with you, your customers should feel like they are entering the bar on the television show Cheers: ‘where everybody knows your name, and they’re always glad you came,’” Panaggio explains. “Whether you want to admit it or not, customers can tell when you see them only as ways to boost the bottom line, and they don’t particularly like it.

“The good news is, showing customers that you value them on a personal level doesn’t have to be difficult,” he continues. “For example:

Communicate using face-to-face interaction whenever possible. Send thank-you notes—preferably handwritten ones—to show people that you value their business. And you can always take a cue from my favorite street hot dog vendor, whose most powerful marketing tool is his memory: He remembers each customer’s face along with their name and specific hot dog preferences.”

Risk keeping the lines of communication open. Yes, it’s true that customers aren’t always convenient. The phone often rings when you’re eyeball-deep in an important project. You can easily spend a half-hour answering a completely irrelevant question. Sometimes, you hear requests and complaints that make your life a lot more
complicated. But despite these risks, it’s crucial for you to make yourself available and keep the lines of communication open.

“If you want to retain your customers, you need to make it easy for them to get in touch, ask questions, and resolve issues, even if you’d rather be doing something else,” Panaggio confirms. “And to ensure that your process actually works, you’ll need to ‘stand in your own line’; in other words, look at the way you do business from the customer’s perspective. For instance: Does the customer have to navigate a confusing labyrinth of phone options to talk to you? Do you wait days before responding to emails? You may think that everything’s fine because you and the customer do eventually connect, but the customer may have a different perspective. Remember, communication has to happen on the customer’s terms, not yours, if they are going to remain happy.”

**Risk staying close (but not too close).** Before technology made it possible for people to connect with each other anytime and anywhere, customer-business interaction was limited to phone calls and in-person visits. This made it relatively easy for entrepreneurs to stay aloof. Today, though, technology has changed that model. Businesses that don’t use email, have websites, and invite customers to become social media “fans” are seen as very old fashioned and probably won’t keep their doors open for long. To remain relevant, entrepreneurs must use technology to stay close—but not too close.

“This can be a tough balancing act,” Panaggio admits. “Customers are sensitive about who has their personal information—such as email addresses, purchase history, and preferences—as well as how it’s used. When you embrace the risk of getting close, you must commit to using personal information to draw customers closer, not drive them away. Nobody wants an email inbox clogged with general promotional emails, for example, or a Facebook newsfeed dominated by gratuitous updates to your company’s page…much less a breach in personal privacy!

“You’d be much better served to use what you know about your customers to create highly targeted and personalized direct marketing campaigns,” he explains. “For instance, an automotive dealership might use customers’ purchase history, service records, and scheduled maintenance recommendations to create emails designed for specific recipients based on the year, make, and model of their automobile. And good news: This tailored approach is vastly more effective than general media campaigns, too!”

**Risk stepping out from behind technology.** Today, many small businesses that wouldn’t be able to exist without technology are thriving. However, some entrepreneurs are indulging in too much of a good thing by hiding behind technology—whether they mean to or not.

“Technology can streamline and improve, but it can also serve as a barrier,” comments Panaggio. “Before incorporating a new tool, device, or program into your business, ask yourself what its effect will be. If it improves the customer’s experience, it’s worth adapting. But if it makes only your own life easier, tread cautiously. Sure, you may love that your website’s new ‘leave a comment’ feature means that you can review customer feedback at your own leisure, but your customers may be increasingly frustrated by the fact that you don’t feel the need to pick up the phone as often!

“In many instances, a blend of old and new will be most effective,” he comments. “For example: Sure, you can use email to send files to a client—it’s more convenient for everyone than regular mail! But don’t include a long, convoluted explanation in the email. Call the client and talk him through the documents in real time so he can ask questions and you can correct misconceptions.”

**Risk going above and beyond.** When many business owners hear the phrase “going above and beyond for a client,” what they really hear is “spend more time, resources, and effort—but get paid the same.” That’s a bad way to look at taking good care of your customers, says Panaggio. In fact, when you don’t risk doing more than you absolutely have to, you’re hurting your company’s future prospects.

“In today’s competitive global economy, you absolutely must provide enough value to keep customers loyal over the long term,” Panaggio comments. “The days of being the only [insert your type of business here] in town are over. Customers have many choices, and if they aren’t more than satisfied, they’ll take their business to the competition.”

He adds: “All that you have to do is exceed your customers’ expectations, not by a huge margin, but just enough so that they’re pleasantly surprised. That’s where word-of-mouth advertising begins. When you hit that point, there’s a multiplier effect to the investment you make to secure the customer. Remember, a client’s real value is not the revenue made from their first order, but the total long-term value. The cost of acquiring a customer can be significant, but the cost of losing one—as well as all of the business that person might have brought to you—is greater.”

“Customers require consistent care and investment,” Panaggio concludes. “You can’t keep yourself separate from them if you want to be successful. So take the risk. Draw your customers closer. Invest in them. Make an effort to understand how they think and what they want and keep in consistent contact. Trust me: Getting personal is worth it.”

**About the Author:**

Tom has enjoyed a 30-year entrepreneurial career as cofounder of two successful direct marketing companies. As a result, he can give a true perspective on starting and running a small business. His practical approach to business concepts and leadership is grounded in the belief that success is the result of a commitment to embracing risk as a way to ensure opportunity. Today Tom lives in Tampa with his wife, Shemi. When he’s not speaking or advising entrepreneurs and small businesses, he’s spending time with his family—his three daughters, Ashley, Christine, and Elizabeth, are all pursuing their college degrees—or he’s out on a racetrack. For more information, please visit www.TheRiskAdvantage.com.

**About the Book:**

Protecting Your “A” Factor: 16 Accountability Killers to Avoid

by: Julie Miller & Brian Bedford

It’s easy to assume that you’re an accountable person if you don’t tell outrageous lies and generally follow through on your commitments. But Julie Miller and Brian Bedford say that even small lapses can affect the way others see you. Here, they list 16 common “accountability killers” you might otherwise be tempted to overlook.

Are you accountable? If you’re like most people, your answer to that question is an automatic “Yes” or maybe even an indignant “Of course, why are you even asking me?” After all, you don’t believe that you’re above the law or lie about your behavior like Toronto Mayor Rob Ford. And you’re no Anthony Weiner (Or is that Carlos Danger?), either: You don’t move heaven and earth to shift the blame when you’re clearly the one at fault. And you’re not like Sarah, your reliably unreliable coworker, who is chronically late and always full of convenient excuses.

But are you truly in the clear? Probably not, say Julie Miller and Brian Bedford. They contend that most of us are guilty of small behaviors that crack our accountability façade and hurt us, both personally and professionally, far more than we realize.

We know from the Lance Armstrongs, Jerry Sandusky’s, and Bernie Madoffs of the world what accountability absolutely isn’t,” notes Miller, coauthor along with Bedford of Culture Without Accountability—WTF? What’s the Fix? “But rarely do we stop to examine what accountability is in action. That’s why it’s so easy for little behaviors—‘accountability killers,’ if you will—to worm their way unnoticed into our lives.”

“Often, we’re critical of these behaviors when we see them displayed by other people, but we give ourselves a pass when we’re the ones engaging in them,” comments Bedford. “We tell ourselves, It’s just a one-time thing…It doesn’t usually act like this. But that just doesn’t hold water. No matter how often it does or doesn’t happen, failing to act accountable can damage your reputation, your relationships, your career opportunities, and more.”

In Culture Without Accountability—WTF?

What’s the Fix?, Miller and Bedford examine what can happen when businesses, teams, families, and individuals shirk accountability. The book is full of real-life stories of what accountability looks like and what can go wrong in its absence. It offers a proven process for installing an accountability-based culture, a platform for success in business and in everyday life.

Here, in no particular order, the authors share a list of their personal pet-peeve “accountability killers”:

Showing up late. Sure, there are legitimate reasons why even the most responsible person might be running late: a fender bender, a sick child, an unfortunate coffee spill, to name just a few. And yes, everybody gets a pass on this one from time to time when life’s curveballs happen. But if it happens again and again, you’ve got a problem.

“If tardiness is a habit—if others expect it from you rather than being surprised by it—you’re not being accountable,” says Miller. “In effect, what you’re saying is, ‘I don’t value your time. I believe I’m more important than you’—or at the very least, ‘It’s not important to me to honor the agreement we made.’”

Saying you’ll do it…and then not doing it. Again, sometimes “life” happens. If an unforeseen accident or crisis derails your best intentions, most folks are likely to understand. But if you fail to meet your commitments more than once or twice, you lack accountability. “If you find yourself constantly making excuses, asking for more time, or expecting others to understand why you ‘just didn’t get around to it,’ it’s time to make a change,” comments Bedford. “Either start pushing yourself harder or stop making promises you can’t keep.”

Being offended by the truth. When someone calls you out—for dropping the ball, for behaving badly, etc.—how do you react? “If you’re indignant or offended instead of accepting that
the other person has made a valid observation, you’ve just killed your accountability,” points out Miller. “Denying or just having a bad attitude about what’s obviously true will cause your credibility and trustworthiness to take a significant hit.”

Covering up mistakes. The fact that others don’t know about a slip-up doesn’t mean it didn’t happen. “If nothing else, your accountability will suffer in your own eyes,” asserts Bedford. “You also run the risk of setting a bad precedent for yourself. The next time something comes up, you’ll think, ‘Well, last time this happened I just shredded the document, or, I’ll just delete the customer’s email again. No one noticed before.’

“Do this sort of thing enough times and the tendency to cover up becomes a habit,” he adds. “You get away with it so you start to think it’s okay. But if your actions do come to light, your public reputation will take two hits: one for the original mistake and one for trying to hide it.”

Blaming others. The so-called “blame game” is one in which nobody wins—at least of all the person pointing the finger. Even if the fault lies with someone else, says Miller, part of being an accountable person means doing your best to offer solutions in addition to pointing out problems. And if the blame does lie with you, it’s dishonest and reprehensible to attempt to shift it to someone else. “Always own up to your mistakes,” she instructs. “And keep in mind that you’re still participating in the blame game, albeit passively, by keeping your mouth shut when you’ve acted wrongly. Even if you experience unpleasant short-term consequences, you’ll build an overall reputation for integrity when you ‘fess up’ to your mistakes.”

Asking others to cover for you. “I have to get into the nitty-gritty details of why? you ask. “Well, yes,” responds Bedford. “Acknowledging that the fault was yours is the first step—but only the first step. If you don’t truthfully explain why you acted as you did, others might still question your motivation, judgment, etc. You may still be viewed as lacking accountability.”

…or trying to justify it with a bad one. There are a lot of adult versions of “The dog ate my homework.” But usually, our peers can see through them. “You don’t do yourself any favors when you try to talk yourself out of taking responsibility,” points out Miller. “It just makes you seem as though you believe you are above the law.”

Ignoring others’ bad behavior. Remember that time when one of your peers was throwing his weight around and bullying one of his employees? Not wanting to get involved in the drama, you took the “none of my business” approach to dealing with the problem. You chose not to speak up about the guy’s bad behavior to keep yourself out of the line of fire.

“Here’s a reality check,” says Bedford. “Ignoring someone else’s bad behavior is just as bad as committing the act yourself. When people see you ignoring these problems, especially when you’re in a position to do something about them, they think you’re approving the bad behavior. They assume you’re the same kind of person as the manager yelling at his employees. Don’t be guilty by association. Speak up and show that you value fairness and respect.”

Communicating in an immature manner. Gossiping at the water cooler. Sniping at your spouse instead of having a mature discussion. Making jokes at your brother’s expense. Giving a friend the silent treatment without explaining why. Making faces behind the boss’s back. The secretive nature of such communications is what makes them immature—after all, adults confront problems head-on—and indulging in it really eats away at your accountability.

“Always strive to be honest and upfront,” advises Miller. “At best, immature communication fails to produce useful results. And much more often, it causes others’ opinion of your character to drop.”

Failing to take—or give—feedback. When you can’t or won’t take feedback, you communicate to others that you aren’t interested in improving your performance. That’s pretty obvious. But there are also accountability implications associated with being unwilling to give feedback—it shows that you’re concerned with only your piece of the puzzle instead of the big picture.

“If you sit back and hope that someone else talks to the team member who’s bringing the whole project down, for instance, you’ve forfeited your right to complain when the finished product fails to meet expectations,” says Bedford. “The same thing goes for complaining about a decision after failing to offer your thoughts and insights while it was being made.”

Expecting an “A” for effort. Accountability isn’t about following orders. It’s about meeting expectations. If you ever find yourself using the “I did what you said!” excuse, know that you’re killing your accountability. “Expecting to be praised for doing what you were told to do even though the end result completely misses the mark won’t win you many friends in your professional or personal life,” says Miller. “You have the responsibility to speak up when you know or suspect that something isn’t right or won’t end up meeting expectations.”
NP NEW PERSPECTIVES

happen to you really aren't your fault. You couldn't have foreseen the fact that last night's storm would cause a tree limb to fall on your car. You didn't cause the economy to wreak havoc on your retirement account. And you certainly didn't intend to catch that nasty flu. But guess what? The way you choose to handle these situations can still add to or detract from your accountability.

"If you didn't grumble, gripe, and complain sometimes, you wouldn't be human," admits Miller. "But after you've vented your feelings, do what you can to find a solution and move forward. You can either be known as a problem tackler or a problem wallower—the choice is yours. I recommend choosing the former, which shows resilience and maturity.

Let others see that you're willing to take responsibility, even when a problem wasn't your fault."

**Having a “me-first” attitude.** During a night out, Bob zips into the last parking space at a crowded restaurant, conveniently “not noticing” that another driver had been waiting on it. After the meal, he sees that he was undercharged, but decides to simply consider the appetizer that didn't make it onto the bill a windfall. On the way home, Bob encounters a car trying to merge onto the freeway, but speeds up instead of letting the other driver into his lane.

“Yes, Bob sounds like quite a jerk,” acknowledges Bedford. “But the truth is, most of us have been Bob at one point or another. Having a ‘me-first’ attitude, especially when it means hurting or willfully inconveniencing someone else, hurts your accountability, because you're showing yourself to be inconsiderate, selfish, and maybe even dishonest.”

“If you want to build genuine, lasting success in any aspect of your life, you need to be someone whom others can trust,” concludes Miller. “Anytime you give another person a reason to question your honesty, your dependability, your intentions, or your values, you'll incur consequences. The good news is, most ‘accountability killers’—as well as their ramifications—are preventable if you're willing to look closely and honestly at your own behaviors.”

