BOARD OF DIRECTORS

International President: Jane Densch, CPCU, AIC, ARe, ARP, AIS, CPIW, 11460 Marks Dr., Conifer, CO 80433, jane.densch@me.com

International President-Elect: Roz Horton, CIC, CIIP, DAE, PIAM, AGCS, Marine Insurance Company, 2021 Greenwood Avenue, Nashville, TN 37206, rosalyn.horton@yahoo.com

International Vice President: Debra Kuhne, AA1, AIC, AIS, CIIP, DAE, CELS, The Litchfield Insurance Group, 126 South Main Street, Torrington, CT 06790, dkuhne.iapip@yahoo.com

International Secretary: Tish Riley, CIIP, DAE, 591 North Alpine Road, Stockton, CA 95215, tish4iap@gmail.com

Region I Vice President: Donna Varin, AIT, CIIP, 3 Fair Oaks Ct. N., Greenville, RI 02828, r1rvpdonna@yahoo.com

Region II Vice President: Brenda Lawhorn, CIC, CPIW, AINS, Walker & Dunlop, LLC, 7501 Wisconsin Avenue, Suite 1200E, Bethesda, MD 20814-6531, blawhorn@walkerundunlop.com

Region III Vice President: Betty Curry, CPSR, CPIA, CIIP, DAE, Lutgert Insurance, 1395 Panther Lane, Suite 100, Naples, FL 34109, bcurry@lutgertinsurance.com

Region IV Vice President: Cindy Prud’homme, AINS, CPIA, CIIP, Meadowbrook Insurance Group, 3181 McGregor St., Grand Blanc, MI 48439-8138, Cindy.Prudhomme@Meadowbrook.com

Region V Vice President: Danny Douglas, AINS, AIS, API, ACS, CIIP, American National Property & Casualty, 1949 E. Sunshine, Springfield, MO 65899, dddouglas@anpac.com

Region VI Vice President: Sonya Embry, CISR, CPIW, DAE, Mid-Continent Group, P. O. Box 1409, Tulsa, OK 74101-1409, sembry@mcg-ins.com

Region VII Vice President: Angie Sullivan, AIC, CPIW, State Farm Insurance, 222 South 84th, Lincoln, NE 68501-2542, angie.sullivan.c4u9@statefarm.com

Region VIII Vice President: Katharine Nohr, J.D., Law Offices of Katharine M. Nohr, LLC, 46-001 Kamehameha Hwy, Suite 306, Kaneohe, HI 96744, katharintg@aol.com

Region IX Vice President: Gail Welfringer, CPIW, Allstate Insurance Company, 18911 North Creek Parkway, Bothell, WA 98011, gail.welfringer@allstate.com

Display advertising is available. For more information on rates and ad requirements, call 1-800-766-6249 ext. 20. The ad closing date for the Fall 2013 issue is August 30, 2013.
## CONTENTS

### FEATURES

<table>
<thead>
<tr>
<th>Page</th>
<th>Title</th>
<th>By</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Corporate Crime: Know Your Client to Limit the Risk</td>
<td>Timothy E. Horton, J.D.</td>
</tr>
<tr>
<td>8</td>
<td>Small Businesses Must Be Proactive in Protecting Against Cyber Theft</td>
<td>Marc Kramer</td>
</tr>
<tr>
<td>12</td>
<td>The New Breed of “Fraudsters”</td>
<td>Bruno Pavlicek</td>
</tr>
<tr>
<td>16</td>
<td>Follow the Money: Prevent Embezzlement</td>
<td>Rhonda R. Savage, DDS</td>
</tr>
<tr>
<td>18</td>
<td>How to Handle Embezzlement in the Family Business</td>
<td>Lois Lang, Psy.D.</td>
</tr>
<tr>
<td>26</td>
<td>Plan Ahead for Your “Online Hereafter” -- Steps to Take Now to Avoid Being the Victim of Fraud After Death</td>
<td>Hillel L. Presser, Esq., MBA</td>
</tr>
<tr>
<td>30</td>
<td>Three Keys to Successful Crisis Management</td>
<td>Lucien Canton</td>
</tr>
</tbody>
</table>

### COLUMNS

<table>
<thead>
<tr>
<th>Page</th>
<th>Title</th>
<th>By</th>
</tr>
</thead>
<tbody>
<tr>
<td>23</td>
<td>At Issue How to Protect Yourself from Identity Theft</td>
<td>Brandpoint</td>
</tr>
<tr>
<td>24</td>
<td>Business Column Insurer Trends Center on Technology</td>
<td>Jared Wade</td>
</tr>
<tr>
<td>29</td>
<td>Technology Tips Cyber What?</td>
<td>Emily Holbrook</td>
</tr>
<tr>
<td>33</td>
<td>Guest Column Question &amp; Answer: Cloud Security</td>
<td>Emily Holbrook</td>
</tr>
<tr>
<td>38</td>
<td>Editor’s Note</td>
<td></td>
</tr>
<tr>
<td>46</td>
<td>72nd Annual Convention Review</td>
<td></td>
</tr>
<tr>
<td>50</td>
<td>International Award Winners</td>
<td></td>
</tr>
<tr>
<td>51</td>
<td>Corporate Partners</td>
<td></td>
</tr>
</tbody>
</table>

### ASSOCIATION NEWS

<table>
<thead>
<tr>
<th>Page</th>
<th>Title</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>2012-2013 President’s Message</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>2013-2014 President’s Message</td>
<td></td>
</tr>
<tr>
<td>36</td>
<td>Insurance Scholarship Foundation of America</td>
<td></td>
</tr>
<tr>
<td>37</td>
<td>Welcome New Members</td>
<td></td>
</tr>
<tr>
<td>38</td>
<td>New CPIWs and CIIPs</td>
<td></td>
</tr>
<tr>
<td>46</td>
<td>2013-2014 Board of Directors</td>
<td></td>
</tr>
<tr>
<td>50</td>
<td>International Award Winners</td>
<td></td>
</tr>
</tbody>
</table>

Photo credit: Seqoya/Shutterstock.com
The quote “Time flies when you are having fun” is so true of this year. As I look back on the 2012-2013 term I can say that your Board of Directors worked hard this past year.

Goals were set for each level of the leadership team. The Executive Committee, Regional Vice Presidents, Council Directors and Local Presidents accepted the goals and many were met. We had 14 local associations that reached the 10% growth in membership along with the other 4 goals that were set for them. Thank you for all who achieved what you set out to do.

Last year, there were several task force committees that were developed to help come up with strategic plans to help the local associations. The committees included Education, Mentoring, Marketing, Communication, Officer Transition, Young and New Professionals, along with two new ones. The Convention Review and the President’s Challenge continued this year and held several telephone conference calls and met at the regional conferences. The information from each committee has been shared in the Connections and on our website. Please take a few minutes to read the reports as there is a wealth of tips and tools to help you.

The Certified Leadership Program and the CLP designation were launched in January 2013. This program was developed for IAIP members and was sponsored by the NAIW Legacy Foundation.

Just a few other things that your Board of Directors worked on this year: we approved a new award -- the Client Service Award; improved communications with Link to the Leadership Team and the monthly Connections; set up the iConnect online community; reviewed and updated education programs; rebranded with the new logo and tagline; reviewed all forms, manuals and bylaws; implemented the changes that were voted on in the 2011-2012 term; and improved IAIP finances by the sale of the building and cutting expenses.

We are all truly passionate about our association and the past few years has had some changes that are hard to accept, however, we must see what is best for the association as a whole and not just for one person, or local, council or region.

Thank you for keeping an open mind to change as we move this association forward by....

..... Connecting Members...Building Careers.

In fellowship,

Penny Haworth-Rich
AU, CIC, CPIW, DAE
2012-2013 International President
2013-2014 President’s Message

I just returned from the 72nd Annual Convention of the International Association of Insurance Professionals, which was held June 6-8 in Orlando. The educational and networking activities were exceptional. Topics included Risk Management, Ethics, Going Green, Rental Reimbursement, Protecting Data, Workplace Flexibility, Personal Strategies to Accomplish More, and Taking Charge of Your Career. Several courses from the new Certified Leadership Program were offered, including Coaching, Business Leadership, Team Building and Delegation. Erick Burton’s keynote address on Future Leaders impacted all in attendance, as he urged everyone to think BIG and overcome their fears.

The first two Certified Leadership Professionals were recognized, along with the new CIIP, CPIW, CPIM and DAE designees. Check out the winners of the IAIP awards further in this magazine! Members who qualify should plan to apply for the Client Services Professional of the Year, which is new this year.

This issue of Today’s Insurance Professionals is another educational source for our members. Crime in the Workplace is a relevant focus for all within the insurance industry. It’s a risk that our clients want to insure and manage and one that we all want to avoid whenever possible. The articles emphasize what everyone should know about this misconduct.

Insurance Professionals continues to provide educational and leadership training and opportunities to its ever expanding membership throughout the coming year. Start making plans to attend the 73rd IAIP Convention in June 2014 in San Diego.

Join us in...

... Connecting Members...Building Careers.

Jane Densch
CPCU, AIC, ARe, ARP, AIS, CPIW
2013-2014 International President
Editor’s Note

We hope we never have to deal with criminals anywhere, and especially not in the workplace. We assume that professionals who are hired to work for an organization are honest, upright citizens, and most are. But a few aren’t, as we’re learning everyday when we watch the news.

I’m always shocked to turn on the television news or pick up a newspaper and see the pictures of people who probably were good citizens at some point in their lives but turned to crime and stole from their employers. They look like people you would see in living in your neighborhood, going to your school functions, at your grocery store. There is not one obvious thing about their appearance or their personality that makes them appear to be criminals.

I have known some of these people in my community who were embezzlers and got away with it for years before being discovered. In each instance, I thought these were exceptionally nice people who were honest, hard-working individuals with the highest integrity. After they were discovered, they went off to their deserved punishment and the people close to them were left to deal with the feelings of betrayal, hurt, anger and astonishment. The company that had the financial loss had to deal with it and cut back in other areas to make up for the shortage.

Sometimes the victim went to prison, but other times, it was kept quiet and only family and friends found out about it. But there are consequences for those criminals, too, because they lose their job, lose their spouse and children, and lose their family’s respect.

This issue of Today’s Insurance Professionals tackles the tough subject of recognizing when a criminal is in your business and what to do when you discover them. It also gives you advice for how to make sure your company doesn’t fall victim to these types of people by putting safeguards in place. And, if your company does have to deal with criminal wrongdoing, we explain how you should handle getting the message out to your stakeholders and the media.

Also in this issue, the International Association of Insurance Professionals is celebrating another successful annual convention. This issue has information about the new Board of Directors, the International Award Winners, our new association members and those who have worked hard to achieve the CPIW and CIIP designations.

Please take time to read this magazine, as well as check out the IAIP Website, Linked In and Face-book pages, where we provide you with information that will help you in your career as an insurance professional.

Sincerely,

Sharon Smith
Managing Editor
My own interest in corporate crime did not originate by watching news accounts of the Enron or Madoff scandals. Rather, corporate crime (and what we can do to limit the risks associated with it) first started to pique my interest years ago when I learned that my family’s favorite neighborhood restaurant was the victim of insider theft by a trusted, long-time employee that rose through the ranks from a waitress to the position of part-time bookkeeper.

Over the course of two years, the employee stole nearly $200,000 by taking cash from the restaurant’s daily deposits and then depositing one of the restaurant’s own checks in the same amount of the stolen cash into the restaurant’s bank account. Even though the restaurant’s own checks were making up much of the daily deposits, the crime went unnoticed because the bank did not routinely send its customers copies of the deposit slips or checks that make up the deposits.
Feature

The office manager noticed that it was one of their own checks and started an internal investigation, which revealed the fraud. Thankfully for the restaurant, the police were able to recover most of the stolen funds.

Most victims of corporate crime are not so lucky. Particularly in the wake of the recent economic downturn, people seem more willing to take the “easy” way to making ends meet. And this reality is not likely to change anytime soon. This incident got me thinking: Who persecutes these types of crimes? How do you catch it? How do we prevent it?

I have represented numerous companies—big and small—that have been impacted by corporate fraud. Through those experiences, and with the help of hindsight, this article will offer some useful tips on how insurance professionals can work with clients to prevent, or at least limit, the damage to clients and resulting insurance claims caused by corporate crime.

TRUST BUT VERIFY

One of President Ronald Reagan’s most often repeated phrases was “trust but verify.” Of course, President Reagan was referring to verification that the Soviet Union was living up to its nuclear arms reduction commitments. While most of us are not concerned with high level matters of State, the phrase nonetheless applies very well when considering insuring or investing in a business.

I represent a closely held manufacturing company. About a year ago, the client noticed a few payroll discrepancies. After a short investigation, we discovered that the company’s payroll manager was writing himself an extra paycheck once every couple of pay periods. By the time my client discovered the fraud, the employee had written himself about $800,000.00 worth of extra checks. Adding to the nightmare involved in recovering the stolen funds, the employee had sent the majority of the stolen money to a “girlfriend” in South America.

Although the payroll manager was indicted and eventually pleaded guilty to the crimes, my client lost hundreds of thousands of dollars. Considering the circumstances, they were fortunate to recover even part of the amount stolen.

I know what you are thinking: “The CFO that was in charge of the payroll manager must have been asleep at the switch.” Or, “This would never happen to the companies I work with or the companies I insure.” In reality, this particular CFO is one of the most conscientious business persons that I have come across in my practice. If it could happen to her, it could happen to anyone. So, what can we learn from this misfortune?

First, we should insist that clients/insured/investment partners have systems in place to verify that the people they trust are doing the right things. In this instance, a simple random check of the number of checks cut each week would have caught the thief very early in the process. An insurance provider might suggest oversight systems for companies’ accounting departments. Routine audits of accounting departments that target vulnerable areas, such as the number of checks cut each week and the source of deposited funds, should be standard operating procedure for companies. If your clients do not have such audit mechanisms in place, you might suggest such procedures (or adjust rates accordingly).

In my experience, broad, general audit policies and procedures are better than targeted audits because individual employees are less likely to feel threatened or singled out by the policies. Employees are less likely to feel threatened or singled out by the policies.

INSIST UPON OVERSIGHT AND ETHICS TRAINING

Of course, corporate crime does not always involve stealing money. Often the theft is of material or goods. We represent a company that melts aluminum scrap for die cast products that was the victim of a theft of aluminum scrap by an organized group of trusted employees who knew exactly how to get around all of the systems that the company had in place to prevent this type of theft. Over a three-year period, one box at a time, the company’s employees stole over $1 million worth of scrap metal.

The three employees who perpetrated the scheme were systematic and careful. They also knew exactly how to avoid detection. One of the employees would separate and set aside the scrap material to facilitate quicker loading onto the “get away” truck at the end of the night. This same employee also arranged all of the daily work activity at the plant so that he could move workers away from the loading area at the time the thefts were occurring. These employees would even shut off certain electricity supplies throughout the plant to disable the security cameras in the area of the theft. The employees would then load the stolen material into a truck that just made a delivery and take it away. The employees also falsified company records so that the company would think that the stolen aluminum had been melted for proper usage.

Despite security cameras and review of smelting reports, these employees were able to perpetrate this scheme for three years without detection. They were only discovered because one night an employee (who was not involved) happened to come back to the plant unexpectedly and noticed the employees loading boxes of aluminum scrap into a truck that normally delivers aluminum scrap. That employee went to his superiors and an investigation commenced that discovered the crime.

So again, what can we learn? This particular case presents interesting issues because the employees were stealing such small amounts of aluminum each time that they fell into the acceptable “waste” rate that the company might not notice as missing. That said, more regular checks of the amounts of product used and regular audits of the cameras might have discovered this crime sooner and, thereby, limited the damage to the company.
Here, the company did have systems in place to prevent and/or catch perpetrators of crime. But the employees knew how to get around the systems and knew that the security systems were, more or less, window dressing. The employees knew that the company did not check their security camera tape and would not notice chunks of time missing from the tapes. Indeed, a simple random but frequent audit of the security tape would have exposed the lapses in the tapes during the “power outages.” Therefore, we must not only encourage our clients to have programs in place that are designed to curtail crime, but we must also insist that our clients properly utilize and audit those systems and procedures.

In terms of how to best prevent these types of crimes from happening in the first place (and without casting any ethical dispensations upon any victim of crime, much less the stories I’ve recounted here) I think the answer is two-fold. First, there are practical solutions such as audits and oversight discussed earlier. But the real answer to prevention might be more esoteric – ethics in the workplace. Simply put, we should encourage our clients to act ethically in all that they do. It is no coincidence that business schools are now being ranked on “ethics” programs. It is my belief that ethics within organizations start from the top down. If the top tier of an organization is close to “the ethical line,” the average employee will notice that behavior and it will influence decisions that they make.

Leaders of organizations make numerous decisions throughout each work day. Usually, the decision maker has the option to take different paths – one path may be ethical/legal and the other may not be. Leaders that choose the ethical/legal path, even in the face of an attractive other option, will be noticed by the rank and file employees. And I posit that those employees will be more likely to make the same kinds of choices in the decisions they face daily in the workplace.

In order to foster a more ethical workplace, we should encourage our clients to conduct periodic ethics training at work. This can take the form of mock decision making seminars or online decision making training. Short of formal training, we can encourage our clients to ask the following questions as they make decisions:

1. How would you define the problem if you stood on the other side of the fence?  
2. What is your intention in making this decision?  
3. Whom could your decision or action injure?  
4. Are you confident that your decision will be as valid over a long period of time as it seems now?  
5. Could you disclose without qualm your decision or action to your boss, your CEO, the board of directors, your family, society as a whole?