**Forcing others to remind you to act.** A colleague sends you several emails prompting you for the feedback you promised. Your spouse is constantly asking when you'll fix the leaky faucet you said you'd take care of. A friend sheepishly reminds you that you owe her money for several meals she covered. Every other day, your boss has to tell you to act as though serving customers is a privilege, not a chore.

“Whenever you force someone else to remind you of an obligation you're fully aware of, you're springing a leak in your accountability account,” Bedford explains.

**Being a victim instead of a solution finder.** Sometimes, the bad things that happen to you really aren't your fault. You couldn't have foreseen the fact that last night's storm would cause a tree limb to fall on your car. You didn't cause the economy to wreak havoc on your retirement account. And you certainly didn't intend to catch that nasty flu. But guess what? The way you choose to handle these situations can still add to or detract from your accountability.

“If you didn't grumble, gripe, and complain sometimes, you wouldn't be human,” admits Miller. “But after you've vented your feelings, do what you can to find a solution and move forward. You can either be known as a problem tackler or a problem wallower—the choice is yours. I recommend choosing the former, which shows resilience and maturity.

Let others see that you're willing to take responsibility, even when a problem wasn't your fault.”

**About the Authors**

In 2001, drawing on their respective years of experience in senior global leadership at Motorola, Julie Miller and Brian Bedford joined forces to establish MillerBedford Executive Solutions. MillerBedford helps businesses and organizations improve strategy, culture, and leadership, while addressing issues that limit success. And their clients actually have fun in the process! For more information, please visit www.millerbedford.com.

**About the Book**

The McGowan Companies (TMC) is built on three generations of dedication to the insurance and financial services industry. TMC consists of the following:

McGowan Program Administrators (MPA) is a Managing General Underwriter and Program Manager for highly-specialized programs of insurance.
Fairview Park, OH • mcgowanprograms.com • 440.333.6300

McGowan Excess & Casualty (MEC) is a Managing General Underwriter that specializes in Umbrella and Excess Liability products for a broad range of types and sizes.
Eatontown, NJ • mcgowanexcess.com • 732.335.8470

McGowan, Donnelly & Oberheu, LLC (MDO) is a Wholesale Insurance Broker specializing in the placement of Professional and Management Liability risks.
Austin, TX • mdoinsurance.com • 512.600.2280
In the insurance sector, customers use mobile technology to retrieve online quotes, update policies, file claims, and document loss events. As mobility becomes a part of everyday life, including in the workplace, mobile devices become a new target for security breaches. Since insurance companies have a tremendous amount of personal information on their policyholders, security becomes even more of a concern. While a credit card can be cancelled, customer addresses, vehicle information, social security numbers, life insurance policy details and other private information managed by insurance companies constitute a more permanent customer profile. If a company does not offer secure mobile applications, customers put themselves at risk every time they access their own information.

Customers are not the only mobile users inviting risk into your business. Your employees are also mobile savvy and may be embracing BYOD (Bring Your Own Device), which allows them to use their own mobile devices to be more productive in the workplace. Insurance providers are even starting to implement proprietary “app stores” for employees to access key applications that can be run on their mobile devices, allowing them to execute company tasks from the comfort of their own personal computers, tablets, and smartphones. BYOD saves your insurance company money by alleviating the need to purchase additional equipment, and it saves your company time by reducing training as your staff is already familiar with their personal mobile devices. However, BYOD can also promote lax or inconsistent security measures which can leave your company open to security breaches.

With all the fraud, corporate deceit, and identity theft that has been made public in recent years, customers want assurance that the companies holding their information are doing so with proper security and ethical protocols. Employees and customers also want more transparency to ensure they are spending their time and efforts with the right company. Transparency is gained by allowing more access to company data and removing layers of misdirection. In terms of technology use, this could involve access to certain audit reports, financials, and transaction history. It can also mean being more self-sufficient by using new technology to manage tasks that were once only executed by internal staff. Most importantly, employees and customers want to feel secure in knowing that sensitive information that can be linked back to them is under lock and key and impenetrable by an outside party.

While all this technology allows you to provide added convenience to your customers, generate new revenue streams from targeted marketing campaigns, and increase efficiency using BYOD, the associated risks must also be considered. Target’s recent credit card security breach affected more than 70 million customers and was an eye-opening experience to
consumers and employees alike. Data breaches like the one Target suffered highlight that there is no easy answer when it comes to securing data. The Target data theft ranks as the second largest credit card breach in the U.S., after the TJX Companies’ announcement that approximately 45.6 million credit and debit users were exposed to fraud in 2007. It was later revealed in court filings that the number of affected customers may have been more than 90 million (D’Innocenzio, 2014). Experts believe hackers stole credit card data from shoppers at TJ Maxx and Marshalls during the POS (Point of Sale) transaction, but this is not the only time that customer information is at risk. Even well after submitting social security numbers, addresses, and other personal information to an insurance company, hackers can still gain access.

Insurance companies can maintain the confidence of their policyholders and employees by taking certain steps that ensure personal information is protected, while providing the transparency that has come to be expected. Doing so involves assessing the company’s risk to security breaches and cyber-attacks. Safeguards can then be implemented to minimize the chance of these types of events becoming a reality. If an event does occur that increases a threat to information security, or results in a loss, there are measures that can help you to take back control.

**Reward & Risks Associated with New Technologies**

As touched upon previously, mobile technology offers numerous benefits to corporations. When properly used, mobile technology can help increase sales, create happier and more loyal customers, and lead to more efficient and effective employee behavior. In the insurance sector, increased sales come from simple quoting applications and incentivized targeted promotions. Customers are happier because they feel a sense of convenience and control over their insurance options. They can take matters into their own hands and receive immediate results, such as mobile policy binding, real-time policy updates, and digital ID cards and rewards programs. Employees grow more efficient by leveraging their own mobile devices to complete work tasks from any location, including their home.

Although new technology is making information more accessible and more easily shared, it also allows more opportunities for attacks and security breaches. Laptops, smartphones and tablets allow businesses to collaborate and share information anytime and from just about any location. When information is so openly shared within an organization, the opportunities for breach of this data could increase.

Statistics show the number of publicized hacks, cyber-attacks and data breaches continue to rise, with the majority of attacks coming from people outside the breached corporation. According to Verizon’s 2013 Data Breach Report, 92 percent of breaches in 2012 were perpetrated by outsiders, and 76 percent of network intrusions exploited weak or stolen credentials. When obtained by untrusted individuals, your customers’ information is compromised, which can have financial implications for policyholders as well as pose a threat to their physical safety. Many security breaches occur when stolen computer devices that contain alarming amounts of private information deliver data into the wrong hands. It is all too easy to have a mobile smartphone or tablet stolen from an employee’s desk, locker rooms, vehicles, and anywhere else people use mobile devices – which is just about everywhere.

In a New Mobile Era, How Can You Protect Your Insurance Assets?

There are ways to help prevent a breach or to minimize damage if one occurs. Yet surprisingly few insurance agencies have taken steps to insure themselves against mobile security breaches. Recent surveys show that only a quarter of midsize insurers have implemented some type of mobile device security for employees. Novarica, an agency providing market and technology information for insurance administrators, conducted a survey which included 22 large insurers and 64 midsize insurers. It concluded that companies must act to protect themselves. “We strongly recommend that all insurers carefully consider their security provisions for BYOD and consider the benefits of using an MDM [mobile device management] platform if they are not already doing so,” urged the analyst firm (Golia, 2013). They stressed the benefits of MDM techniques, which track lost devices and provide remote-wipe capabilities, as well as other strategies. Here are some areas of research we recommend you explore to help protect your insurance assets in a mobile world:

**START SIMPLE**

One of the first places to start might also be the simplest to manage: physical theft of mobile devices. Train your staff to be aware of the sensitive information that can be extracted from a smartphone or tablet. Urge them to take simple precautions to prevent theft. Too often employees leave their mobile devices on their desks, in conference rooms, or in the cafeteria for an easy steal. Advise your employees to wear a belt-clip or a carry bag. This may not make the hippest fashion statement, but it can help employees keep track of their mobile devices and may deter loss or theft. Install tracking software on mobile devices so that locating them is possible if they go missing. You can also install cameras throughout your company premises to monitor activity. There are several ways to ensure that information will stay secure even if a mobile device falls into the wrong hands. Always password-protect mobile devices with strong authentication credentials and never store passwords on a computer or mobile device. Install remote-wipe software that enables you to delete information if a device has been stolen. Do not keep sensitive information on any mobile device. Store such information in the Cloud or on private secure servers in a company network. Tie any work related applications or data to a virtual private network (VPN) and require strong authentication that forces changes every thirty days or less.

These simple steps will help keep hardware and information safe. Next, we will discuss options for monitoring and securing employees’ access to information.

**BYOD, MAM & MDM - Managing the Alphabet Soup**

Mobile application management and mobile device management solutions are newer options for securing mobile technology in a BYOD work environment. Mobile application management solutions wrap mobile applications in a secure container that is managed by your insurance company. A team of security experts is assigned to manage the MAM solution and keep track of any malicious activity or possible threats. The MAM solution will require strong authentication from the employee before they can access company information through mobile applications on their device. Once access is allowed, all communication to and from the mobile device and company network is tracked and encrypted. Each application that is loaded on the mobile device is assigned a company profile and a security wrapper. This means that when the same application is installed on another device, such as a tablet, that iteration of the application is also wrapped
in a security container and tracked against the employee’s profile.

Mobile device management tracks the physical device. GPS technology can identify the physical location of the mobile device and also allows remote-wipe capability. MDM provides an ID unique to the device and allows the company to keep a watchful eye on the whereabouts of its sensitive information.

CLOUD DATA
If none of your sensitive insurance information is kept on a mobile device, then the loss or theft of that mobile device poses no significant threat. Sensitive information should be kept on a secure server or in a Cloud environment when applicable. This information would be accessed only via secure authentication measures, such as SSL and two or three-factor authentication security processes. The information on the server would be encrypted using hash algorithms and various methods such as MD5, MD6 or AES, among others. Many of these encryption methods are probably already taking place in your insurance company.

One of the last remaining security concerns, then, is the wireless communication to and from the mobile devices. How secure are the wireless signals sent through the air to retrieve sensitive information?

WIRELESS TRANSMISSION SECURITY
Wi-Fi (Wireless Fidelity) handles transmission of wireless specifications for managing packet traffic for users over a wireless network. A wireless network uses signals such as light or radio waves to provide connection among the different devices, including laptops, smartphones, and tablets. These waves travel in many directions and are typically controlled by directional antennae, which focus waves in tight beams and limit the area a hacker can access a transmission. If these transmissions are not encrypted, stealing information becomes relatively simple.

Therefore, encrypting transmissions is a paramount effort that must be taken seriously by network administrators of insurance companies. Gateways and firewalls must also be put in place at key intersection points. These measures alone do not mitigate attacks, but they can minimize them.

There are other types of attacks that do not only deal with encryption challenges, but which also require advanced monitoring solutions. (One example would be a DOS (Denial of Service) attack, which results in the network being inaccessible by intended users.) Cryptography is an evolving form of mobile security, and algorithms and encryption methods are changing daily. Ensure that you are on a secure network when sending and receiving private information and that you are using a secure method such as HTTPS and SSL.

Beyond securing the connections and transmissions, your insurance company can create secure partitions that separate personal and business mobile usage. Personal usage can be blocked in a private corporate network, so that only secure and approved business applications would be allowed via authentication headers when accessed via a secure corporate network. When the user of the mobile device is outside the business network, the business applications would be disabled and the personal partition would be re-enabled. There are other permutations of this concept that can be adapted to fit your particular operational needs. For example; your claims representatives would need access to business applications when onsite at a loss event or a policyholder’s location. In this instance, the aforementioned configuration would not work. However, you can arrange things so that the business functions (possibly implemented as an SOA – service oriented architecture) can be accessed by a public network but filtered when an authentication request is received. This would allow your field workers to use the business applications in a “public” network and then, after authenticating, tunnel the requests through a virtual private network (VPN).
REMEMBER THE BASICS
In any case, these are the basic principles that should guide your decisions regarding mobile security:

Secure systems with hardware/software protection. By protecting your devices, you can respond immediately to intrusions and keep logs of activity to detect unusual events and trigger real-time action measures.

Create a strong security policy. Train employees against opening attachments or responding to messages from unknown sources. Apply filters to screen out suspicious messages and ensure that security precautions are being followed within your organization.

Back up Critical Information. Every organization should have a system for backing up their critical documents and data in case an emergency occurs. A backup plan is a way of controlling risk. Whether you work for a small insurance company or a large insurance corporation, you should have a backup plan in place.

Be proactive. Keep software and security management solutions up to date. Set firewalls and perform security audits regularly. Most importantly, keep abreast of the latest information related to threats and incidents within the insurance industry. By always staying aware of cyber terrorism and how it can affect your business, you will know how best to prepare yourself and reduce the chance of terrorist threats to your business.

Understanding Cyber Security Insurance
In response to a rise in data security losses, more companies have begun to seek cyber security insurance coverage. According to the official website of the Department of Homeland Security, cyber security insurance is designed to “mitigate losses from a variety of cyber incidents, including data breaches, network damage, and cyber extortion.” Companies are urged to adopt preventative measures against cyber-attacks and obtain protection through the purchase of cyber security insurance in the event that loss does occur. Although there are cyber security regulations strongly supported by federal and state government, procurement of cyber security insurance remains in the private sector. Comprehensive coverage plans may include cyber extortion, cyber terrorism, and breaches of privacy, administrative or operational mistakes, and numerous other digital liability exposures. Insurance policy coverage can vary, so it is important to be aware of the level of first-party and third-party coverage your company needs.

The federal government has also put in place a safety net of their own in response to terrorist activity. The Terrorism Risk Insurance Act (TRIA), administered by the U.S. Treasury Department, has set up a backstop intended to protect insurers in the event that an act of terrorism results in losses totaling over $100 million. It is not quite clear for insurance industry officials whether cyber terrorism is covered by the program. However, since terrorism tactics have evolved since TRIA came into being, some are arguing that cyber terrorism should now be acknowledged under the act.

Companies from all industries are turning to cyber security insurance in order to protect themselves, their employees, and their clients. In particular, the insurance industry has a naturally vested interest in promoting greater security to businesses. Insurance companies must put the right security measures in place to protect their digital assets and sensitive customer information. This can be achieved by being proactive and using some of the security techniques discussed above, such as cloud storage, and MAM and MDM solutions.

The Future of Cyber Security in Mobile Technology – Biometric Authentication
Biometric authentication marks a new era of security protocols. Authentication measures, such as fingerprints, retina scans, and even more advanced bio-authentication techniques are starting to make their way into our mobile world. Biometric authentication removes the typical user ID and password combination security credentials and replaces these with unique human characteristics that are difficult to counterfeit.