Clients may be surprised how the decisions of top leadership filter down to all the employees within an organization.

**KNOW YOUR CLIENT**

Perhaps the most important thing we can do to help limit our risk is to get to know our client’s business and industry. By “know” I mean really spend the time to understand what clients do and how they do it. Get on the ground, take a look around. Have meetings in your client’s office so that you can get a feel for the place.

I have heard CEOs of major corporations give speeches across the country on various topics, and a common thread among the most successful CEOs seems to be that they have a deep and comprehensive understanding of their company’s business.

Speaking around the time of the MCI/WorldCom bankruptcy, the then-chairman of (competitor) AT&T said something very interesting. Basically, that he knows his company so well that he knows how much everything costs. His point was that as the person in charge, he should know the cost of even the smallest line items in his budget to better understand the workings of his company and understand or ferret out potential problems or discrepancies. While we probably cannot know our clients’ industries that well, we should strive to understand our clients’ businesses as well as we can.

For example, if you know that your client deals in scrap metal, and you know that there is a certain amount of scrap that is “wasted” each day, you can work with your client to develop procedures to ensure that the company’s employees are not taking advantage of that particular vulnerability. Getting to know your client will only enable you to serve them better, and you might be able to limit some of the risk associated with corporate malfeasance at the same time.

In summary, in order to limit the risk of corporate crime, encourage your clients to put policies in place that are designed to verify that their employees are doing what they are supposed to do. Encourage your clients to make the oversight policy broad so that individual employees do not feel targeted. Encourage your clients to actually use the policies/tools that are in place on a regular basis. (If they have a security camera, check the tapes!) Get to know your client’s business so that you can make individualized suggestions for that particular business. Finally, encourage your clients to act ethically. Their employees will notice their good behavior and likely follow suit.

**Photo credit:** Wollertz/Shutterstock.com

---

Timothy E. Horton is a partner in the litigation practice at the law firm of Ungaretti & Harris LLP. He focuses his practice on internal investigations, securities litigation and complex commercial disputes.
If anything, the Federal Deposit Insurance Corp. (FDIC) has done too good of a job in assuring bank customers that their assets are safe.

News about cyber thefts isn’t particularly rare, but 77 percent of small businesses don’t believe an attack will happen to them – and figure the FDIC (or their bank) will protect them in case the unimaginable does happen.

That’s a big mistake based on misinformation.

The truth is, the FDIC only covers bank accounts against the bank going out of business. And second (and perhaps more importantly), while banks are obligated to cover losses to personal accounts, the same is not true for business accounts.

Here are some frightening statistics:

● At a March hearing, U.S. Rep. Chris
By Marc Kramer

Collins (R., N.Y.) cited a recent study showing that “nearly 60 percent of small businesses will close within six months of a cyber-attack.”

- Bloomberg has reported that more than $1 billion is stolen annually from bank accounts.
- In 73 percent of those cases, money gets transferred, according to a joint study by Guardian Analytics and Ponemon Institute. In 61 percent of the attacks, money was lost.
- The average annual cost of cyber attacks on small- and medium-sized businesses is $188,242, which is hardly chump change. Yet 77 percent of small businesses don’t believe an attack will happen to them.

Not convinced? Here are stories from a couple of victims, the firm of whom now speaks publicly about ways to prevent cyber theft.

Ann Talbot, the chief financial officer of engineering and construction company Golden State Bridge, Inc., of Martinez, Calif., has twice seen her company victimized by cyber theft.

In 2006, someone reached into the company’s bank account, established a wire and sent about $100,000 to the Philippines. Golden State Bridge was able to claw back about $70,000, but the perpetrator never was caught. Talbot believes the breach happened on the bank side, which the bank denied, even though the breach occurred in a building across the street from the bank. Talbot’s login and password were used to make the theft.

A second incident occurred in May 2010, involved a different bank and likely involved a breach in Golden State Bridge’s system. The login and password of the company’s office manager were used to make the theft. Talbot believes it happened on Facebook, as someone was able to load a “Zeus” keylogger virus and waited until she entered the bank account.

The company initially lost about $125,000, but was able to pull back $30,000. A blanket business policy covered the rest.

Then there’s Philadelphia-area chiropractor Kevin Kita who was twice victimized, but isn’t sure exactly how. Both times, however, he was left in the lurch while the cybercrime was under investigation. While he could deposit money, he couldn’t withdraw any or pay bills, considering he had what appeared to the bank to be a large deficit.

Luckily for Kita, his bank eventually did reimburse him, but you can’t count on that.

Sure, complain to a bank long enough and it might partially reimburse you or,
if you’re really lucky, make your account whole. But that’s needlessly risky.

Furthermore, there’s no guarantee of anything, and you might spend a few weeks with your account locked down. In the meantime, it might be impossible for you to meet payroll or pay vendors, stop checks from bouncing and even prevent loans from possibly being called in because you are out of covenants.

In essence, you’ll largely be out of business for a while.

Obviously, you must project yourself. The question is how?

The most important thing is to not turn a blind eye. Real problems require proactive responses.

Many of these cyber-thieves are from Eastern Europe and the Middle East and know how to stay one step ahead of the authorities. They specialize in what’s called a corporate account takeover -- they create fake accounts and, via the Internet, inch into a bank’s computer records. Then they transfer millions, often in small amounts, to untraceable accounts.

Your first step is to consider dual computer systems. Have one dedicated solely for banking, with the other for the rest of the company operations.

Next, authenticate everything with your bank, especially anything that’s even remotely suspicious. Hackers often start small as a test run. It might seem fool hearted and a waste of time to check out a 27-cent transfer, but it could be a precursor to a $27,000 withdrawal.

Third, buy insurance.

Yes, we know buying insurance isn’t fun and there always seems to be a better or more pressing need for company funds. And yes, you probably already have some or all of the following insurance – general liability; errors and omissions; auto; worker’s compensation; employment practices liability; and commercial excess liability.

However, none of them typically cover cyber theft.

Some offer the coverage as part of a rider on other policies, but you also may buy specific cyber theft protection.

Those specific policies generally aren’t expensive and offer a simple path toward peace of mind. It doesn’t take long to buy. You can learn more about this coverage and bank account cyber theft by visiting www.cdiaus.com.

Next we come to the standard suggestions for safer Web use. Most are common knowledge by now, but it never hurts to review them:

● Turn off your computer when it’s not in use. This limits access.

● Develop strong passwords instead of “12345” or “password.” At least make it tough for cyber thieves.

● Back up your data. This should go without saying.

● Keep your firewall on.

● Install or update your antivirus software. Try to stay up with the bad guys.

● Install or update your antispyware technology.

● Keep your operating system up to date. Older systems are easier to hack.

● Be careful with what you download, especially if you don’t know the sender. Use common sense.

German playwright Bertolt Brecht lived in the days before computers, but nearly 60 years after his death, his quote rings true: “You don’t need to pray to God any more when there are storms in the sky, but you do have to be insured.”

Marc Kramer is the co-founder of Commercial Deposit Insurance Agency, Inc. (www.cdiaus.com) of Radnor, PA. CDIA is backed by two AM Best “A”-rated insurance companies to provide insurance to business, non-profit and trust bank accounts against cyber theft.

Photo credit: Andrey_Popov/Shutterstock.com

Today, those storms in the sky – maybe he was referring to “the cloud” – surface as someone who may be continents away, but is looking to metaphorically rain down thunder and lightning on your business.

Be safe, which means being smart. At bare minimum, take a proactive approach to cyber security. Better yet, buy insurance protection. Don’t become a statistic.
Certified Leadership Program

Insurance Professionals’ Certified Leadership Program provides individuals a premier learning program to develop essential leadership skills for career development. The program consists of 4 modules encompassing 17 course topics.

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 have current active membership in Insurance Professionals.
• Must complete entire Leadership education program.

Renewal requirements for existing designee:
• Must maintain continuous active membership.
• Must complete 8 hr. designation update class.

Learn more under Education - Course Offerings at www.insuranceprofessionals.org
By: Bruno Pavlicek

The term “white collar crime” was coined by sociologist Edwin Sutherland in 1939. It was meant to describe a crime committed by a person of respectability, high social status and in the course of one’s occupation. In recent years, as major scandals have unfolded — Enron, Worldcom, Tyco, subprime mortgage fraud — white collar crime has become elevated in the public’s conscious. Then, federal investigators uncovered one diabolical con to trump them all.

The massive Ponzi scheme orchestrated by disgraced stockbroker Bernie Madoff...
That may no longer be the case. As more thieves like Madoff are discovered, it seems we are seeing a new, harsher, more deviant brand of white collar criminal.

Donald R. Cressey is one of the most renowned theorists on occupational fraud. He started out as a doctoral student of the legendary sociologist Edwin Sutherland, who literally re-wrote the book on criminology when his aptly named work, *Criminology*, was published in 1924. Like his mentor, Cressey moved on to study white collar criminals during the 1940’s and developed a hypothesis that would influence everyone who has researched workplace fraud since.

Cressey’s study of embezzlement matured into what became referred to as “the fraud triangle,” which describes three factors that must be in place for workplace fraud to occur: pressure, opportunity and rationalization.

In terms of pressure, fraudsters would violate the trust of their employers when faced with personal problems that led them to misappropriate their company’s assets as a solution. In more common terms, one would describe this as the motive behind the crime.

This pressure could be created by other desires as well — revenge against the employer being a common example. In such situations, the offender psychologically displaces blame for his actions onto the employer — or perhaps a coworker — and the company, in their mind, becomes the cause of their behavior. The opportunity aspect is simple enough: a fraudster must be able to capitalize upon a chance to engage in theft. Such opportunities generally happen when there is a loss or breakdown with an organization’s internal controls.

The third and final factor that must be present in Cressey’s fraud triangle model is the act of rationalization. This occurs before the theft, wherein the employee looks upon themselves as being a good person and not as a criminal. In essence, before committing fraud, an offender must overcome the psychological hurdle...
that the negative act in and of itself presents for them. They do this by justifying it first within their own minds, where the act becomes more of a way out of a problem or a justifiable act of retribution than a crime.

Although it has long been studied and held up as an accurate description of white collar crime, Joseph Wells of the Association of Certified Fraud Examiners believes the fraud triangle model no longer reflects current times. Researchers such as Cressey have led us to believe that occupational fraud offenders are people who possess a sense of morals, and therefore need to rationalize their criminal acts before committing them. But Wells says that society has changed over the decades. Looking at many of the fraud cases we have seen in recent years, it is hard to disagree.

With criminals like Bernie Madoff being thrust into the public eye, a new view of fraud is emerging. It is one in which occupational offenders operate without any moral compass in life. They feel no need for self-rationalization in their actions.

Instead, they act with self-perceived impunity in the face of all regulations or laws in place to deter such activity. These offenders possess deviant personality traits that represent unorthodox profiles compared to the traditional criminal profiles of the corporate embezzlers before them.

Some employees today do not steal because of need or even revenge; they steal simply because of opportunity and have very little fear of discovery. More than that, they steal no matter what an employer does.

This category of employees is described as dishonest, manipulative and lacking integrity. These truly bad-to-the-core employees have a tremendous need for power, prestige and wealth and operate according to their own self-serving needs in life, bearing no conscience whatsoever. In other words, they are psychopaths who operate with a lack of any feelings, or empathy, as well as guilt, or loyalty to anyone but themselves.

Many may argue that Madoff is the epitome of the modern, psychopathic fraudster. Although this may be true, one could also attribute such a distinction to Sam Antar, or Crazy Eddie, a consumer electronics retailer that was founded in Brooklyn in 1971 and was brought down by the SEC in 1989.

As CFO of Crazy Eddie, Antar conspired with the store’s two founders — his cousin, Eddie Antar, and uncle, Samuel Antar — in a massive scheme that defrauded company investors and countless others. Antar’s culpability and criminal actions included skimming, money laundering, insurance fraud, securities fraud, and a host of other illegal activities. After being convicted in federal court and pleading guilty to three felony charges, he was subsequently sentenced to only six months of house arrest, 1,200 hours of community service and $10,000 in fines.

Antar confessed in a manner befitting someone with psychopathic personality traits, stating publicly that he and his family committed their crimes at Crazy Eddie for “fun and profit.” He has openly acknowledged having no empathy for his victims and that neither he nor his co-conspirators have ever had a conversation about morality or remorse. Moreover, Antar admits that his subsequent cooperation with the government to serve as a witness against his own family members had nothing to do with regret. He did it to avoid a longer prison sentence.

In a 2009 interview with Fox News, Antar was asked by a reporter if he was any “healthier today for what had happened.” He responded by saying that he was still the same person and that no one really knows anyone’s intentions. He was later asked whether he would commit fraud again if given another opportunity. “You never know,” he said.

Former Tyco CEO Dennis Kozlowski, who is currently serving an 8-to-25-year sentence in New York state prison for securities fraud and embezzlement, was not as forthcoming during a 2008 interview on CBS’ news program 60 Minutes. During this interview, he adamantly denied any criminal intent or wrongdoing during his time as head of Tyco.

This refusal to admit to his crimes or show any remorse came from a notorious defendant who lived a lavish lifestyle. This was a man who was publicly vilified for owning a $6,000 shower curtain and throwing a $2 million exotic, Roman-style birthday party in Italy for his wife — half of which was expensed to Tyco. After Kozlowski joked about his penchant for purchasing priceless works of art, news correspondent Morley Safer asked him what it was like to earn the type of money he was making. The disgraced CEO responded by saying it was simply a way of “keeping score.”

Although Kozlowski may be viewed as a real-life version of Gordon Gecko from the movie Wall Street, his behavior, past actions and statements reflect someone with psychopathic characteristics. He had a great desire for personal gain and possessed a wheeler-dealer attitude towards acquiring new companies that earned him the nickname “Deal-A-Day Dennis.”

Within this world of white collar crime, we begin to encounter a newly observed phenomenon: behavior devoid of morality but replete with a psychopathic drive to defraud anyone and everyone. And the more powerful the employee’s position, the greater their sense of entitlement, the larger their propensity to lie and the more absolute their lack of remorse, the more grandiose the fraud becomes.

Dr. Robert D. Hare describes many occupational offenders as criminals who are insignificant and harm a limited amount of victims. When it comes to white collar psychopaths, however, companies are faced with highly problematic offenders, says Hare, a professor of psychology at the University of British Columbia and president of Darkstone Research Group. They can become involved in grossly lucrative scams while living lavish
lifestyles as their victims lose their life savings.

Steve Lee, managing director of Steve Lee & Associates, a forensic accounting firm in Los Angeles, describes how his firm is continuing to see an increase in inquiries about fraud perpetrated by C-level executives. This is a type of fraud that entails grandiose thievery involving millions of dollars. More than that, Lee says that the suspects who engage in these large-scale frauds are usually motivated by anything but intense financial needs or pressure.

As companies and working-class employees continue to be scammed by these jet-setting psychopaths, it becomes increasingly apparent that occupational fraud, as a form of white collar crime, is a problem that will never cease to exist. From the simple pilfering of cash from a register or warehouse inventory to intricate schemes of embezzlement or financial statement manipulation, employee theft will always be a scourge on the business world and society.

The degree of this problem will always depend, as it does today, upon internal controls that are set in place within an organization, coupled with training, education, and awareness of unethical and illegal workplace behavior. This loss prevention philosophy keeps in mind the fact that human nature is such that most employees, as described through the contributive theories of Donald Cressey, will always continue to engage in theft from their employers as a result of available opportunities, the financial need or external pressures facing employees, along with their actions of rationalization.

However, there are those deviant offenders who pose the greatest challenge to all organizations, for they cannot be deterred or educated to stray away from their most diabolical of intentions. Outside of catching and prosecuting them after the fact, there is only one method of loss prevention against such criminals: do not hire them.

Then again, this is easier said than done, for the Devil comes in many forms. Hence, the question at the end of the day is, how does an employer recognize the Devil during a job interview?

Written by Bruno Pavlicek, March 3, 2012, who is senior corporate security investigator for Verizon Wireless. He is a certified fraud examiner, and formerly has served as both a county prosecutor’s detective and police officer. Reprinted with permission from Risk Management Magazine. Copyright 2012 Risk and Insurance Management Society, Inc. All rights reserved.

Photo credits: Corepics VOF/Shutterstock.com and Sergey_Bogomyako/Shutterstock.com
Follow the Money: Prevent Embezzlement

By: Rhonda R. Savage, DDS

With the economy improving, John was thrilled to see his small company starting to boom. With all the new business, John was so busy signing new accounts and training his new staff members that he delegated the bookkeeping responsibilities to a long-time employee he trusted. As time passed, John started noticing discrepancies in the business’s account and discovered the employee had been embezzling money from the company. Unfortunately, embezzlement is not uncommon and is often difficult to detect. What could John have done differently to prevent this kind of problem?

Embezzlement is a crime of opportunity and trust. A person who is trusted is placed in a position that allows him or her complete access to the financial data of the business, typically with minimal or no oversight by the supervisor or owner. The best way to prevent embezzlement is to first, be honest yourself in your activities. Leaders must lead by example. Second, pay your employees well and treat them well. Third, hire the right employee. Start by checking all references. Consider obtaining fidelity bond insurance coverage on this employee. If the employee is not bondable, do not place them in the position of handling your financial matters. Run a criminal background check.