It is hard to say exactly where the insurance industry is headed with regard to mobility, since consumer demands largely inspire and influence organization changes. However, we do not need to know the future of insurance in order to take the necessary precautions to protect ourselves and our customers. We must consider mobile security and practice what we preach by doing exactly what the insurance industry exists to do: identify threats, secure ourselves against potential losses, and be prepared to act when damages occur.

About the author
Michael D. Croft has over 15 years professional experience in the computer science and technology industry. He is Founder and CEO of eSavV Technologies, a company specializing in new web, mobile, and cloud software. The software solutions have been topics of discussion for local business magazines, the World Economic Forum, TEDx, conferences, and various press. Michael has been a speaker at BOSCON, RI Business Quarterly, Positive Business Radio and academic institutions. In 2012, he earned the 40 Under Forty award, which cites 40 professionals under the age of 40 who are making an impact on a local or national scale. He is a member of the Chief Executives Club of RI and Boston, and is a technology advisor to United Nations renewable energy affiliate, IREO. To learn more about Michael and eSavV, visit http://www.eSavVcom, call (401) 305-3420, or email operations@eSavV.com.

Works Cited


Strategic solutions designed to fit your business insurance needs

Local team, national resources, customized services

At Wells Fargo Insurance, we focus on building long-term relationships with our customers. Our clients have a local team backed by the national strength, resources, and tools of Wells Fargo Insurance. This local support, combined with Wells Fargo Insurance’s strategic approach to risk management, property and casualty, and benefits, means we can support your business now and for many years to come.

Team up with us today.
Wells Fargo Insurance Services USA, Inc.

wellsfargo.com/wfis
How Independent Insurance Professionals Can Help Their Clients Create Safer Workplaces

It is widely believed that employees are a company’s most valuable assets. Yet in meeting customer demands and managing unpredictable daily operations, many businesses overlook the importance of having a thoughtful risk management and workplace safety program in place to protect their employees. This is where independent insurance professionals can help their clients promote a culture of safety by providing recommendations to improve workplace safety initiatives.

At its core, workplace safety is about establishing a culture where employers actively care about their employees and, in return, employees take greater responsibility for their own safety and the safety of others. It’s about doing the right thing and protecting the people who are integral to the long-term success of an organization. Successful workplace safety programs instill safety as a value, integrate it as a core business function, and target prevention as the primary means of reducing the frequency and severity of potential accidents. Moreover, establishing a culture that promotes workplace safety can lower workers’ compensation costs and result in a more productive work environment.

Relevant, Local Impact
As policyholders look to their insurance professionals as trusted advisors, it is important that agents and industry professionals keep current on legislative reforms affecting workers’ compensation insurance and related compliance changes that could impact their customers. For example, in 2013 legislation commonly referred to as “The Oklahoma Option” was signed into law, with plans that went into effect in early 2014. The reforms were designed to give Oklahoma’s businesses more choices and help control workers’ compensation costs. But the changes also made it more important for policyholders – and the insurance professionals that serve them – to understand the implications of those choices.

These legislative reforms are intended to give businesses more choices and reduce costs by modifying how litigation and medical treatments are handled for injured workers. For instance, employees can no longer pursue a negligence action through the civil courts. Instead, all litigation has to go through the normal workers’ compensation administrative process. Businesses now even have the option to opt out of workers’ compensation insurance entirely, though they still have the responsibility to protect their employees and bear the costs related to workplace injuries and illnesses.

What You Need to Know
Even with all of the recent discussion of workers’ compensation reform and its impact on businesses and workers, many people still do not fully understand what workers’ compensation is, how industry reforms impact it, and how businesses can use it strategically. Simply put, workers’ compensation insurance covers employers for their statutory and legal obligations for employee expenses that are a direct result of on-the-job injuries or illness. While benefits differ within and among the states, they typically include weekly payments in place of wages and reimbursement for medical and rehabilitation expenses.

Insurance professionals have an opportunity – and responsibility – to help their clients better understand how workers’ compensation insurance can benefit their businesses. The Occupational Safety and Health Administration (OSHA) estimates that for every $1 invested in effective safety programs, $4 to $6 may be saved as illnesses, injuries and fatalities decline. Realizing these gains begins with loss control, which not only helps to make workplaces safer, it also results in direct cost savings for the business. As a result, workers’ compensation costs decrease, fewer overtime costs accrue, productivity increases, turnover rates decrease and relations between labor and management improve. By creating a culture of safety in the workplace, with a management culture that keeps everyone accountable, everyone benefits.

Top Tips to Establish Workplace Safety
As you help customers plan out their risk management strategies, consider the top four steps to promote safety.

Top Four Steps to Promote Safety
1. Bring safety out of the back room and into the boardroom.
2. Become proactive about health and safety by establishing a culture of workplace safety.
3. Implement safety as an enterprise value, not just a cost center.
4. Use objective tools to quantify results.

A strategic approach to workers’ compensation is just as important to cost savings as smart tax planning. By advising policyholders to create a culture of workplace safety, independent insurance professionals can solidify their relationships as trusted advisors to their clients.

About the author
Mark Hogle is Senior Vice President, Regional Manager of the Western Region for EMPLOYERS®, America’s small business insurance specialist®, which offers workers’ compensation insurance and services through Employers Insurance Company of Nevada, Employers Compensation Insurance Company, Employers Preferred Insurance Company and Employers Assurance Company. Insurance is not offered in all jurisdictions. For more information, please visit www.employers.com.
Understanding Cyberterrorism

Without a doubt, cyberterrorism poses a real threat to governments, organizations and individuals around the globe. In today’s high-tech world, all types of computer networks are logical targets for all sorts of adversaries. In fact, according to a figure from U.S. officials, an astounding 60,000 new malicious computer programs are identified every day.

But how does one exactly define cyberterrorism?
In a 2000 testimony before the Armed Services Committee of the U.S. Representatives, Dorothy Denning of Georgetown University coined a still-popular definition of cyberterrorism: “the convergence of terrorism and cyberspace…generally understood to mean unlawful attack and threats of attack against computers, networks and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives.”

While that may be a mouthful, it does seem to sum it up. Depending on who you ask, however, cyberterrorism can have a somewhat surprising variety of meanings. Why this ambiguity? Well, since cyberterrorism is a relatively new term and is a product of the technological age in which we currently live, its definition is naturally still evolving. And as the technology surrounding cyberterrorism itself changes, the definition of the term will continue to change as well.

“It’s hard to define something that’s so intangible, so shifty, so below the radar of an otherwise law-abiding society,” said Carmi Levy, an independent technology analyst and journalist. “It’s also hard to define something most of us would rather shunt out of sight. This is typical behavior, and nothing we haven’t seen with earlier forms of anomalous technology-related threats, such as viruses and malware.”

The other hurdle he sees is our collective unfamiliarity with the threat. “It’s hard to define something until the majority of society agrees it’s a problem and has seen enough of it to merit actual recognition,” said Levy. “Unfortunately, we’re not there yet. Until it touches more of us in a more direct manner, expect it to remain difficult to pin down.”

Perhaps the thorniest issue is that the term’s root word is something society still struggles to define. “The simpler term ‘terrorism’ itself can have a variety of definitions, and ‘cyber’ just adds layers of complexity and misunderstanding to the issue,” said Kurt Baumgartner, a senior security researcher at Kaspersky Lab, a Moscow-based computer security company.

As the terms “terrorist” and “freedom fighter” have been debated in the past, when it comes to cyberattacks, there can be a fine line between activism and terrorism. And which side of that line an event falls on often varies depending on your perspective. In today’s digital world, some see the progression from activist to “hacktivist” as a natural one.

“It’s pretty easy to imagine past activist heroes might well have engaged in some type of hacktivism depending if they’d had access to the technology,” said John Kindervag, a security expert and principal analyst at Forrester, a research company in Cambridge, Massachusetts.

Kindervag also wonders if defacing a website or bringing down an ecommerce portal, like the 2011 disruption of Sony’s PlayStation Network, an online video game platform, is actually terrifying or merely inconvenient. “For me, the issue is if individual lives are in jeopardy at the moment of the action,” said Kindervag. “Disrupting the air-traffic control system to make planes crash would definitely be cyberterrorism. The Sony PlayStation Network attack would not be.”

What Kind of Damage Can Cyberterrorism Do?
Since cyberterrorism is such a new brand of crime, we as a society do tend to be somewhat complacent when it comes to cybersecurity. However, in the near future, we can only expect to hear more about both cyberterrorism threats and actual incidents. “The threat will only grow with the passage of time,” said Levy. “And it’s up to everyone to begin treating it as it deserves to be treated: with respect.”

Currently, the most frightening potential attacks are those that come from all angles. Baumgartner envisions a scenario in which cyberterrorists simultaneously disrupt communications systems,
In May 2012, another piece of malware, a virus called Flame, was uncovered. This virus infiltrated the computers of high-ranking officials in Iran with the goal of collecting information. Flame appeared to be approximately five years old when it was found, and the Washington Post has reported that it was designed by the United States; publicly, U.S. officials have not stated that they were responsible for creating this particular virus.

During April and May of 2007, Estonia was the victim of violence, riots and cyberattacks after officials moved a memorial commemorating the Soviet liberation of Estonia from the Nazis during World War II. Hackers shut down government ministry websites, two important banking websites and political party websites. They even disabled the email server for the Estonian parliament. Officials in Estonia accused the Russian government of orchestrating the denial-of-service attacks, but NATO and the European Commission were unable to find concrete evidence to prove these allegations.

In 2011, researchers from various high-tech companies uncovered a Trojan horse called Sykipot. This cyberweapon attempted to obtain documents from high-ranking executives, mainly those in the defense field at companies that developed unmanned drone planes. Officials believe that these attacks are coming from an established group located in China.

While we all like to hope that our government infrastructure is infallible, such attacks show that 100% protection is likely impossible. “Every system has areas of vulnerability, and there is no such thing as an inviolable or impenetrable solution,” said Levy. “Like conventional crime, military and quasi-military threats, it’s foolish to think we’ll ever be 100% safe. The world has simply never worked that way, and it isn’t about to start now.”

How Do We Stop Cyberterrorists?

While no amount of improvement will ever ensure society is cyberattack-free, experts say that governments and organizations should be proactive when it comes to investing in preventative measures. As technology continues to move forward at an alarming rate, so too must the laws regarding cyberactivities. Because currently, neither civilian nor government officials are truly able to combat this new and ever-changing threat. “Traditional law enforcement tools and processes need to be updated or replaced entirely,” said Levy.

Baumgartner feels similarly. “It is important to get past the short-term political gimmicks and silliness that we have seen and get down to business,” he said. “Addressing the problem effectively is a complex and difficult task, and overburdening defenders with ineffective tasks that waste time instead of necessary solutions is a difficult balance.”

To reach the proper balance, Levy recommends that law enforcement officials and business leaders strive for improved task forces, specialized training, and a re-prioritization of resources toward this class of crime. This, he believes, will greatly reduce the risk of attack and lower the severity and impact if an attack does occur. “They can raise the vulnerability bar sufficiently high to discourage the lesser-skilled and motivated attackers, and make life sufficiently difficult on the true pros,” said Levy. Unfortunately, in his view, those who built the last-generation standards of policing the digital world may not be up to the task without extensive and expensive retraining. And even then, they may not be able to adapt their capabilities to this new reality.

“The existing culture within law enforcement may be inadequate,” said Levy. “No one project or initiative will be enough to adapt. Nothing short of a wholesale rebuild of government and law enforcement best practices will do.”
Employees and Their Social Media: Managing the Risk

by: Frank J. Saibert

In just a few short years, it has become part of the fabric of everyday life. We use it to post pictures of our travels and other noteworthy (or not so noteworthy) events (e.g., Facebook), to keep up with the comings and goings of professional colleagues (e.g., LinkedIn), to apprise our followers in almost real time of our every “significant” move (e.g., Twitter) and to pontificate on subjects from great to little general interest (e.g., blogs). Social media is here and it looks like it’s staying.

For businesses, including insurance agencies and their clients, social media can provide unprecedented opportunities. While the avenues social media allows for niche marketing and access to heretofore unattainable demographics are becoming generally known, social media also has a growing role in employers’ relationships with the people they hire, don’t hire, employ and, in more and more cases, terminate. For example, recent studies suggest that nearly forty percent (40%) of employers in the United States utilize some social media websites to screen, or screen out, job applicants. See “37 Percent Of Employers Use Facebook To Pre-Screen Applicants, New Study Says.” Huffington Post, April 20, 2012.

But, of course, with opportunities come risks. This article provides an overview of some of the legal pitfalls that insurance agencies and their clients, as employers, can expect to face if they use social media in the management of their workforce.

Discrimination Risks
Employers, and especially smaller employers for whom every hire is so significant, obviously want to perform as much lawful and reasonable due diligence on prospective job candidates as they can. Better to weed them out before they get in the door than having to tolerate a poor or disruptive employee on the inside who ultimately may bring an expensive and distracting lawsuit once they finally are fired. Or so the conventional wisdom goes.

Yet employers nationwide continue to encounter difficulty in obtaining solid intelligence on candidates from the best possible sources – the candidates’ former employers. Fearful of defamation or other lawsuits from their former employees, most former employers give the neutral reference (position, dates of employment and maybe salary information) and little more. Such reticence does little to advance the new employer’s evaluation of the candidate’s potential for future success.

Hence, the turn toward the internet. With a few clicks of the mouse, an agency executive or human resources manager can access all manner of information on the unwitting potential job candidate who fails to make private her social media. That picture of you on Facebook smoking weed in Amsterdam or slurping down jello shots? Your request to your “friends” for a service that provides “clean” urine samples? A mention of a long ago criminal conviction? These are all real life examples of social media activity that resulted in a person losing or not getting a job when their boss or potential boss snooped.

But just as social media portrays employees or applicants acting irresponsibly, it also may reveal to the employer facets of the employee the employer has no legitimate business knowing. And therein lies significant risk. A person’s sexual orientation, religion, pregnancy or disability status all may be on display on social media. If an employer then discriminates against an employee or applicant on the basis of such a protected classification, it almost certainly has broken a discrimination law. And even if the employer fires or does not hire a person for completely legitimate business reasons, that person most likely will be able to use the employer’s knowledge of the protected classification against the employer. The “I didn’t know he was gay, etc.” defense, which if true...
can be highly effective in court, may be unavailable to the employer monitoring social media.

We won’t presume to advise you as to whether you should use social media as a tool for the evaluation of applicants or employees. But we will caution you that, in employment litigation, where forensic technology experts can determine after the fact every internet site an executive or human resources manager has visited, the knowledge you gain from these searches can be as damning as it is useful.

**State Law Restrictions**
The potential for a discrimination lawsuit is not the only risk for employers seeking to use social media. Several states, including California, Delaware, Illinois, Maryland, Michigan and New Jersey, have passed laws that, in one form or another, prohibit employers from compelling employees to divulge their social media passwords or information. Employers who run afoul of these laws could subject themselves to serious financial risk.

The Illinois law is illustrative. Effective January 1, 2013, it prohibits “any employer to request or require any employee or prospective employee to provide any password or related account information in order to gain access to the employee’s or prospective employee’s account or profile on a social networking website or to demand access in any manner to an employee’s or prospective employee’s account or profile on a social networking website.” 820 ILCS 55/10. That means that Illinois employers cannot ask or require passwords and cannot otherwise “demand” access to an applicant’s or employee’s social media website, by, for example, coercing the employee to go onto the site in front of the human resources manager.

Employers who violate the Illinois law may be subject to a circuit court lawsuit by the aggrieved employee or prospective employee. A prevailing employee or applicant in such an action can recover actual damages, which may include substantial backpay for the time she was out of work, fines and attorneys’ fees. Criminal sanctions also are available: the employer, prospective employer, or their agent (i.e., the agency executive who broke the law) is guilty of a petty offense.

Illinois employers still maintain the right to prevent their employees from being on social media during working time. The law includes a provision expressly allowing employers to promulgate and enforce workplace policies that govern employees’ internet, email and social media usage. Nor does the Illinois law restrict an employer’s monitoring of its own emails or computer systems. And of course, Illinois employers still are free to search for information, through Google or other search engines, available in the public domain.

Obviously, if you or your clients operate in a state with a restrictive social media access law, you need to familiarize yourself with the specific restrictions.

**The National Labor Relations Board and Protected Concerted Activity**
As if state law restrictions concerning employers’ access to employee social media are not enough, agencies and their clients also must worry about the National Labor Relations Board (“NLRB” or “Board”) and its recent revival of the “protected concerted activity” doctrine.

The Board is the federal agency that oversees employers’ relationships with unions. As the insurance industry is very lightly unionized, most agencies have had little reason to come into contact with the Board. Until now.

As unions today represent less than seven percent (7%) of the country’s private sector workforce, the NLRB, to remain relevant, had to find new law enforcement opportunities consistent with its enabling statute, the National Labor Relations Act (“NLRA” or “Act”). The “protected concerted activity” doctrine under the Act recently has been the Board’s most prominent, and for it, promising chance for the agency’s reinvention.

Under this doctrine, employees’ actions taken for the mutual benefit or aid of co-workers (e.g., internal safety complaints, criticism of supervisors, inquiries about wage disparities, etc.) are protected under the Act and employers cannot lawfully retaliate against employees who raise such concerns. The critical point here is that all employees, whether unionized or not, can seek protection under the doctrine. So by focusing on the
doctrine, the Board, in practical terms, has expanded its reach into industries it traditionally did not regulate much.

A couple of recent NLRB cases applying the protected concerted activity doctrine to employee social media demonstrate the NLRB’s zeal.

In the first case, filed in October 2010, the Board’s General Counsel alleged that American Medical Response of Connecticut (“AMR”) had illegally fired an employee who criticized an AMR supervisor on her Facebook page. American Medical Response of Connecticut, Inc., Case No. 34-CA-12576. AMR at the time maintained in its Employee Handbook a policy, titled “Blogging and Internet Posting Policy,” that expressly prohibited workers “from making disparaging, discriminatory or defamatory comments when discussing the Company or the employee’s superiors, co-workers and/or competitors.” The Handbook further forbade employees from posting pictures of themselves “in any media, including but not limited to the Internet, which depicts the Company in any way,” without management’s prior written approval.

The case was set to be tried before an NLRB Administrative Law Judge (“ALJ”) in February 2011, but settled the day before. According to a Board press release, AMR agreed to reform its “overly broad” employee communication policy. AMR also reached a private, non-union agreement with the terminated employee. The Board’s first shot in the battle over protected concerted activity in a social media world had been fired.

In the second case, the Board’s General Counsel’s office continued to display its obsession with the protected concerted activity doctrine in the context of social media. Richmond Dist. Neighborhood Ctr., NLRB ALJ, NO. 20-CA-91748, November 5, 2013.

Ian Callaghan (“Callaghan”) and Kenya Moore (“Moore”) worked on teen activities for a non-profit San Francisco organization that provides community programs. During a May 2012 staff meeting, employees expressed to management multiple problems regarding poor supervision and a general feeling of mistreatment.

On July 30, 2012, the employer sent a letter to Callaghan offering to retain him at his teen activity leader position. It also sent a letter to Moore offering to employ her at a downgraded position.

Days later, Moore and Callaghan engaged in a Facebook dialogue over the course of two hours that was available for viewing to multiple co-workers. During the online chat, Moore and Callaghan, using profane language, indicated that, unhappy with their employer, they were going to act uncooperatively and insubordinately on a going forward basis. If Moore and Callaghan thought that their Facebook conversation was going to remain secret, they were delusional. Within a day, a co-worker sent the screenshot to management which promptly fired Moore and Callaghan.

Callaghan filed an unfair labor practice charge with the NLRB and the Board’s General Counsel issued a complaint. Fortunately for the employer, following a hearing, the ALJ dismissed the complaint. The ALJ first found that Moore’s and Callaghan’s Facebook discussion indeed was concerted activity. In his view, the two employees simply were continuing the dialogue about perceived adverse working conditions that had begun in the May staff meeting.

However, the ALJ ultimately ruled, the concerted activity was not “protected.” Because Moore’s and Callaghan’s Facebook conversation emphasized their planned insubordination and non-cooperation with the employer’s mission, it lost any protection it otherwise might have had under the Act, allowing the employer to lawfully fire Callaghan and Moore. Wrote the ALJ, “Respondent believed that the Facebook comments jeopardized the program’s funding and the safety of the youth it serves.”

Of course, the full NLRB has not passed on the ALJ’s decision. And the fact that the Board’s prosecutorial arm continues to bring these social media cases should be a cause for real concern among employers, even in the insurance industry.

Conclusion

The law is beginning to catch up to the technology, and not in a good way for employers. Agencies and agency clients seeking to avoid the risks attendant to employee social media use should consider the following:

• Dedicating an employee or contractor to fulfill a human resources function within the organization. Having a human resources professional who can identify risk in this area and advise management as to how to proceed lawfully is essential.
• Auditing the organization’s social media and internet policies for compliance with state law and the NLRB’s protected concerted activity doctrine.
• Evaluate the costs and benefits of using social media as a way to evaluate applicants and employees. Sometimes, the risk just isn’t worth it.

About the Author

Frank J. Saibert is chair of the labor and employment practice at the law firm of Ungaretti & Harris LLP. He represents public and private sector employers nationwide in labor relations and employment matters. He can be reached at fjsaibert@uhlaw.com.
The average length of a collision repair is 13 days. Are your customers prepared to borrow a car from the family for that long?

Research shows that Rental Reimbursement coverage drives both satisfaction and retention.

FIND OUT MORE AND SHARE THE NEWS AT MY13DAYS.COM.
I AmTrusted
to provide my insureds with the best coverage.

Insurance agents are trusted to provide their customers with the best protection at every turn. That’s why the best agents in the industry recommend the superior small-business insurance coverage available only from AmTrust. Not only is AmTrust the 10th largest workers’ compensation insurance provider in the nation, we’ve also earned an “A” rating from A.M. Best. It’s some of the industry’s best small-business insurance coverage, available only from the industry’s best agents like you.

To learn more about AmTrust, visit us at amtrustnorthamerica.com or call 877.528.7878.
Widening Wealth Gap is Biggest Global Risk, World Economic Forum Predicts

From Risk Management Monitor

According to the World Economic Forum’s Global Risks 2014 report, the chronic gap between the incomes of the richest and poorest citizens is the risk most likely to cause serious global damage in the next decade. Looking forward, the 700 experts queried emphasized that the next generation will only feel this disparity more acutely if current conditions continue. Those presently coming of age face “twin challenges” of reduced employment opportunity and rising education costs, prompting the World Economic Forum to consider the impact on political and social stability as well as economic development.

“Many young people today face an uphill battle,” explained David Cole, group chief risk officer of Swiss Re. “As a result of the financial crisis and globalization, the younger generation in the mature markets struggle with ever fewer job opportunities and the need to support an aging population. While in the emerging markets there are more jobs to be had, the workforce does not yet possess the broad-based skill-sets necessary to satisfy demand. It’s vital we sit down with young people now and begin planning solutions aimed at creating fit-for-purpose educational systems, functional job-markets, efficient skills exchanges and the sustainable future we all depend on.”

After a widening global wealth gap, experts predicted that extreme weather events will be the global risk next most likely to cause systemic shock on a global scale. They identified fiscal crises as the global risk with the potential to have the biggest impact over the next 10 years.

THE TOP FIVE MOST LIKELY AND MOST POTENTIALLY IMPACTFUL GLOBAL RISKS ARE:

<table>
<thead>
<tr>
<th>Most Likely Risks</th>
<th>Most Potentially Impactful Risks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Income disparity (societal risk)</td>
<td>1. Fiscal crises (economic risk)</td>
</tr>
<tr>
<td>2. Extreme weather events (environmental risk)</td>
<td>2. Climate change (environmental risk)</td>
</tr>
<tr>
<td>3. Unemployment and underemployment (economic risk)</td>
<td>3. Water crises (environmental risk)</td>
</tr>
<tr>
<td>4. Climate change (environmental risk)</td>
<td>4. Unemployment and underemployment (economic risk)</td>
</tr>
<tr>
<td>5. Cyberattacks (technological risk)</td>
<td>5. Critical information infrastructure break down (technological risk)</td>
</tr>
</tbody>
</table>
**Sochi: The Power of Social Media for Spreading the Terrorist’s Message**

The fundamental reason that the Modern Olympic Games are a terrorist target is that they are on the world stage, with media ready to spread the message of any violent acts committed by terrorists. Before social media, that widespread message was disseminated by traditional means, such as newspapers, television and radio. Now, news spreads like wildfire so that even false stories gain traction, creating worldwide fear.

**Incident:** Within 24 hours after the 2014 Sochi Opening Ceremony, 16,000 users of Facebook and Twitter shared the false story that the operator of the malfunctioning five animatronic snowflakes that were supposed to transform into Olympic Rings was found dead in his hotel room with multiple stable wounds and that officials didn’t suspect foul play.

**Lesson:** The challenge is that the Olympics are a major global media event, which attracts terrorists who seek publicity that would naturally arise from any successful threat or attack that could be associated in time or location with the Olympic Games. Now, with the power of social media, terrorist publicity can be spread in less traditional means, such as Facebook, Twitter, or YouTube, and could potentially be false, yet accomplish the same results.

In the months leading up to the 2014 Winter Olympic Games in Sochi, the world watched in fear over the safety of athletes and spectators, amid threats of terrorism that were felt to be imminent. U.S. athletes were advised not to wear team clothing outside of the Sochi venues and many of them left their families and friends at home in order to avoid the risk. Safety concerns at the Olympics are nothing new as they have been of primary concern since 1972 when eight Palestinian terrorists infiltrated lax security at the Olympic Village and took eleven Israeli athletes, coaches and officials hostage. During a botched rescue attempt all of the hostages were killed. For the first time in modern Olympic history, the competition was suspended.

While concerns of terrorism have made headlines leading up to recent Olympics, the incidents that have occurred in the Modern Olympic Games exemplify numerous risk management and legal principles that can be applied to sporting, recreation, and other events in public venues. In the most recent Olympics, in Sochi and London, record amounts of money were spent to make the venues safe, creating atmospheres more akin to security events than athletic contests. A few incidents of interest did occur in those Olympics despite extraordinarily heavy security.

**Incident:** At the 2012 London Olympics, a spectator threw a bottle onto the track during the men’s 100 meter final. The Dutch judo world champion assisted in subduing the man who was arrested. No one was injured due to the incident.

**Lesson:** Unruly spectators can throw objects onto the playing field, which is a risk for any sporting or public event. Well trained security should be present and attempt to prevent and quickly react to such incidences. Spectators should be advised that this behavior will not be tolerated and items brought into the venue can be prohibited and regulated through use of screening.

The following incidences in previous Olympic Games are memorable because of the significant amount of media attention that followed as well as the tragedy of such events. The legal and risk management issues that such incidences raise are listed below and can be used as discussion points or checklists for risk management planning in sport and recreation.

**Incident:** 21 year old Luger Nodar Kumaritashvili was killed following a crash on the luge course at the 2010 Vancouver Olympic Games during a training run. He lost control of his sled, went over the track wall...
and struck an unpadded steel pole near the finish line at the Whistler Sliding Center. The tragedy occurred hours before the Opening Ceremony, when he lost control of his sled near the bottom of the course, crashing into a metal pillar traveling at 143.3 kilometers per hour (88 mph). Officials from the Vancouver 2010 organizing committee and the International Luge Federation did not find any deficiencies in the track that caused the accident. However, the track was closed and changes made in order to avoid any further accidents.

Legal Issues
- Were organizers negligent in failing to pad the steel pole, designing the course, or not erecting a wall high enough to protect the luger?
- Was the luger comparatively negligent by traveling at a speed that was unsafe, causing him to lose control?
- Did the luger assume the risk of the accident as he knew that the sport is dangerous and can cause injury or death?
- What was the significance of the findings of the organizing committee and the International Luge Federation?
- If a lawsuit was filed, would the changes made to the luge course be admissible as evidence in court?

Risk Management Issues
- How should the luge course be designed so that athletes can be challenged, but at the same time be safe?
- Are straight-aways and curves designed in such a way that lugers will not gain excessive speeds and/or lose control?
- Have all poles, posts and other hazards been padded?
- Are walls high enough to protect athletes, but also allow for media access?
- Should there be exceptions to prohibitions of entry to the course? For example, should the media be able to freely enter the course?

Incident: In the 2004 Athens Summer Olympic Games, Brazilian Vanderlei de Lima was leading when an Irish protestor pushed him to the side of the road four miles from the finish. The athlete won the Bronze medal after losing momentum.

Legal and Risk Management Issues
- Were event organizers negligent in failing to provide sufficient security for the course?
- To what extent should event organizers provide security so that spectators are prohibited from entering the course?
- What barriers should be erected around the course in order to keep spectators out?
- How can a 26.2 mile marathon course be secured?
- Was Harding an accessory to the crime against Kerrigan?
- Were event organizers negligent in failing to provide sufficient security?
- Was it reasonably foreseeable that athletes competing for a place on the Olympic team would require security to protect them from possible assailants?