Here are some simple techniques that decrease the opportunity and temptation for embezzlement:

1. **Assign designated duties.**

   Do not have only one person handle the incoming mail, deposits, balance the checkbook and send statements. This is difficult in smaller businesses with only a few staff members. In this case, the owner needs to handle or outsource payroll, tax preparation, balancing the checkbook and management of the accounts payable. If the owner chooses to outsource this work to a bookkeeping company, the same due diligence of inspecting the bookkeeper’s work is very important.

2. **The owner should review reports.**

   Every day, you should have an end-of-day report, an adjustment report, a history of payment that breaks down cash receipts, credit card payments, checks and outside financing for services on your desk. The owner should compare the deposit slip receipt to the deposit. Do an occasional mini-audit of the books.
Let your staff know you’re looking daily by questioning them. For example, say, “I see Mrs. Smith didn’t pay for today’s fee; is there a reason why?” This shows your employees you are keeping an eye on the day’s activity. These checks take 5-10 minutes of your day.

3. **Review your bank statement.**

Inform your staff that they are not to open any mail from a banking institution. Even better…have your bank statements sent to your home address if your mailbox is secure. Scan the checks that were written. Your signature should be on each check.

4. **Know where your money is going.**

If you do utilize an employee to process your accounts payable, develop a system for your mail. Staff members should put the incoming mail in one location on your desk. Review the bills and put them into an in-basket for the employee to process. Have them print the checks and attach them to the invoice, then sign them. If you don’t recognize a check, question it. A different staff person should stuff the envelopes and mail the payments. If the same person pays and stuffs the envelope, the checks can be changed.

5. **Establish office policies.**

Make deposits daily, close and balance each day, bill as services are rendered and send periodic statements if purchasing extends over time. Review your monthly reports. Each month should be closed out prior to running the reports to prevent changes from happening. Write pre-numbered receipts for all cash payments and monitor petty cash. All records should be kept at the office. Do not allow employees to work extended hours and establish password control for sensitive areas, such as payroll.

6. **Watch your overhead numbers.**

Learn to read your financial statements. You should know the basic overhead numbers for the business. One example of a common fraud/embezzlement system involves double payment for supplies, or the creation of dummy vendors. Another example is the ease of obtaining preauthorized credit cards in your name, using the credit card to pay personal bills and developing schemes to pay the credit card. Run periodic credit checks on yourself and watch open lines of credit.

7. **Be a fair, consistent, honest leader.**

Leaders live in glass houses. We cannot expect our staff to model differently than we ourselves model. Don’t take supplies from the office home. If you do, it teaches your team that stamps, pens and office supplies are okay to take home. Watch your use of time in the office. If your time involves taking personal calls, surfing the Internet or running a side business and you are not focused on your primary business, your team will do the same.

**Time embezzlement is the greatest loss to the majority of practices.**

General Norman Schwarzkopf said, “You don’t have to be loved to be a leader, but you do need to be respected. Respect must be earned. To be respected, you must give respect.” Set your office policy regarding cell phone and Internet usage during office hours, and then abide by it yourself. An employee that embezzles by spending time on the phone or Internet not only hurts your bottom line, but he or she impacts the entire business. Because of the increased burden on the team that is working, resentment builds. And with the resentment, you’ll experience decreased morale, which leads to loss of production.

Know that you shouldn’t become immediately suspicious of your team, but that there are steps you can take to reduce your risk. Consider these steps to be a positive focus for your business.

---

Dr. Rhonda Savage is an internationally acclaimed speaker and CEO for a well-known practice management and consulting business. Dr. Savage is a noted motivational speaker on leadership, women’s issues and communication. For more information on her speaking, visit www.MilesGlobal.net or send her an email to: Rhonda@MilesandAssociates.net

Photo credit: stable/Shutterstock.com
How to Handle Embezzlement in the Family Business

By: Lois Lang, Psy.D.
Hearing about embezzlement in a public company rarely shocks anyone, but when it happens in a family business, people are often stunned. “How could he steal from his own family?” “Doesn’t she know she’s hurting her siblings/cousins/parents?”

As tough and painful as embezzlement is, it’s not as uncommon as many of us would like to think. Sure, the kind of embezzlement that results in jail time is rare, but other levels of it happen daily.

How could this happen? Many factors lead to embezzlement, including chronic financial strain, a general sense of family entitlement, lack of internal company controls, and the reality or perception of being overworked and underpaid.

To make matters worse, often the embezzler doesn’t even know that what he or she is doing is wrong.

Here’s an example of how embezzlement can start small and quickly grow: Jim (the business owner’s son) fills up his gas tank once on a Friday and pays for it with the business account, knowing that the miles he drives will be primarily for personal, not business use. He tells himself it’s okay because he has filled the tank on his own some weekends and used “his gas” for business use on Monday and Tuesday. Then he takes a few vacation days and doesn’t record it as paid time off. He picks up gift cards for employee recognition and pockets a few for himself. He knows that Dad pays him less than local competitors, and this is the way he evens it out. He notices other family members treating the business the same way, so it simply becomes the “way we do things around here”—it is their company culture, not embezzlement.

The misuse of company assets, time, and money escalates. Soon, Jim adds a non-working family member to payroll, petty cash disappears, one out of ten customer checks are rerouted to Jim’s personal account, and personal items are consistently charged to the business credit card. Eventually, an employee in accounting notices and agonizes about who and when to tell.

So while embezzlement starts small and often innocently in a family business, it can quickly escalate to something big that damages the business, hurts non-family employee morale, and breaks family trust.

Take Action
What do you do when you realize a family member is embezzling from the business? Action is obviously required, and taking a cautious, thoughtful, respectful approach is wise. To begin, have a pre-meeting of key leaders, without the suspect family member present, to address the following questions:

1. Do we have clear, hard, verifiable facts before we assume fault and intent?
2. Who will be at the meeting to lay the facts out?

3. Are we going to involve the legal system?

4. If we continue employment with this family member, do we need to change their job position?

5. How or will we message this to the rest of the family? To other employees? To the Board of Directors?

6. How or did the company contribute to this problem?

7. If the company did, what steps will we take to prevent it in the future?

8. How or did the family contribute to this problem?

9. If the family did, what steps will we take, as a family, to prevent it in the future?

10. Has this family member had chronic, known problems with finances?

11. Generally, how can we protect the company from future misuse of company assets or embezzlement?

12. How do we protect the whistleblower?

13. Do we have a whistleblower program set-up internally? Are employees trained annually?

14. Do we talk openly in Family Council about our responsibility to financially protect and care for company assets? Do we give specific examples of what is and is not allowed?

15. Do we have a solid non-compete clause in our employment contracts and/or employee handbook in case we have to release the family member from employment?

16. Do we consistently run a professional background check on applicants?

17. If I need to walk the family member out the door, how do I prepare? Computer security, locks, passwords, current company asset retrieval, bank account access protection, social media tracking, last paycheck, etc.

18. Do we need to involve the corporate attorney, Board of Directors, outside legal attorney, CPA, business psychologist? If so, when and how?

Once you’re clear on these aspects, it’s time for the second meeting—this one with the suspect family member. When you begin the meeting, keep it at the level of discovery. Lay out the facts and ask the family member their perception of what happened. Really listen to what they say and how they say it. Remember, it’s common for family members not to realize that they are indeed embezzling. If this is a first offense, and if the embezzlement is not excessive, some education may be the best course of action. However, if you believe the family member knew what he or she was doing and did it anyway, or if the embezzlement is substantial, termination may be the only option.

During the meeting, you need to be vigilant in checking yourself by asking “What would I do if this wasn’t a family member?” and “Is this at a level where I will be able to trust them again?” Your answers to these two questions will reveal a lot about your best action plan.

Keep Your Family and Business Strong

Of course, education of all employees (family and non-family), strict policies about how the company’s assets and resources can be used, and enforced controls that can spot any wrongdoing are the best ways to reduce your family business’s chances of falling victim to embezzlement. Acknowledging what could happen, along with some planning to prevent it, will keep your family and business strong, successful, and honest.

Lois Lang is a speaker and consultant with Evolve Partner Group, LLC where she helps organizations become high performance workplaces. Lois works with clients on management succession readiness, organizational/team strengthening, executive coaching, executive compensation design, wage studies and mediated conflict resolution. For more information on Lois’ speaking and consulting, please visit www.evolvepartner-group.com or contact Lois at lois.lang@evolvepartnergroup.com or (209) 952-1143.

Photo credits: Aletia/Shutterstock.com
Imperial PFS, the leader in premium financing, continues to focus on the success of our agency partners.

Our regional sales force and local branch offices offer a unique perspective to understand your challenges. Our creative service offerings include numerous programs that are designed to benefit you and your clients. We look forward to your continued partnership with Imperial PFS and providing you the most comprehensive benefits in the industry.
RENTAL REIMBURSEMENT DRIVES SATISFACTION.  
Are Your Policyholders Covered?