Risk Management Issues
- To what extent should athletes be provided security in order to protect them from criminal actions by other athletes or their agents?
• Should athletes have their own body guards?
• If so, at what stage of their careers should athletes provide for their own security?

Incident: In the 1988 Seoul Summer Olympics, Greg Louganis hit his head on the springboard while doing a reverse dive with 2 somersaults in a pike position. As he descended, his head came too close to the board and he hit the end of it with the top of his head, falling clumsily into the water. He scored 6.3 on the dive, but his scalp was bleeding and required 4 temporary stitches. It was reported that Louganis had practiced and performed 180,000 springboard dives in his 18 year career and that he had never hit his head on the board. What was unknown at the time is that Louganis was positive for HIV, which was not disclosed to the physician who stitched up his bloody head without wearing gloves. The physician, when he found this out tested negative for HIV.

Legal Issues:
• Would Louganis have been found negligent for not informing the doctor that treated him that he was HIV positive?
• Did Louganis have a duty to inform the doctor, and if so, did he breach that duty?
• Did the doctor assume the risk by suturing Luganis without using gloves?
• Did the doctor suffer damages even though it turned out that he did not contract HIV from Louganis?

Risk Management Issues:
• Wear gloves to protect from exposure to bodily fluids
• Proper disposal of contaminated items
• Needles from injections should not be reused
• Surgical masks and eye wear should be used for protection
• Sterilize Equipment

Incident: In the first women’s Olympic marathon in 1984 Los Angeles Summer Olympic Games Gabriela Anderson Scheiss was near the finish line when she staggered onto the track, suffering from heat exhaustion. She pulled the number off of Budd’s back as she fell. Budd, an 18 year old barefoot runner had to endure boos from the crowd. At the time, Decker was considered by many to be the greatest women’s distance runner in the world. She had missed the 1976 Olympics due to injury and the 1980 Olympics due to the U.S. boycott of the Moscow Olympics. The 1984 Olympics was Decker’s chance for a gold medal in that event. Decker had been one of Budd’s heroes while growing up. Budd finished seventh with tears coming down her face. The winner of that event was Maricica Puica.

Legal Issues:
• Did Budd cause Decker to trip or was it Decker’s actions that made her fall?
• Would Budd’s actions have to be intentional, willful or wanton or would simple negligence be sufficient for her to be deemed liable in this case?
• Does it serve public policy to have athletes sue each other or do such lawsuits impede the free play of sport?

Risk Management Issues:
• Should athletes be required to wear footwear when competing in track and field events?
• If Budd’s actions caused the incident, was disqualification appropriate?
• Should rules enforcement be consistent in order to prevent future violations?

Incident: In the 1984 Los Angeles summer Olympics, Great Britain athlete, Zola Budd tried to pass Mary Decker during the finals of the women’s 3,000 meter run. Decker became entangled with Budd’s left leg, causing Decker to fall to the infield. She pulled the number of Budd’s back as she fell. Budd, an 18 year old barefoot runner had to endure boos from the crowd. At the time, Decker was considered by many to be the greatest women’s distance runner in the world. She had missed the 1976 Olympics due to injury and the 1980 Olympics due to the U.S. boycott of the Moscow Olympics. The 1984 Olympics was Decker’s chance for a gold medal in that event. Decker had been one of Budd’s heroes while growing up. Budd finished seventh with tears coming down her face. The winner of that event was Maricica Puica.

Legal Issues:
• Did Budd cause Decker to trip or was it Decker’s actions that made her fall?
• Would Budd’s actions have to be intentional, willful or wanton or would simple negligence be sufficient for her to be deemed liable in this case?
• Does it serve public policy to have athletes sue each other or do such lawsuits impede the free play of sport?

Risk Management Issues:
• Should athletes be required to wear footwear when competing in track and field events?
• If Budd’s actions caused the incident, was disqualification appropriate?
• Should rules enforcement be consistent in order to prevent future violations?

Risk Management Challenges for the 2016 Summer Rio de Janeiro Olympic Games
Shortly after Brazil won the bid for the 2016 Summer Olympic Games, the competition between rival drug gangs in Rio de Janeiro’s “Monkey Hill” slum captured the world’s attention. Will Brazil be able to replace the sound of automatic gun fire with cheering crowds encircling Olympic competition ovals? Would it be better to use the countries’ resources to eliminate poverty and violence rather than to gain world stature as the first South American country to host an Olympic games? Whatever the answers to these questions, Brazil has a pressing deadline of two years to address its risk management issues. Certainly, Brazil need not reinvent the wheel in developing its risk management plan as there have been previous, recent Olympic venues with special security issues, namely Athens in 2004, Beijing in 2008, London in 2012 and Sochi in 2014. The cost for security has escalated, with the concern of potential terrorist threats to Olympic venues, representing primarily external security threats. Rio is hosting the FIFA World Cup in July of 2014, which provides the city the opportunity for a dress rehearsal for Olympic Games risk management.

Conclusion
With each Olympics, risk management knowledge, skills and tools have increased commensurate with each incident, threat and challenge. Hopefully, the Olympic ideal will continue despite the economic, political, and cultural challenges and that every two years the competitors in the Modern Olympic Games will continue the ancient practice of laying down their arms and embrace the philosophy of Olympism – building a better world through sport.
YOUR Time. YOUR Terms.
YOUR Insurance Expertise.
Phase into retirement by working from home.

Wahve
Work At Home Vintage Employees
www.wahve.com

WAHVE was one of the best decisions I ever made. — Sarah Ellis

Become a WAHVE Vintage Worker and extend your career working from home. WAHVE gives you choice when you’re thinking it’s time to phase into retirement. Choose the type of work you want to do. Work remotely for one of our insurance firm clients. Create a new life-work balance.

If you are ready or know someone who is ready to phase into retirement and work from home, just click on Become a Wahve on our website or call us at 646.807.4372 ext. 504.

www.wahve.com
646.807.4372 x504
Many people say things. Few people deliver.
Everybody says, “You can count on us”—but can you?

Whether the loss is large or small, residential or commercial, your customers need immediate response to begin the recovery process. With Paul Davis as a resource you have instant access to our network of insurance restoration and reconstruction experts. And our streamlined claims resolution is designed to make the claims process as smooth as possible throughout every loss, every time. Our goal is to get your policy-holders up and running as soon as possible.

At Paul Davis, the difference is not in what we say, but in how we perform.
At first when his wife said that Sargent Willis was on the phone and had some questions, Reverend Bobby thought he might have run a red light and was caught by a traffic cam. Sadly, the actual problem was much graver. The police officer began to question him about Sue Hardy, the church’s treasurer, and the role she played in the church’s business affairs. It seemed that there were some suspicions of financial impropriety, and that Sue was the likely perpetrator.

The Shock of a Collapsing Illusion
We hear a lot these days about identity theft, Internet fraud, email scams or Wall-Street defalcations, but the truth is most organizations are more vulnerable to fraud than they might think. Whether it is a church, a non-profit or a small business that you’ve put blood, sweat and tears into, the chance that you’re at risk for fraud is substantial.

The conversation between Reverend Bobby and Sargent Willis led to the arrest and conviction of what Reverend Bobby once described as a pillar of sainthood in their small but growing church. Sue was a Christian’s Christian. The backbone of the church, Sue gave of her time, taught Sunday school and was the treasurer for years.

Sadly, regardless of the type of organization, most frauds take place from within the company’s own ranks, and more times than not, by trusted individuals that we would never suspect.

By their nature, small businesses, non-profits or associations are typically run on a shoestring budget, which makes staffing tight and internal controls limited. And while most people are trustworthy, external factors can create a need that, combined with opportunity and a dose of rationalization, create the potential for unethical and fraudulent activity.

When the perfect storm of fraud hits and the illusion fades into reality it becomes clear the devastation that fraudulent activity creates. Every choice has a consequence and the consequences of fraud are significant and far-reaching.

What to Look For
Let’s use the example of Sue above to frame the discussion about how good people make very bad choices, which leads to fraud. According to the Association of Certified Fraud Examiners the following are red flags for fraudulent behavior:

1. Most frauds are committed by people who have worked in the organization for a number of years. People who have ten years or more of experience with the organization cause higher fraud losses. Why? The answer is simple: the longer a person is employed within a company, the greater the trust and responsibility. Likewise, trusted employees are not often considered likely candidates for fraud.

2. Individuals in one of six departments commit the vast majority of all frauds: accounting, operations, sales, executive/upper management, customer service and purchasing. If fraud occurs in your business, it is likely by someone who has opportunity; individuals in these six areas have the greatest opportunity to violate trust.

3. Fraudsters displayed one or more of these red flags before or during the commission of the fraud: living beyond means, financial difficulties, unusually close association with vendors or customers, and excessive control issues. Any of these behaviors could be a sign of impending danger.

In looking back on the situation, Reverend Bobby could have seen disaster coming. Sue was a trusted member of the church holding her position for more years than Reverend Bobby had been there. Not that longevity is a bad thing, but church leadership could have required a change of roles from time to time disrupting the natural flow of funds. Typically, when things change, inappropriate behavior comes to light.

But, beyond Sue’s tenure, she was quite protective over the money and monetary processes for the church. Excessive control is a significant sign that something might be amiss. When people are unwilling to let go of their control, take a vacation or insist that only they can do the task, leadership should step back and examine the role and function more carefully.

Finally, in Sue’s case, there never seemed to be enough. Sue received calls often from creditors. Consistently she would either quickly hang up, showing her dissatisfaction with the call received, or take the call on her cell phone, out of ear shot, and return to work irritated at the interruption.

Final Outcome
In the end, Sue embezzled over $200,000 from the church where she was trusted. The discovery was both a shock and disappointment to Reverend Bobby and the entire congregation. Every choice has a consequence. Sue’s choices – made over time – created significant consequences. Today she is serving a prison sentence that will leave a permanent scar on her and those close to her. Bobby shared that he now understands the importance of his role in this whole troubling problem. As management, Bobby has a responsibility to understand the three components of unethical behavior and often-illegal behavior: need, opportunity and rationalization. Most importantly, Bobby knows that with some minor changes Sue might have, although tempted, been prevented from making those dangerous choices, which led to an outcome that no one wanted. As a manager of your organization, what steps are you taking to protect your most valuable assets – your employees – from making dangerous decisions that impact them and your organization?

About the Author
Chuck Gallagher is the President of the Ethics Resource Group and an international expert in business ethics. Chuck provides training, presentations and consultation with associations and companies on ethics and creating ethical cultures where people do the right thing, not because they have to, but because they want to! Information can be found at http://chuckgallagher.com or Chuck can be reached via email at chuck@chuckgallagher.com or by phone at 828.244.1400.
The First Steps to Managing Cyber–Risk

Today, every company is reliant on technology, and data is often a critical asset. Managers and IT personnel must monitor reports via their computers and mobile devices 24/7—but even that seems like a futile attempt to keep up. Because each day, according to a June Financial Times article, companies generate 2.5 exabytes, or 1 billion gigabytes, of data. This daily deluge means that nearly 90% of the stored data in existence today has been created in just the past two years.

With this unprecedented growth, new threats emerge constantly. Such risks historically have been the domain of the IT department, but while cyber-risks are by definition rooted in technology, they are not actually technological risks; they are business risks. And business risks are best addressed through a holistic risk management process that includes systematic risk identification, assessment, quantification and mitigation.

The following three steps will pave the way for risk professionals to better protect one of their company’s most important assets: data.

**Step #1: Assemble a Cyber-Risk Team**

When it comes to cyberthreats, it is not about if the company will be attacked but when. The first, and one of the most important, things a risk manager can do is to talk to the information security team and involve them in a cyber enterprise risk management effort. Specifically, ask them what assessments have already been done. Then, examine what they have put in place to provide reasonable safeguards spanning people, processes and technologies. And keep them involved throughout the process, not just at the outset.

A good way to get the input and buy-in of the entire organization is to appoint a cyber risk management team to evaluate the company’s enterprise-wide threats. Include the chief information technology officer, head of IT security, general counsel and others from departments including communications, manufacturing and human resources. These are the personnel who will stand as the frontline response to any threat.

Get everyone involved and keep the organization informed of the efforts and steps you take to protect the corporation. Periodically report on the state of the organization’s cyber-preparedness to top executives and the board of directors. Both the board and senior leaders have a fiduciary responsibility to protect the information assets of the company.
In particular, the board needs to be made aware of all cyber-risks and receive regular reports on how new developments and trends could affect the company. Recently, the SEC weighed in on the issue, stating that it is a company's responsibility to not only understand its cyber-risks, but to ensure that the corporation secures its computer systems.

If there is an incident, the company's reputation is on the line. News outlets will be quick to pick up on cyber-incidents, and most company officers will not know where to turn.

Take the recent LinkedIn breach, which exposed some six million user passwords. Not only was LinkedIn lax with security measures, but it took the company hours to discover that its network had been attacked—and hours longer to notify the victims. No one was managing the risk. And that is not unusual. Only after Sony was the victim of an attack in 2011 did it hire its first chief information security officer.

**Step #2: Identify and Assess the Risks**

Once you have formed the cyber risk management team, the second step is to identify, assess and measure the risks for their potential frequency and financial impact. Think in terms of vital data and where it resides—not just on the computer in an office, but how it flows throughout your organization. Is the data in transit (on a USB drive), at rest (on an employee's desktop PC) or mobile (on an iPhone)? Once you understand where the data is and its importance, you can assess the risk and develop strategies to protect it.

Work with your team to understand your situational awareness. Think about the value of your data to a hacker, hacktivist or cybercriminal. What information would they target? Or, could you be a potential target of cyber-espionage or cyber-terrorism? And do not forget about non-tech-based threats, such as a hurricane, that could shut down systems or prevent access to data. Or, consider the exposure when an employee unintentionally obtains unauthorized access to data. These are risks related to technology but ultimately rooted in other realms (natural disasters and access control management).

Examine the vulnerabilities and current mitigation practices and then, based on resources, make determinations as to where people, processes and tools must be deployed. Threats must be evaluated for their potential likelihood and financial severity. Risk managers need to be part of the decision-making process to determine which risks pose the greatest threat to the corporation and which of the many IT security options will best mitigate these risks.

**Step #3: Develop an Incident Response Plan**

Companies with incident response plans fare much better after a data breach than those without plans. Thus, the final step is to develop a plan that, first and foremost, defines who will be the point person for external and internal activities when a breach occurs.

Unfortunately, very few companies maintain internal experts who can deal with all aspects of this kind of risk. So one thing to note while creating the plan is whether or not a cyber-insurance policy exists. If it does, alert all departments about its existence so that the company can take advantage of the insurer’s expertise.

Some insurers offer crisis management experts, frontline breach professionals and cyber-risk lawyers. Some policies even provide a risk management package that includes self-assessment tools.

But whether you buy insurance or not, you will need an incident response plan. So ensure that the company does research beforehand to find third-party experts to lean on when disaster strikes.

One last component of any plan is to ensure it includes a means to learn from the breach. Include a formal debriefing step after an incident to get to its root cause and understand when the attack took place, how the system was infiltrated and what the motivation of the attacker was.

Lastly, remember that a plan is only valuable if it works and if everyone involved knows it. So even if you are lucky and no breach occurs, take the incident response plan out and test it at least once a year.

**About the Author**

Thomas Dunbar is chief information risk officer of XL Group. www.xlinsurance.com
Companies can partner with IAIP to promote the insurance industry through providing education, networking and industry alliance, as well as providing insurance products to the general population. Several levels of corporate partnership are available to meet your business’s needs.

Contact the Director of Marketing at 800-766-6249 extension 20, or email marketing@iaip-ins.org today to find out how your company can benefit from partnering with IAIP.
Since its’ founding, the ISFA Board of Directors have awarded over $435,000 in college and professional scholarships. With the continued support of our corporate donors and the IAIP members the ISFA Board of Directors can continue to provide vital education dollars for scholarships to deserving applicants.

These young men and women are just a few of the ISFA scholarship recipients that have gone on to have a career in the insurance industry.

Today, we are asking you to join us by becoming a Partner in Education. What is a Partner in Education? It is an easy way to support ISFA’s goal of Promoting Excellence through Education. Partners in Education is an online sustained giving program. When you make a commitment to support Partners in Education you create an automatic monthly credit card charge for the amount and period you designate. The minimum monthly donation is just $10. You can’t imagine how important your monthly donation of $10 can be to both the current and future employees of the insurance industry. A small amount that can make such a significant difference!

The greatest reward for pledging a sustaining donation or any donation to ISFA is the knowledge that your dollars are enhancing the education and careers of others in the insurance industry. We need your help to continue the Insurance Scholarship Foundation of America’s 20-year legacy underwriting excellence in education through scholarships!

We need your support. ISFA is asking you to become a Partner in Education and begin investing in OUR industry’s future. Visit the ISFA website:  www.insfa.org, click on the "Donate Now" button and become a Partner in Education today.

While an online donation is quick, easy and safe, we appreciate that some would rather donate with a check. Donations can be mailed to ISFA, P.O. Box 866, Hendersonville, NC 28791.

Every donation dollar counts. The Insurance Scholarship Foundation of America’s strength is in its donors and we are counting on you in 2014 to continue your support of Promoting Excellence through Education.

ISFA is a 501 c 3 Public Charity. All donations are tax deductible.
WELCOME
New IAIP Members!

Welcome our new members from February 7, 2014 through April 30, 2014

REGION I
Abigail Leigh Allman
Emily Briglia
Kelly Davis
Jennifer L. Dilworth
Cassandra Ghiatis, CISR
Cynthia Kettering
Meagen LaComb
Carol Maragni
Pamela Pelletier, CISR, CRIS
Christine Phillips
Joseph Sellenny
Carrie Veronesi

REGION VI
Ruth Bost
Jenny D. Dahl
Ronda Diver
Kristin Dion Gay
Robyn Gillispie, CISR
Mary Gorbet, CISR
Twan Johnson
Heather R Muslow
Alex Plotkin
Michelle Renee Smith
Carmon Thompson
Frederick Wagner
Sandra Weathersby

REGION VII
Melissa Bernard, CIC, CISR
Pauline Michelle Dorsett
Janet Kush

REGION VIII
Thomas B. Anderson
Doug Barney
Walt Bennett, MAT, CPCU, AIS
Tamara Durente
Patrick L. Finch
Rachel Garcia, AIS
Valiena Hoffert
Ashley Houlihan, CISR
Helen Jang
James Kamanski
Melissa Langley
Michelle L. Marchini
Jessica Mendoza
Tom Nowell
Kathy Rogan
Rachael Rose
Jenny Schaeffler
Evan Scott
Eric Senna, LUTCF
Ken Stewart
Gerald H Yamane, CIC

REGION IX
Hadley Arnits
Karin Bruhn
Danielle M. Butkins

International Association of Insurance Professionals is a professional association open to individuals in the insurance and risk management industries, and provides insurance education, skills enhancement and leadership development. Membership provides you the opportunity to increase your business productivity and profitability by participating in educational offerings and making business connections with other industry professionals. More than 70% of our members have advanced their careers through belonging to IAIP.

To join, contact John McColloch, Director of Membership, at 800-766-6249 extension 26, or email membership@iaip-ins.org.
Advance Your Career

IAIP offers the following prestigious industry designations:

Certified Insurance Industry Professional (CIIP)

Members may choose to earn the CIIP or the:

- Certified Professional Insurance Woman (CPIW)
- Certified Professional Insurance Man (CPIM)

Diversified Advanced Education (DAE)

Certified Leadership Professional (CLP)

CONGRATULATIONS!

NEW CLPs

Jacquie Long, AAI, ACSRP, AINS, ACS, CIIP, CLP – Region I
Pamela M. Holt, AINS, CIIP, DAE, CLP – Region III
Melissa G. Peak, ACA, CCA, CIIP, CIR, CISR, CPSR, DAE, PPIA, CLP – Region III
Margaret A. Wildi, M.S. CPCU, AIM, AAM, AINS, CLP, CIIP, DAE, CPD – Region III
Chelle Carey, CLP – Region IV
Katie Liljeberg, CLP – Region VI
Lori Phillips, CLP – Region VI
Carol D. Burke-Maurizio, AINS, CIIP, CLP – Region VIII
Kate Gilbert, CLP – Region VIII
Christina Murphy, CISR, CLP – Region VIII
Lauri M. Oakden, CLP – Region VIII
Sheree Pendergrass, CIC, CRM, CLP, CIIP – Region VIII
Kelly M. Radkowski, CLP – Region VIII
Letitia R. Riley, CIIP, DAE, CLP – Region VIII

NEW DAEs

Yesenia Flores Morales, CISR, CPIW, DAE – Region III
Kimberly Dawn Shattruck, CISR, CPIW, CPIA, DAE – Region III
Gina Thomas Patterson, CISR, CPIW, DAE – Region VIII

NEW CIIPs | CPIWs | CPIMs

Tiffany E. M. Butler, CRIS, CPIW – Region I
Jacquie Long, AAI, ACSRP, AINS, ACS, CIIP, CLP – Region I
Sheree Pendergrass, CIC, CRM, CLP, CIIP – Region VIII

To learn more about these designations, including how to qualify, visit internationalinsuranceprofessionals.org and click on Designations under the Education tab. Contact Rebecca Clusserath, Director of Education at 800-766-6249 extension 18 for more information.
Meet the 2014-2015 Board of Directors

rosalyn (roz) horton
CIC, CIIP, PIAM
President
Rosalyn (roz) horton joined the association in 1992 when she changed careers, from running a family-owned business, and entered the insurance industry. She is currently a Member-at-Large in the Tennessee Council of Region III. Over the years of her membership she has served on or chaired committees on all levels of the association. Officer positions she has held include Tennessee Council Director and Region III Vice President, and she was elected International Secretary at the Las Vegas Nevada Convention. She has received numerous awards including Rookie of the Year – local and regional, Claims Professional of the Year – local (twice), Insurance Woman of the Year – local and state, CWC Speak Off – state (winner – four years); regional (runner-up), AAMGA Award – state (twice), AAMGA Presidential Award – international, and TJ Mims Award of Excellence (Region III Award).

She is a Gold Member of ISFA and a Trendsetter contributor to the Legacy Foundation.

roz retired, after 22 years, from her position as Underwriting Team Lead for AGCS Marine (a division of Allianz Global Corporate & Specialty). During her employment she was the recipient of numerous peer and management awards including Employee of the Year. She currently holds the CIC-CIIP-PIAM designations and is in the process of obtaining her CPI from the Professional Career Institute. In addition to her insurance education roz also has her Certification in Convention and Meeting Planning from Calhoun College (GA) and received her FCC Broadcast License from Elkins Institute.

She is a member of Delta Master Chapter of Beta Sigma Phi, where she holds the Ritual of Jewels degree. She is a sustaining sponsor of St Joseph’s Indian School in South Dakota, and a member of St. Mary of the Seven Sorrows Catholic Church serving on the wedding and funeral preparation committee. She is also very active with her high school alumni association. Over the past several years she has volunteered and been a sponsor at the ISFA and MTSU Chair of Insurance golf tournaments.

roz is a widow and has three children, five grandchildren and five great-grandchildren. Her interest include traveling, reading, annual celebrations with the Birthday Girls, family and friends outings and “cruising” in her Smart Car convertible. She loves music (played loud with the top down on the car) and enjoys dancing. Her bucket list includes the following: trip to the Galapagos Islands, rafting/camping the Colorado River, learning to paddle board, zip lining through the Amazon Rain Forest and jumping from the Stratosphere Hotel a second time. She has already jumped once but wants to do it again, at night, to see the lights of Las Vegas.

roz attributes her success in her career – and involvement in the insurance industry – to her membership in IAIP. She received her education through the courses offered by them and was encouraged to seek other opportunities outside of the association. The networking opportunities at council, regional and international conventions encouraged her involvement in the association and the industry as a whole.

However, mentoring was the biggest factor in her success. Coming into the industry (past middle age) with no knowledge of the ins and outs of the business or the association, she was at a slight disadvantage to her peers. Luckily, along the way she had people who saw her potential and cultivated it. She gives a special thank you to everyone who has touched her life/career in that special way. Most of all she gives a very heartfelt thanks to E. Faye Evans (past International President) and Sylvia Robinson (past Tennessee Council Director) who still remain her staunchest supporters and best friends after 22 years.

Debra C. Kuhne
AAI, AIC, AIS, CIIP, DAE, CELS
President-Elec
Debbi has been a member of IAIP since September 1992 and is a member of the Waterbury Association of Insurance Professionals. Debbi was named Region I Insurance Professional of the year in 2009. She has served in many positions on her local level, was Connecticut Council Director 2008-2010, Region I RVP from 2010 to 2012, International Secretary 2012-2013 and most recently International Vice President 2013-2014. Debbi is an avid supporter of the IAIP Legacy Foundation.

Debbi is an Injury Management Consultant at Litchfield Insurance Group in Torrington, CT. In her position she is responsible for Workers’ Compensation Claim Management for their clients as well as providing “back office” HR assistance for clients. Debbi’s expertise in Workers Compensation Claim Management and cost reduction strategies helps to mitigate
the impact workers’ compensation claims have on the client’s bottom line. With so many employment laws and regulations in effect today, Debbi’s extensive training in the areas of FMLA, ADA and Sexual Harassment gives her the unique ability to advise employers on day-to-day workplace issues to ensure client’s HR policies and practices comply with state and federal requirements and are free of flaws that can put their businesses at risk.

Debbi holds the AAI, AIC, AIS, CIIP, DAE, and CELS designations. She has taken several of IAIP’s courses, competed in two regional CWC Speak-Offs and this year she became an instructor for CLP courses.

Debbi loves to garden, perform home renovations, read and spend time with her two cats – Sarah and Phoebe.

**Tish Riley**
**CIIP, DAE, CLP**
**Vice President**

Tish Riley’s career in insurance spans 30+ years working for three different P & C companies. Like many of us in the industry, she had not intended to make insurance her career, but in 1974 she landed a job as a file clerk for St. Paul Fire & Marine Insurance in their Southern California office and worked her way up to manual rater over the next couple of years. Tish left insurance and began working for the Los Angeles Times where she was employed as an accounts receivable lead. After her second son was born, Tish and her family moved to Northern California where she spent time as a stay-at-home mom before rejoining the workforce in the retail sales field, eventually becoming a sales manager for Macy’s.

Tish returned to insurance in 1983 when she became an operations supervisor at Crum & Forster Personal Insurance. Over the next seven years, Tish supervised various operations units then moved into an underwriting position. When Crum & Forster moved to another state in 1990, Tish went to work for a small, niche-market company, Western Pioneer, as an underwriter. The company was later purchased by the national carrier, Commerce Insurance Group, which was subsequently obtained by MAPFRE Insurance, an international insurance carrier. Tish spent 21 years with the company serving in various rolls from Underwriting Manager to Underwriting Specialist to Compliance Analyst and eventually as Senior Business Analyst.

In 1998, a prior co-worker invited Tish to dinner with some friends who worked in the insurance industry. The “dinner with friends” turned out to be the monthly meeting of Tri-Valley Insurance Professionals, the local association of NAIW. She was so impressed with this group of people that she joined the association immediately. Tish took the CWC course three months later and represented TVIP at the following California Council Meeting. Since then, Tish has served in every elected position in TVIP, chaired numerous committees and been TVIP’s CWC instructor since 2005.

Beyond the local level, Tish has served as the California council’s Education Liaison, Public Relations Chair and two terms as Council Director. She was elected Region VIII Vice President in 2009 and International Secretary in 2013. She has served/chaired committees at every council meeting, regional conference and international convention she’s attended since 2001 and chaired the 2012-13 Mentoring Task Force. Tish also created an educational course, “Leadership Relationships: Building Better Relationships for More Effective Teams”, that she taught at the 2012 Convention in Dallas and at the 2013 Region VIII Conference in Las Vegas. She recently obtained her CLP designation and has been teaching CLP courses at council meetings and regional conferences.

Tish retired from “paid employment” in April of 2012 and she is enjoying spending more time with her family and friends. Retirement also gives her the flexibility to truly focus on the needs and future of IAIP.

**Linda H. Luka**
**CPCU, CIIP, AAI, AINS, AIS, DAE, CISR**
**Secretary**

For the past six years, Linda has been the Agent Education Coordinator at West Bend Mutual Insurance Company. This 120-year-old mutual property and casualty insurance company has allowed her many personal and professional opportunities.

Her duties now include coordinating continuing education classes in the home office as well as off site, using both in-house and outside presenters. Some of these classes qualify for continuing education credits in the eleven states where they conduct business. She is responsible for finding new topics, speakers and then filing new courses for approval, renewing of current courses along with overseeing registering CE credits for all attendees. She is responsible for various specialty producer and agency staff programs. She works with various Office of Commissioners of Insurance, PIA, National Alliance, BIG I and THE Institutes staff.