Rental Reimbursement Facts*  
• There are more than 19.3 million car accidents each year in the United States.  
• The average car is in the repair shop for nearly 2 weeks after an accident.  
• On average, 1 year of rental reimbursement coverage costs less than a 1-day car rental.  
• Research shows that rental reimbursement coverage drives both satisfaction and retention.  
• 1 in every 8 drivers will be involved in an accident this year.

Contact us at RentalCE@erac.com for details about an IAIP Rental Reimbursement Continuing Education (CE) course in your area.

SPONSORED BY enterprise

* 2011 The Renters Group, Internal Data, National Safety Council  
©2013 Enterprise Rent-A-Car  D9669 0613
Identity theft occurs more frequently in the United States than people want to believe. According to the U.S. Department of Justice, identity theft and identity fraud are referred to as “all types of crime in which someone wrongfully obtains and uses another person’s personal data in some way that involves fraud or deception for economic gain.”

The Federal Trade Commission compiles a report every year for identity theft complaints in the United States. These complaints increased more than 78 percent between 2009 and 2011. With identity theft becoming an increasing problem, Professor Duanne J. Thompson, the acting program chair of Criminal Justice at Argosy University, Atlanta, offers some advice for consumers to take in order to protect themselves from identity theft:

1. Protect your identity like you would protect your house.

2. Don’t give out sensitive information such as social security information. In most states it is illegal for a business to ask for your social security number for transactions.

3. If purchasing on the Web, make sure you know who you are buying from and that the site is secure.

4. Don’t fall for phishing scams. Legitimate websites will never ask for your password or account information. If in doubt contact the vendor before you send your information.

Thompson also says that consumers should be aware that they have a right to have one free credit report from every credit clearing house, such as Equifax, TransUnion and Experian, at least once a year. In some states, consumers are allowed a free credit report at least twice a year. Consumers should look at the information from their reports and ensure that the information is correct and accurate. They should look specifically at each credit statement every month for suspicious fraudulent activity.

The bigger question is what a consumer should do if they find themselves victims of identity theft. Thompson suggests to first notify your credit vendor that your card has been compromised and that there is an individual acting as you. Consumers should then call their local police department and file a report. Afterward, gather as much information as possible about your accounts and all transactions to help aid the investigator in the case.

Once the police report is obtained, file an identity theft claim with all three credit clearing houses (Equifax, TransUnion and Experian). All three credit clearing houses will require a copy of the local police report and all the information you have supporting the theft.

With the rise of online trends such as social media and online banking, consumers must be more vigilant about their identity as these trends lead to more and more avenues for identity theft criminals. The best way a consumer can protect their identity is to simply be smart and be aware of their financial records.

Reprinted with permission from Brandpoint.

Photo credit: RobByron/Shutterstock.com
Insurer Trends Center on Technology

By: Jared Wade

Volatile markets, greater regulatory scrutiny and continuing technological advancement are forcing insurers to “increase their focus on controlling liability risks and improving transparency and stakeholder confidence,” according to Don Canning, vice president of insurance for SunGard, a software and technology services company.

This is the driving force between many of what SunGard recently identified as the “Ten Insurance Risk Trends in North America.” Given the source, it is no surprise that improving technology to address new risks features prominently on the list, which stresses insurers’ “need for data quality,” “faster, more efficient modeling,” “platforms that can support risk visibility” across borders, “expanded service capabilities” and “more frequent risk reporting.”

The company views insurers’ wealth of information as arguably their greatest asset for pricing risk more accurately and adjusting risk appetite. And the easier it is to access and analyze this data, the more an insurer can turn it into a competitive advantage.

“U.S. carriers are looking to centralize information from disparate and traditionally separate valuation and projection modeling systems to achieve consistent views of risk,” states the report. It is this integration of information into a “Big Data” warehouse that is increasingly allowing insurers to make better risk decisions.

Written by Jared Wade, October 2012. Reprinted with permission from Risk Management Magazine. Copyright 2012 Risk and Insurance Management Society, Inc. All rights reserved.

Photo credit: Melpomene/Shutterstock.com
Based in Atlanta, Ga., Crawford & Company (www.crawfordandcompany.com) 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 Crawford System of Claims Solutions® offers 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. The Company’s shares are traded on the NYSE under the symbols CRDA and CRDB.
Now, you really can live forever, but that’s not necessarily a good thing. Many of your online accounts – from automatic bill payments to eBay – may remain active after you pass away, unless you take steps to ensure they don’t, says attorney Hillel Presser, author of “Financial Self-Defense” (Revised Edition).

Automatic bill pay, for example, can theoretically keep tapping your bank account long after you’re gone or, at least, until your money is.

“It’s important to make sure your online bank and shopping accounts, even your social media, can be closed out, or that your loved ones are authorized to access them,” Presser says. “You may ask, ‘Why would I care if I’m gone?’ I can tell you from experience: because it can create real headaches, and more heartache, for your family.”

Bank and shopping accounts will be vul-
nerable to identity theft, which would affect your estate if someone opens credit cards in your name. You might have valuable intellectual property, like domain names. They may need access to your health records, particularly if you died under questionable circumstances, he says.

There’s the sentimental stuff – photos and emails -- that your family may want as a remembrance of you, and the libraries of music and ebooks, which may represent a considerable investment on your part.

“The problem is, even if you provide a family member with all of your accounts, log-ins and passwords, they may not be legally allowed to access them,” Presser says. “In many cases, they may be violating the accounts’ terms of service or violating federal privacy and computer fraud laws. Some states have laws governing online materials, but they’re different and which of your accounts are covered depends on where the provider is located.”

What can you do to ensure your family isn’t left with a virtual nightmare after your passing? Presser offers these tips:

**Create a list of all of your accounts, including log-in names, passwords, and answers to any security questions.**

Obviously, your list will need to be securely stored. Since you’ll need to update it regularly as you add accounts or change passwords, it will be easiest if you keep the list on your computer in a password-protected folder. Some versions of Windows allow you to create protected folders, but you may need to get third-party software to do this, such as free Ax-Crypt. Remember to create a backup of your list, whether it’s on a jump drive or printed out on paper. Store the backup in a secure place such as a safe deposit box. Do not put password informa- tion in your will, which is a public document.

**If you have a Google account, set up the new inactive account manager.**

In May 2013, Google became the first site to give users an option for choosing what becomes of their content if they should become debilitated or die. Under the profile button, click “Account,” scroll down to “Account Management,” and you’ll find instructions for “Control what happens to your account when you stop using Google.” You can select how long the account should be inactive before your plans are set into motion; choose to whom you want to offer content, such as YouTube videos, Gmail, Google+ posts, Blogger and Pic-casa web albums, or whether it should simply be deleted.

**Appoint a digital executor.**

Perhaps the simplest way to ensure your online life is taken care of is to appoint a digital executor – a tech-savvy person who will be willing and able to carry out your wishes. Authorize the person to access your inventory of log-in information and spell out what you want done with each account, whether it’s providing access to loved ones or business partners, or deleting it.

The digital world has grown and transformed so rapidly, the law hasn’t kept up, which makes managing your digital afterlife challenging, Presser says.

“Until there are more consistent laws and procedures governing this area, it’s best to plan ahead, leave clear instructions and be sure you have a list of accounts where your estate lawyer or a loved one can find it and access it,” he says. “It will make a world of difference to your survivors.”

---

Hillel L. Presser, Esq., MBA. Presser’s firm, The Presser Law Firm, P.A., represents individuals and businesses in establishing comprehensive asset protection plans. He is a graduate of Syracuse University’s School of Management and Nova Southeastern University’s law school, and serves on Nova’s President’s Advisory Council. He is a former adjunct faculty member for law at Lynn University. Complimentary copies of “Financial Self-Defense” are available through www.assetprotectionattorneys.com <http://www.assetprotectionattorneys.com>

Photo credit: Rudy Uman/Shutterstock.com
Celebrating 20 Years of Promoting “Excellence through Education”

It was 1991, when a group of very dedicated members of the NAIW Long Range Planning Committee, (now IAIP) came together to brainstorm the future of the Association. The LPR Committee charge was to brainstorm the organization’s future 5, 10, 20 years down the road.

One key accomplishment of that particular LRP Committee was the establishment of a scholarship foundation to assist insurance professionals and college juniors/seniors following a course of study leading toward a career in the insurance industry.

The NAIW Education Foundation (now known as the Insurance Scholarship Foundation of America) was established in 1993 as a separate 501c3 charitable organization to provide scholarships to college students preparing for a career in the insurance industry, and for men and women working in the insurance industry seeking to improve their career opportunities.

It was the very next year, 1994, that the first scholarships were awarded by the ISFA Board of Directors. Two Professional Scholarships and 3 College Scholarships were awarded and ISFA was on the road to Promoting Excellence through Education.

20 years later, the Insurance Scholarship Foundation has awarded gifts of education to 461 college and professional scholars, representing over $430,000 in scholarships. ISFA was able to award these scholarships, and have success in our mission to promote excellence in the insurance industry by underwriting the education of current and future employees because of the generous support of individual donors, members of IAIP and other industry supporters.