She began her insurance career as a personal lines typist. She moved on to become one of four data entry specialists for homeowners and inland marine policies. Later, she supervised this unit, until moving into personal lines rating, and then underwriting. She has been a personal lines underwriter for fifteen years, spending sixteen years in commercial lines underwriting. This year marks her thirty eighth year with the company.

Linda has taught many courses for West Bend and her local and council IAIP groups. Topics include Ethics, CLP and Customer Service. She is a certified instructor for the Dynamics of Service for the National Alliance. Her industry designations include, CIIP, DAE, CPCU, AIS, AAI, AINS, CISR and most recently, CLP.
Linda is the charter and founding president of her local association, Kettle Moraine Insurance Professionals. She is part of Wisconsin Council, Region V. Linda competed in her local and council CWC competitions. Linda was the Wisconsin Council Director in 2007 and Region V Vice President in 2011. In 2008, she won the regional Professional Underwriter of the Year award. She was co-winner of the international Insurance Professional of the Year in 2013.

Linda loves to travel having attended eleven council meetings, ten regional meetings and six international conventions. As RVP, she also attended the Region IV conference.

Linda is a past member of Toastmasters International and is currently involved in the Society of Insurance Trainers and Educators, Greater Milwaukee chapter of CPCU and PR chair of Chix 4 a Cause, LTD., a non-profit organization, which helps people fight cancer in the local area. Linda is on the CISR Board of Governors for the National Alliance.

She is active in her church and loves to spend time with her family and travel to Mexico. Talk to her about her beloved Green Bay Packers too! Linda is married to a former insurance underwriter and they have a son, Willy. She will be a Grandma sometime in early July. Her newest goal is to be a cool Grandma.

Brenda Lawhorn
CIC, CPIW, AINS
Region II Vice President

Brenda began her insurance career with Wright & Company in Washington, DC in November of 1987. Her focus has been in Commercial Insurance with an emphasis in international exposures and association coverages. She has a 26-year track record as an Account Manager, Account Executive, Marketing, Sales Representative, Agency Management and Underwriting. She possesses leadership, supervisory, interpersonal, communication and coaching skills.

Brenda is currently the Commercial Lines Insurance Manager in the Servicing Department with Walker & Dunlop, LLC. Her responsibilities include managing the front-end insurance review for Fannie Mae, Freddie Mac and HUD loans. Brenda performs high-end reviews for master policy programs for concentration of risk, limits, deductibles, etc. for borrowers who wish to utilize these programs for their insurance coverage. She assists with the monitoring and supervising of their third-party compliance company for compliance with current lender coverage requirements and coverage waivers for over 4,000 loans. She also assists other members of the Servicing Department, answering their questions regarding procedures and coverage requirements.

Brenda has taught licensing classes for Property and Casualty and Life and Health coverages for the states of Maryland, Virginia and the District of Columbia. She has also taught classes at local, state and regional meetings and conferences for the International Association of Insurance Professionals (IAIP). She has served in all positions in the local DC Chapter and as the State Council Director for the District of Columbia and Maryland for IAIP. She is the Regional Vice President for the 2013 – 2014 term for Region II, comprised of DE, MD, VA, WV and NC. She holds professional memberships in International Association of Insurance Professionals, National Association for Female Executives, Chartered Property & Casualty Underwriter Society, Professional Liability Underwriters Society and National Association of Professional Women.

Donna Varin
AIT, CIIP
Region I Vice President

Donna retired on December 1, 2012 after serving 35½ years with Amica Insurance in Lincoln, Rhode Island. She began her career with Amica as a programmer trainee, and after numerous career ladder promotions, retired with the title of Senior Project Manager. She was responsible for the successful and timely delivery of highly complex and/or large scale IT projects ensuring optimum levels of integrity, performance and reliability.

Donna graduated on the Dean’s List from Rhode Island Junior College with an Associate’s Degree in Computer Science. In 2003, she obtained both the Associate in Information Technology (AIT) and Certified Insurance Industry Professional (CIIP) designations.

Donna joined IAIP in 1998, and is an active member of IAIP of Rhode Island where she has held every office within her local association, as well as chaired just about every committee. She was the Rhode Island Council Director 2003-2004 and was awarded the AAMGA Award in 2011. She has chaired many regional committees and has served on several national committees. On the national level, Donna was a Golden Gavel designee in 2002 and was in the national Winner’s Circle in 2003. She served as alternate to the national nominating committee in 2005 and delegate in 2006.

Donna is currently a member of the Hopkins Hill Fire Department’s ladies Auxiliary. She was active in Cub Scout Pack 1284 Warwick from 1991-1994 and Boy Scout Troop 1284 Warwick from 1994-1996. She was a member of the Project Managers Institute from 2000-2011 and served as the VP of Administration for the Ocean State Chapter in 2004-2005. Over the years, Donna has worked at many Walkathons, participated in the United We Stand Telethon and was on several committees for the local Habitat House.

A Rhode Island native, Donna grew up in Coventry and has resided the last 9 years in Greenville. She has one child, Keith, who is a member of the RI Army National Guard and has served in Kuwait. Donna’s first grandchild, Mason Alexander was born in November. She is a passionate dog lover and is mom to Isis—a Min-Pin, and Simba—a Toy Poodle. In her spare time, she loves to travel, read a good book and crochet.

Brenda graduated on the Dean’s List from Rhode Island Junior College with an Associate’s Degree in Computer Science. In 2003, she obtained both the Associate in Information Technology (AIT) and Certified Insurance Industry Professional (CIIP) designations.
Brenda resides in Waldorf, MD with her husband Chuck and their two spoiled, beloved Golden Retrievers.

Betty Curry  
CPSR, CPIA, CPIW, DAE  
Region III Vice President  

Betty joined IAIP in 1989 and is a charter member of the Insurance Professionals of Collier County. She has held all offices on the local level, serving as the local president three times. Betty was the Florida Council Director from 2011 to 2013 and has taken and taught numerous IAIP classes. Betty is a certified continuing education instructor in the state of Florida and teaches classes for her local association, as well as the Florida council. She has served and chaired numerous committees on the council, regional and national level. Betty has been the recipient of several IAIP awards, including local VIP of the Year, local and council Insurance Professional of the Year, local, council and regional Individual Education Achievement, council Distinguished Service and regional TJ Mims. She is a Founders Circle member of the Insurance Scholarship Foundation of America.

Betty has been in the insurance industry since 1972, starting out as a receptionist. On May 30, 2014 Betty retired as the Operations Manager at Lutgert Insurance, where she oversaw their five offices and 80-plus employees. She states that IAIP was instrumental in her career growth. Betty holds her CPSR, CPIA, CPIW and DAE designations and is a graduate of the State University of New York at Potsdam, and earned a bachelor’s degree in French. During her junior year, she studied in Tours, France.

For many years, Betty has been involved in the American Cancer Society’s Relay for Life, serving as team captain and has served as the co-chair of the local Relay event, which is the largest in Florida. She loves working in her yard, reading and traveling. Betty retired in May and is looking forward to enjoying her free time.

Danny Douglas  
AINS, AIS, API, ACS, CIIP, ACSR  
Region V Vice President  

Danny has been a member of IAIP for six years. He is a member of the Insurance Association of the Ozarks from Springfield, Missouri. Danny has received both the Rookie of the Year award and Insurance Professional of the Year award from his local association. He served as the Missouri Council Director for the 2012-2013 year and as Regional Vice President for the 2013-2014 year. He has served on and chaired many local committees and has served on the National Nominating Committee in 2012. Danny was the chairman of the IAIP President’s Task Force in 2012-2013.

Danny is employed by American National Property and Casualty Company as the manager of the Underwriting Service Operations Transition Unit. In this role, he is responsible for transitioning several existing books of business to a new policy maintenance system. In November 2014, he will celebrate his sixteenth anniversary with ANPAC. Danny holds the AINS, AIS, API, ACS, CIIP, and ACSR designations. He has taken many IAIP courses and has earned his Supervision Certificate and Management Certificate from the Management Development Institute at Missouri State University. Danny serves on the Community Investment Panel of the United Way of the Ozarks and volunteers for various events hosted by Big Brothers / Big Sisters. He serves on the C-Street Zombie Corps Planning Committee, helping plan the annual “Thriller” event in Springfield. In his free time, he enjoys teaching yoga, running, knitting, and travelling.

Miriam A. Rich  
JD, CIIP  
Region IV Vice President  

Miriam A. Rich is Counsel with Hill Fulwider, PC, in Indianapolis, Indiana, where she practices insurance defense and coverage law, retail and transportation industry defense, and is a certified civil mediator.

She is a member of the American, Indiana State, and Indianapolis Bar Associations; DRI; the International Association of Insurance Professionals, for which she will serve on the International Board as Region IV Vice President for the 2014-2106 term; the National Retail and Restaurant Defense Association, for which she is Conference Chairperson for the 2015 Annual Conference, and the National Society of Professional Insurance Investigators, for which she serves as the Indiana Chapter President.

She also enjoys performing in regional musical theatre, singing, arranging, and directing choral music, and spending time with her husband Bill and her dogs.
Beth Walters
AINS, DAE and CIIP
RVP VI Vice President

Beth has been in the insurance industry for 41 years, working in various capacities of the insurance field. She has worked as an assistant to producers and agency principals, as well as worked in the accounting departments of several agencies. She also held a producers license in both Health and Life and Property and Casualty Lines. She worked as a producer for many years. In the recent 23 years, she has worked with a local workers’ compensation insurer in several capacities beginning as underwriter and progressing to position of management. She has held management positions for accounting, underwriting, loss control, and the audit departments and has helped develop procedures for each department. Beth currently holds the position of Senior Vice President, Compliance and Internal Controls. Beth is currently employed and has been for the past 23 years at LUBA Workers’ Comp, a regional WC insurer.

At LUBA, she is responsible for Regulatory Compliance, Forms and Rate filings for Louisiana, Mississippi, Arkansas and Texas. She assists management with annual reports and is responsible for internal controls for procedures in all departments. She has extensive knowledge of rating and regulatory rules, classifications, experience ratings and basic-manual rules in Louisiana and neighboring states. Beth holds AINS, DAE and CIIP designations. She is a member and past president of the Insurance Professionals of Baton Rouge, member of Institute of Internal Auditors, past Council Director, Louisiana IAIP International, a member of Association of Insurance Compliance Professionals, and a member of IAIP International.

Beth has held all offices in IAIP – on the local level, office of State Director on council level and is current RVP Elect for Region VI, IAIP International. She is committed to her personal and professional development and in addition to the already attained designations; she is currently working on her CLP designation and ACP Designation (accreditation program Associations of Insurance Compliance Professionals).

Beth has been a member of IAIP since the 1980s. She did have a break in her membership for a number of years, however rejoined to help her local association when membership dropped in recent years. Beth’s personal interests are reading and spending time with her husband of 41 years, her two daughters and her five grandchildren. She is a member of St. Alphonsus Catholic Church. She participates in local community activities and charitable works and fundraisers such as La. Public Broadcasting, Junior Achievement (work-readiness developing student skills to realize opportunities of work), and St. Jude Research Hospital.

Angie Sullivan
AIC, CPIW
Region VII Vice President

Angie has been in the insurance industry for 22 years, working in various departments and capacities of the insurance field which have developed her professionally and personally. She has worked as a team member and a consultant in insurance agents’ offices. She created, developed, facilitated/trained various educational programs for agents and their team members in a six-state area (WI, MN, ND, SD, IA and NE), as well as operations center employees in the insurance field across the nation. She has worked with various members and leaders of the insurance industry from service levels up to senior vice presidents on personal and professional development and goal setting. Angie has held various leadership roles in IAIP and in the insurance industry. As a member of IAIP she has held every local level office, was a Council Director in Nebraska for two years and is currently the Regional Vice President of Region VII. Angie chaired numerous agency conventions for her company and an number of agent and team member universities, which required setting up food services, hiring keynote speakers, facilitating classes, arranging extra activities such as golf events, and making sure the agenda stays on time and runs smoothly for up to 500 attendees. Angie developed her insurance knowledge through the various courses and designations she has obtained, including AIC designation, four parts of the LUTCF, and four parts of the CPCU. Angie was variable licensed for her company, holding the Series 6 and 63 license from 1998 to 2006 (Federal and State licenses for securities products).

Angie is committed to her personal and professional development through her membership in IAIP and the various classes and workshops she attends each year. In 2011, she participated in the Confidence While Communicating program giving the three-minute speech and a one-minute impromptu, and was well received. Her speech allowed her the opportunity to participate at the various levels of IAIP competition – the local, council, regional and international levels. Angie holds her CPIW and is currently working on her Leadership designation via IAIP’s new leadership courses.

Angie has been a member of NAIW from 1992 to 1999, and then from 2006 until the present time. She left from 1999 to 2006 due to a position change in her employment that required travel, which prevented her from attending the monthly meetings. Angie realized the value of IAIP and therefore once her travels began to slow down and her role changed, she once again became a member. She is active in her community, helping at the “Center for People in Need,” gift wrapping at local stores during the holidays, assists with information sharing for the Lincoln Marathon and the Alzheimer’s walk. Angie is a member at St. Paul United Methodist Church, and has two kids and one granddaughter with a grandson to be here in August of 2015.
Lauri Oakden
CLP
Region VIII Vice President
Working in the risk management industry for 20 years, Lauri has observed and experienced the many changes in the Southwest’s diverse business environment. Careers in the legal and medical communities evolved into management positions in the risk management/insurance fields, including managed care and workers’ compensation.

Lauri’s niche specialty is workers’ compensation. She is a Branch Manager for ICW Group Insurances Companies. Also a licensed casualty and property producer in Nevada, California and Arizona, Lauri participates in various insurance industry professional organizations. She firmly believes that sustaining her membership and active participation in IAIP is an investment in her professional and personal development, and has served IAIP in various local, state and national capacities, including Nevada Council Director and past Regional Vice President of Region VIII, 2012-2013.

An advocate of professional development, continuing education and mentoring, Lauri enjoys sharing her avid interest in the insurance industry through developing, facilitating and conducting workshops, continuing education classes, mentoring activities and speaking engagements to insurance agencies, industry groups, associations and Chambers of Commerce.

Lauri resides in Las Vegas, Nevada. Her local association affiliations are with the Las Vegas Insurance Professionals and Sierra Nevada Insurance Professionals in Reno. Community involvement includes participation in projects that make Nevada a great place to live, promote education and foster resources. In her spare time, she enjoys exploring the back roads of Route 66; ghost towns, Nevada history, National Parks, junking, travel, spending time and adventures with extended family and friends.