“Twenty Years” of making a difference in the lives of individuals who have chosen Insurance as their career, who have enhanced their knowledge and skills, and contributed excellence to our Industry is an exciting legacy.

To continue the legacy, ISFA needs the ongoing support of our donors. There are many ways you can provide support:
• Come play golf with us at the 7th Annual ISFA Charity Golf Tournament on Monday, September 9th. The tournament is held at the Clubs of Cherokee Valley in Travelers Rest, South Carolina. Join us as an individual, bring another golfer, or bring a foursome for a great day on the course and support this important educational effort.
• If you are unable to participate as a player, we would appreciate your consideration as a sponsor or donor. Contact ISFA at foundation@inssfa.org for additional information.
• Become a part of the legacy with a visit the ISFA website at www.inssfa.org. Click the “Donate Now” button, select the type and amount of donation you would like to make and complete the information form.
• Or, you may print the form and mail it along with your check to:
  ISFA
  P.O. Box 866
  Hendersonville, NC 28793-0866

“Thank you” to each and every donor of the Insurance Scholarship Foundation of America for 20 Years of Making a Difference!

“ISFA is a 501 (c) (3) public charity. All donations are tax deductible.”
Cyberattacks are the new normal. It seems each week a news outlet reports yet another high-profile data breach affecting businesses and consumers. Even so, many companies fail to realize the severity of the threat.

In fact, a recent report from the Federation of European Risk Management Associations (FERMA) reveals that, surprisingly, only 16% of companies have designated a chief information security officer to oversee cyber-risk and privacy, and less than half have a strategy for communicating a cyber-risk incident to the public.

The report, “Meeting the Cyber Risk Challenge,” reveals another disturbing statistic: Companies are failing to purchase coverage for a cyberattack. Only 19% of respondents claimed they have purchased security and privacy insurance designed to cover exposures associated with information security and privacy issues.

But preparing is about more than just insurance. “Information security is a classic enterprise risk,” said Julie Graham, a FERMA board member. “It is not solely a subject for the domain of the chief information officer or the chief information security officer.”

Indeed, everyone plays a part in keeping a company’s data safe. Now if all companies would just act on that.

Written By Emily Holbrook, March 2013. Reprinted with permission from Risk Management Magazine. Copyright 2012 Risk and Insurance Management Society, Inc. All rights reserved.

Photo credit: David Evison/Shutterstock.com
When the first hijacked plane slammed into the North Tower of the World Trade Center at 8:46 AM on September 11, 2001, Robert Scott, president and chief operating officer of Morgan Stanley-Dean Witter, was at 3 World Trade Center addressing 400 members of the National Association of Business Economists. Scott evacuated the building just in time to watch a second aircraft slam into the South Tower which he knew housed his company offices and several thousand employees. By 9:30 he and his senior executives had convened at a backup site that became their command center. The decisions made by Scott and his team that day would make Morgan Stanley a case study in successful crisis management and would enhance Scott’s reputation as a leader.

What is the difference between a Morgan Stanley and less successful companies? Why do some organizations come out of crisis with enhanced reputations while others may not even survive as a business? While the reasons are many and varied, it frequently comes down to three main areas:

• Failure to consider the human factor;
• Failure to gather adequate information to support decision-making;
• Failure to act quickly and decisively.

By: Lucien Canton
• No matter how much information on risks they are given, people do not believe that a crisis will happen to them. They may understand it intellectually but viscerally they do not believe it will happen. This hampers their willingness to prepare for crisis.
• When confronted with a crisis, a person’s first reaction is denial – they often do not recognize that a crisis is occurring. This leads to a hesitation to act.
• There is a tendency to normalize crisis, that is, to see what one expects to see rather than what is actually occurring. It is easy to misinterpret or completely miss indicators that a crisis is imminent or occurring. These indicators may be obvious after the fact but are easily missed during the crisis.

2. **Good information is essential to good decision-making.** The second phase that people experience when confronted with a crisis is to deliberate – they need to seek corroboration about what has occurred or is occurring and to consider courses of action. There are, however, problems inherent in this process:
• Most information available in the early stages of crisis is fragmentary, contradictory, and unreliable. There can also be a considerable volume of information available, most of it not really helpful. Sorting through this mess requires an understanding of what information is important and why it is needed by decision-makers.
• A common failing in crisis is the tendency to seek only information that confirms what the crisis team thinks is happening or expects to see happening. The problem with this is that the team misses the true nature of the crisis and makes decisions that can be counterproductive or flat out wrong.
• The paradox of information collection is that while the better the information the better the decision-making, there will never be a situation where one has all the information needed. At some point, you will have to make decisions based on incomplete information. Information collection cannot become an end in itself that delays decision-making.

3. **Act Decisively.** Overcoming denial and moving through deliberation leads to action. In most cases, the quicker you are seen to act and to provide information on the crisis and your actions the more likely you are to mitigate the effects of the crisis. Effective action depends on a number of elements:
• Isolating the crisis by identifying a crisis management team and dedicating them solely to the crisis. Other parts of your organization can continue to be devoted to business as usual, but your crisis management team must be focused exclusively on the crisis and must have the authority and resources necessary to act.
• Speed is essential, particularly in crisis communications. Depending on the nature of your organization, you may have only minutes to get your story out. Even if it’s just acknowledging that the crisis has occurred and that you are assessing the situation, it is critical that the public, your employees, and your shareholders hear from you.
• Acting quickly, demonstrating empathy with anyone affected by the crisis, and, above all, being honest can go a long way to countering the negative effects of a crisis.

Surviving a crisis requires that you quickly recognize and accept that a crisis is occurring, gather sufficient information to make decisions regarding the crisis, and move quickly to implement those decisions. Incorporating these three keys into your preparations for crisis may not guarantee success but they will certainly go a long way to preventing failures.

Lucien G. Canton, CEM is a consultant specializing in preparing managers to lead better in crisis by understanding the human factors often overlooked in crisis planning. A speaker and lecturer, he is the author of the best-selling “Emergency Management: Concepts and Strategies for Effective Programs.” For more information, please visit www.luciencanton.com, or email Info@luciencanton.com.

Photo credit: Kzenon/Shutterstock.com

These failures are so common that they suggest three keys to successful crisis management:

1. **Recognize that you are your own worst problem.** Too often in preparing for crisis one tends to ignore the human factor. Understanding human nature and how people react to crisis is one of the fundamental keys to crisis management.
State Auto
committed to excellence and the International Association of Insurance Professionals

• Excellence in products—
  auto, home, business, bonds, farm and ranch

• Excellence in claims service—
  call our contact center 24x7, 800-766-1865

• Excellence in distribution—
  committed to the independent agency system

If you are interesting in partnering with State Auto, please contact Terra Boroff at 614-917-5128 or email Terra.Boroff@StateAuto.com

STATE AUTO
Insurance Companies

STATEAUTO.COM
Guest Column

Question & Answer: Cloud Security

By: Emily Holbrook

The trend of businesses turning to the cloud for server space has become more popular as companies look for an easy and economical way to store data. Even the U.S. government is getting on board. Just last summer it was announced that the Department of Defense plans to use cloud computing for data management. But how can you ensure that your data is secure in a virtual environment that is beyond your control? For more insight on this critical security issue, editors at Risk Management Magazine spoke with Carson Sweet, CEO of CloudPassage, a...
cloud security service provider.

**RM:** As more companies turn to the cloud, the threats to information security increase. How are companies handling this?

**Carson Sweet:** The interesting thing that people don’t get when they use cloud servers is they don’t realize their own responsibilities. There’s an education process. When people use cloud servers, there’s a shared responsibility. Amazon EC2 [Amazon-owned cloud servers] will take care of part of the security. The owner of the virtual machine has to do the rest.

The analogy I use is renting an apartment. A landlord will say, “I’ll take care of the security of the common areas, the front door, the elevators and all that stuff.” But once they give you the key to the front door, you’re on your own. They can’t take [on] the risk for what goes on inside. It’s the same thing with cloud servers. They are rented just like an apartment. So a lot of people think that the cloud provider is going to do everything, but the cloud provider, in fact, doesn’t. If the cloud provider is going to do everything, that’s more like a hotel.

That is where things are going; there is a shared responsibility model, and security technologies, auditors and the whole risk management world is moving to try to deal with an issue where some of the controls are with the provider and some of the controls are with the actual owner of the system. It’s going to be a shift in IT, a shift in thinking, a shift in the way that security is achieved.

**RM:** Why don’t traditional security models translate to the cloud?

**Sweet:** Part of it is that shared responsibility model. Typically the way you handle security is walls and moats. So you’ve got all of your servers inside your data center, and you build a nice big firewall environment around it, intrusion detection and so forth to create this perimeter environment. In order to create a perimeter like that, you need to be able to control the IP addressing and the hardware configuration. You can’t do that in a cloud. So when you use these cloud-server environments, there’s no hardware involved. Basically, everything we’ve come to rely on from a security perspective in a traditional data center is just gone. You can’t use it that way anymore.