Gail Welfringer
CPIW
Region IX Vice President
Gail has been part of the Allstate family for 33 years. She began her career as a part-time file clerk while attending high school and launched her career after graduation. She has enjoyed the vast opportunities offered to her, including operations trainer, underwriter, risk management specialist, and claims adjuster. In 1997, she opened her own “scratch” Allstate agency, which she operated for 10 years prior to her role as a Field Sales Leader. “Owning my agency was clearly the hardest and most rewarding opportunity to date, and for me, it was ‘living the dream.’ The best part of my role as a Sales Leader is that I get to share what worked and more important, what did not work which helps new agents develop and implement plans for running a successful small business.”

Credibility is important in the insurance industry, and with the level of knowledge and integrity Gail brings to her market place, she is considered a strong leader for Allstate’s sales team. Currently, Gail manages the geography of Central Washington and Eastern Oregon (about 1,000 miles on a map) with a total of 29 agency owners, four exclusive financial specialists and 42 sales staff. Her day-to-day routine is to troubleshoot issues with the partnership between Allstate and business owners, agency economics and planning that includes strategic goal setting and education within the agency. Because of her approach to managing her market much like if it were a very large agency, her practical skills and “hands on” approach really allow the agents to spend their time on new business and retention processes. “Because I spend a great deal of my time on the road, it is really important for me to leverage technology so I can respond quickly and efficiently to agency needs. You don’t always have to have the answer, but it is a good idea to always know where to find it.”

Gail has been an active member of the International Association of Insurance Professionals since 1984 and will tell you that back then, it was much more a formal organization and her key to success was jumping in with all she had to be “part” of the association. She learned and developed her skills by the leaders before her. “Dinner arrangements were the best because you got to meet everyone.” Gail completed her CWC in the late 1980s and has competed and won at the state level, regional level and – had it not been for emergency surgery – was well positioned for the 2012 International competition. Her response was, “next time.”

IAIP is such a strong part of who Gail is as a leader that she wants us all to remember that it is important that we all recognize the spirit of what the association has to offer. Everyone comes to the table with a different set of ideas, requirements, expectations and it has been the opportunities working at the local, state and now regional level that have allowed her the opportunity to advance in her career with Allstate. It has also helped her contribute to IAIP in making it stronger as an organization. Gail is the past Washington State Council Director and is excited to represent Regional IX as RVP. Her goals are simple – continue the climb! Her advice to all members: “Get involved. When you put yourself out there, great things happen.” Her theme is “circle the wagons,” because it is power by numbers and when you are challenged it is the strength, the talent and the tenacity of many that helps you succeed.

Born and raised in the Pacific Northwest, Gail is a 50 year resident of Edmonds, Washington. She and her husband are “landscaping junkies.” She enjoys time with family – husband of 25 years, Kevin, and her two boys; Nolan, age 21 – “Go Huskies;” and Dillon, age 18 – “Go Wildcats;” as well as their pride and joy, 5-year-old black lab, Jake.
IAIP 73rd Annual Convention

The International Association of Insurance Professionals’ 73rd Annual Convention kicked off on Thursday, June 5th in San Diego, California with almost 300 members and industry professionals in attendance. Thank you to all of our attendees for your participation and contributions, but special recognition and honor is deserved for this year’s “25 Plus” attendees who have participated in an amazing 25 (and more!) Annual Conventions. Also, we extend a warm welcome to the energetic group of first time attendees or “First Timers”.

The convention was launched with an energized crowd brought to their feet for Judson Liapply’s “Evolution of Dance” segment in the Opening General Session. Judson was thanked for his spectacular presentation with a standing ovation. The excitement continued throughout the convention as attendees had the opportunity to participate in 25 diverse educational workshops and sessions spanning topics on everything from mastering speaking under pressure to hoarding in the insurance industry. An intense pre-convention leadership workshop focused on developing personal action plans with Cheryl Krier leading an exclusive limited-attendance class. A trade show, a lively welcome reception, several networking events, two keynote addresses, three 20-minute spotlight sessions, and a Business Meeting rounded out attendees’ many options for convention participation.

At the Business Meeting, Jane Densch reviewed the IAIP mission, vision, focus and value proposition; highlighting the organization’s greatest accomplishments and ending with an inspiring reminder for us all to savor our ‘moment in time’.

Courses from the Certified Leadership Program were offered, along with topics on social media, ethics, fact gathering, Medicare, problem solving, report and proposal writing, association management, meeting planning, leading change and more. The exhibit hall provided attendees the opportunity to meet with the exhibitors and network. During the Recognition Luncheon, the international award winners were announced as follows:

**Client Service Professional of the Year**
Kristina E. Donaldson, CPCU, CISR, AINS, CPIW, DAE

**Professional Underwriter of the Year**
Samantha DeBates, AIC, AINS, AIS, AU, CPIW, SCLA

**Claims Professional of the Year**
Joyce N. McCutcheon, CCLA, ACLA, SCLA, CPIW

**Insurance Professional of the Year**
Margaret A. Wildi, M.S., CPCU, AIM, AAM, AINS, CIIP, DAE, CPD, CLP

**Risk Management Professional of the Year**
Elizabeth Stillwell

**Rookie of the Year**
Katie Scheuer, CISR

**Confidence While Communicating Speak-Off**
Therease Thompson, AINS, AIS, AIT, MCDBA, MCTS, ITIL, CLP, CIIP

In addition to these awards, scholarship recipients from The National Alliance, The Institutes and International Risk Management Institute were also announced and those in attendance were recognized. Our closing keynote speaker, Jean Gatz, led the Closing General Session with a provocative message on “the success equation”, using our leadership roles to influence others in a positive way, and developing life skills that will take you wherever you want to go. What’s your “wow” factor?

The 2013-2014 Board of Directors were recognized and honored for their inspiring service over the past 12 months. The 2014-2015 Board of Directors were installed during the Closing General Session.

**2014-2015 Board of Directors**

<table>
<thead>
<tr>
<th>Position</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>President</td>
<td>Rosalyn Horton, CIC, CIIP, PIAM</td>
</tr>
<tr>
<td>President Elect</td>
<td>Debra Kuhn, AAI, AIC, AIS, CIIP, DAE, CELS</td>
</tr>
<tr>
<td>Vice President</td>
<td>Tish Riley, CIIP, DAE, CLP</td>
</tr>
<tr>
<td>Secretary</td>
<td>Linda Luka, CPCU, CIIP, AAI, AINS, AIS,</td>
</tr>
<tr>
<td></td>
<td>DAE, CISR</td>
</tr>
<tr>
<td>RVP I</td>
<td>Donna Varin, AIT, CIIP</td>
</tr>
<tr>
<td>RVP II</td>
<td>Brenda Lawhorn, CIC, CPIW, AINS</td>
</tr>
<tr>
<td>RVP III</td>
<td>Betty Curry, CPSR, CPIA, CPIW, DAE</td>
</tr>
<tr>
<td>RVP IV</td>
<td>Miriam Rich, JD, CIIP</td>
</tr>
<tr>
<td>RVP V</td>
<td>Danny Douglas, AINS, AIS, API, ACS, CIIP,</td>
</tr>
<tr>
<td></td>
<td>ACSR</td>
</tr>
<tr>
<td>RVP VI</td>
<td>Beth Walters, AINS, DAE, CIIP</td>
</tr>
<tr>
<td>RVP VII</td>
<td>Angie Sullivan, AIC, CPIW</td>
</tr>
<tr>
<td>RVP VIII</td>
<td>Lauri Oakden, CLP</td>
</tr>
<tr>
<td>RVP IX</td>
<td>Gail Welfringer, CPIW</td>
</tr>
</tbody>
</table>

The International Association of Insurance Professionals extends our heartfelt thanks to all of our convention exhibitors, attendees, presenters, sponsors and guests – without each of whom this event would not have been such a success. Please mark your calendars now to join us in Minneapolis, Minnesota on June 4-6, 2015 for yet another fun, successful and rewarding convention where we will continue to Connect Members and Build Careers.
2014 International Award Winners

**CLIENT SERVICE PROFESSIONAL OF THE YEAR**
Kristina E. Donaldson
CPCU, CISR, AINS, CPIW, DAE
Region VI

**CLAIMS PROFESSIONAL OF THE YEAR**
Sara Arman accepting on behalf of Joyce N. McCutcheon, CCLA, ACLA, SCLA, CPIW
Region I

**RISK MANAGEMENT PROFESSIONAL OF THE YEAR**
Elizabeth Stillwell
Region I

**CONFIDENCE WHILE COMMUNICATING SPEAK-OFF**
Therease Thompson
AINS, AIS, AIT, MCDBA, MCTS, ITIL, CLP, CIIP
Region V

**PROFESSIONAL UNDERWRITER OF THE YEAR**
Jennifer Christensen, CISR, CIC, CRM, CRIS, CPIW accepting on behalf of Samantha DeBates AIC, AINS, AIS, AU, CPIW, SCLA
Region V

**INSURANCE PROFESSIONAL OF THE YEAR**
Margaret A. Wildi
M.S., CPCU, AIM, AAM, AINS, CIIP, DAE, CPD, CLP
Region IV

**ROOKIE OF THE YEAR**
Katie Scheuer
CISR
Region V
Convention Candids
The LAST LINE

**Insurance Association of Suburban Kansas City** recently made changes in an effort to attract new members by planning every other association meeting as a business luncheon and including more Continuing Education opportunities. Not only did our member attendance increase but we had several new guests attend as well. Growth in our local membership is a direct result of these improvements.

Martha Elliott
Kansas Region VII
Insurance Association of Suburban Kansas City

---

Mary Nesman, a 50 year charter member of Greater Lansing Insurance Professionals, is celebrating her 50th anniversary with IAIP.

L. Jane Densch
Region VII
Denver Association of Insurance Professionals & Cindy Prud’homme
Region IV
Mid-Michigan Association Insurance Professionals

---

**Melanie Elias Speaks on Handling Insurance Fraud Claims**

Melanie Elias was promoted to Corporate Associate Vice President, Minuteman and recently attended the 15th Annual Worley Claims Expo. Melanie spoke with Mathew Monson, J.D. on the topic of Handling Insurance Fraud Claims. The session was 50 minutes for each speaker and the course was approved for General CE in AR, FL, LA, MS, OK, TX, and AL.

Melanie M. Elias
Region IV
Insurance Association of Metropolitan Detroit

---

**I have added another designation to my name. R-E-T-I-R-E-D!** On March 16th I concluded 22 years as a Field Underwriter/Trainer with AGCS Marine Insurance (a division of Allianz Global). With my upcoming term as President of the Association, I will be quite busy in assisting the board and all our members in moving the association into a greater presence in the insurance industry. We will do this by ‘connecting members’, across diverse lines of insurance, and assisting everyone whom we come in contact with to ‘build careers’ that fulfill their lives.

rosalyn horton
Region III
Tennessee Member-At-Large

---

**“Our local association, Kettle Moraine Insurance Professionals, has held five CLP classes** on Saturdays over this long winter season. We averaged ten attendees, learned a lot, had fun sharing experiences and got to know each other a bit better too. (Update: as of 5/19/14 KMIP has offered 13 of the 17 CLP classes for its members!)

Linda Luka
Region V
Kettle Moraine Insurance Professionals

---

Suellen Unzicker-Kelley was awarded The Florene Briley Award of Excellence at Industry Appreciation Night in February 2014. Mrs. Briley has been a member of our association for over 50 years. This award was established by Deb McCurdy to honor Mrs. Briley for her dedication and commitment to the industry. We are very proud of Suellen and blessed to call her member and friend.

Janis Hart
Region III
Greater Montgomery Insurance Professionals

---

**Congratulations to the Region VI award winners:**

- **Rookie of the Year** - Brittany Davis
- **Insurance Professional of the Year** - Shelly S. Power, CISR, CPIW, AIS, DAE
- **Client Service Professional of the Year** - Kristina E. Donaldson, CP CU, CISR, AINS, CPIW, DAE
- **CWC Winner** - Joycelyn M. Peer, CIC, CPIW, DAE

Sonya Embry
Region VI
Insurance Professionals of Tulsa

---

Cherri Harris was recently promoted. Her employer cited her growth through IAIP as contributing to that.

Cindy Prud’homme
Region IV
Mid-Michigan Association Insurance Professionals

---

After 40 plus years in the insurance field I am retiring May 1st! I will continue being an active member in IAIP. We will enjoy traveling to visit the grandchildren and great grandchildren.

Betty Watson
Region VIII
Valley of the Sun Insurance Professionals

---

**“Our local association, Kettle Moraine Insurance Professionals, has held five CLP classes”**

---

**Suellen Unzicker-Kelley was awarded The Florene Briley Award of Excellence at Industry Appreciation Night in February 2014. Mrs. Briley has been a member of our association for over 50 years. This award was established by Deb McCurdy to honor Mrs. Briley for her dedication and commitment to the industry. We are very proud of Suellen and blessed to call her member and friend.**

Janis Hart
Region III
Greater Montgomery Insurance Professionals
DEVELOP YOUR INNER LEADER

Certified Leadership Program
Develop essential leadership skills for career enhancement

“The Certified Leadership Professional program is a solid, professional development series that cannot be matched by any other. The skills of Managing, Mentoring, and Motivating are essential to career development which leads to our personal and professional success. It is a clear choice for ‘managers’ and it should not be overlooked by those who feel that it is not applicable in their individual roles. To consider ourselves as professionals, we must also recognize the importance of focusing on constantly seeking ways to grow our leadership skills.”

Angelia Poyner, CIC, CPIA, KACSR, CLP and IAIP Member

Insurance Professionals’ Certified Leadership Program provides individuals with a premier learning program consisting of four modules encompassing seventeen courses. Individuals completing the entire program are eligible to apply for the Certified Leadership Professional (CLP) designation.

Certified Leadership Professional (CLP) Designation
Applicants must renew their designation every two years by taking an 8 hour update class.

New designee requirements:
Must complete entire leadership education program.

Renewal requirements for existing designee:
Must complete 8 hour designation update class.

Learn more under Education - Course Offerings at www.insuranceprofessionals.org
The Legacy Foundation was formed in 2006 as the philanthropic arm of the International Association of Insurance Professionals, best known for providing insurance education, skills enhancement and leadership development to its members. Make a contribution by mail or online at:

Legacy Foundation • 3525 Piedmont Road • Building Five, Suite 300 • Atlanta, GA 30305
or visit www.internationalinsuranceprofessionals.org

The NAIW (International) Legacy Foundation is an IRS approved 501(c)3 foundation. Contributions to the NAIW (International) Legacy Foundation are tax deductible as a charitable contribution.