**RM:** Are private clouds a safer option?

**Sweet:** It’s a little bit easier of a situation. The difference between a private cloud and a traditional private data center is that things in the private cloud move faster. So in that environment you’ve got a cloud within a perimeter. You’ve got that initial perimeter security, which is great. But where things get a little hairy is that you’re creating servers very fast. You used to have a six-week lead time.

For example, if you needed a server, you called up IT and you told them. They would order it, ship it, put it in a rack, turn it on. And that took weeks. During this time there was a lot of opportunity to really get things in order. Now, if a private cloud wants a server, they just click a button and it’s there. So that makes for a very dynamic environment—it’s wild.

The other thing that’s risky from a private cloud perspective is that they do not stay private for very long. People are attracted very quickly when they realize the benefits and they start to see certain articles written by companies like eBay, who say “the way to do this is to take your excess need and put it out into EC2.” So you’ve got your private cloud and then you burst out [with excess storage needs] and use temporary capacity, so you don’t have to pay for that high watermark. That, all of a sudden, makes that private cloud into a hybrid cloud. And hybrid clouds are where everything is headed.

**RM:** What are the benefits of hybrid clouds?

**Sweet:** Hybrid clouds are like if you have a four-bedroom house and you need more room, you have a deal set up with the hotel down the street for more space. People will actually take servers and plug them into a public cloud for temporary workload. Good examples would be tax season, when the load goes through the roof. Instead of buying more servers, they can just turn on a bunch of web servers on Amazon.

Another good example is retail during the holidays. The capacity needs go way up. Social media is another good example. We see the server count of social media companies go up and down dramatically even within a week because on weekends more people are tweeting and more people are checking in so they need more servers. Usually on Thursdays the server count starts to grow and it will shrink back down on Mondays.

The flexibility with that is really attractive. You can either buy all the capacity you need and only use a third of it most of the time or you can use a temporary capacity in a public cloud like EC2 or Rackspace. But you have to do it safely.

**RM:** Will there ever be a universal set of compliance regulations or authenticity guidelines for the cloud?

**Sweet:** Probably not universal, but that’s one of the things the Cloud Security Alliance (CSA) is trying to do. The CSA is putting together standards that map together other existing standards. The health-care industry is always going to have their HIPAA stuff, the financial industry is always going to have their FFIEC stuff, the federal government is always going to have their FISMA stuff. They will never unify but there will be kind of a layer to link them together.
Your Time. Your Terms.
Your Insurance Expertise.
Phase into retirement working from home.

Become a WAHVE Vintage Worker. WAHVE Gives You Choice when you’re thinking it’s time to phase into retirement. Work remotely in the comfort of your home. Create a new life-work balance. Choose the type of work you want to do. Continue to contribute your intellectual capital.

To learn more, visit our website at www.wahve.com and find out how happy our clients and wahves are. If you are ready to work from home, just click on Vintage Professionals/Apply on our website.
Welcome New Members

New Members from February 20, 2013 through July 10, 2013

REGION I
David Abarzua
Soraya Accioly
Felicia Amaral
Kathleen Armstrong
Christy Ann Berard
Stevanie Bickford
Katherine Bouton
Janna Byrne
Rachael Caron
Chanel Clancy
Lisa Cook
Kristy Copeland
Margaret Davis
Angela DeChiara
Gretchen Doumit
Joann Dunsing
Caitlin Earle
Maryanne Edsall
Joyce Felici
Nancy Finnegan
Kirk Flanagan
Sara Fritz
Gail Hill
Kim Hillman
Carla Hope
John Hull
Pamela Humphrey
Yasmina Hussain
Lisa Iadevaia
Jacqueline Kenworthy
Bryanne Kingsbury
Dara Kirk
Ursula Knowles
Shannon Latham
Penny LeBlanc
Kelly Manning
Ruth Martin
Sue Martin
Laureen Mathon
Stephanie McAlinden
Lori Miskell-Hauser
Linda Moler
Eva Morel
Jessica Murante
Renee Nevins
Lindsay Norman
Karen O’Connell
Jonathon Pacheco
Deborah Pennington
Sonya Porter-Burill
Philip Reemes
Sylvia Remisiewicz
Lisa Riviin
Kiern Robillard
Bonnie Rousseau
Luanna Schmitz
Haley Shaud
Lourdes Sikora
Anjana Singhvi
Joanne Skribis
Lacey Steeves
Donna Tamburini
Emily Thomas
Janeen Thomas
Dezray Titman
Alison Urang
Joanne VanDyk Cory
Deborah Verdier
Kim Watson
Shelley Wyman
Julie Zando-Dennis

REGION II
Rita Budreckas
Kimberly Daugherty
Kathy Hodges
Amanda Legg
Dianne Mayhew
Ryan Morgan
Wendy Owens
Dana Richardson
Karen Terry
Tracy Thomas
Dale Williams

REGION III
Stephanie Allen
Patty Bakmaz
Rachel Bigley
Sandra Blanco
Ronald Bognar
Tabitha Burrow
Curt Crapo
Nancy Crapo
Melissa DeAngelo
Terri Diephouse
Luis Falcon
Tracy Fero
Chuck Gore
Robert Hoban
Veronica Huzzard
Richard Littreal
Lara Lopez Valentin
Stefanie Lund
Lee McManus
Audrey Moore
Eloisa Morandi
Michaela Nelson
Diane Offen
Felicia Plunkett
Eva Ponko
Lana Pugh
Mercedes Rivera Valdes
Griff Rogers
Laurie Sisk
Linda Smith
Jessica Summerlin
Robert Swetland
Rebecca Wylie

REGION IV
Cheryl Bowker
Marianne Brandle
Jessica Bussie
Shirley Dashkevicz
Patricia Day
Debi Dehne
Amy Halaburda
Lee Herman
Carol Hess
Nancy Hester
Robin Hutchisson
Mandy Johnson
Ian Kitson
Kim Moncman
Scott Mull
Sheri Noll
Trish Scharrr
Jennifer Thompson

REGION V
Sarah Anderson
Deborah Biggane
Ashley Black
Helen Collins
Sarah Duncan
Hannah Eginoire
Robin Fuzzell
Bonnie Gauerke
Travis Guess
Theresa Gutsch
Shannon Hawkins
Holly Heiberger
Jenny Horner
Staci Huseman
Marlys Maciona
Heather Pering
Danice Rein
Kris Sheffield
Nattlie Woodley
Kim Woods
Shannon Worlin
Association News

REGION VI
Lisa Barthelemy
Belinda Brown
Lydia Ertle
Rhonda Flake
Jeannie Foty
Rachelle Harms
Chad Harrington
Briana Hester
Yan Jiang
Beatrice Kathert
Kimberly Laborde
Kathryn Lambert
Tiffany Logan
Judi Louviere
Frank Lubrano
Scott Mackey
Dara Martin
Debra Moreno
Cynthia Richardson
Lindsey Rohm
Brandon Yesse

REGION VII
Nancy Alonso
Carol Darnell
Suzanne Hammers
Sherrill Johnson

REGION VIII
James Armitage
Michael Bibeau
Beth Billstein
Brandy Brazil
Iris Bursiaga
Kirstin Candy
Carla Cave
Claudia Cervantes
Shantih Charlton
Rosie Contreras
Trish DeVore-Gray
Cynthia Easley
Jennifer Eaton
Shieh Choo Ersery
Haley Gaines
Alexander Gareeb
Jessica Gauna-Miller
Britni Gordon
Robyn Grandy
Justin Haagen
Rodney Henderson
Marni Hernandez
Robin Hodson
Kelsey Howard
Raymond Huff
Carla Hutton
Marcia Kealohi
Lori Kilantang
Andrew Ko
Dawn Kyles
Barbara Larson
Deborah Lee
Meg Lee
Robin Mann
Dawn Manzano
Julie Nease
Joe Neroda
Michael Nogueiras
Ella Otto
Linda Padick
Kyle Phelps
Michael Ray
Carol Reynolds
Matt Reynolds
Steve Roth
Teresa Salcedo
Katie Sandoval
JoAnn Schaub
Robin Souza
Eric Strongin
Dennise Tittnich
Brandi Trujillo
Enid Turner
Linda Urner
Jill Van Gundy

REGION IX
Teresa (Teri) Fabry

REGION I
Joyce McCutcheon
Francine Yotsko

REGION II
Kelly Bryant

REGION III
Denise Godwin
Roxanne Sima

REGION IV
Michelle Ackermann
Pam Allen
Cherri Harris
Cheryl Hoffer
Marcella Shinabery
Natalie West

REGION V
Jennifer Murphy
Jennifer Weiterman

REGION VI
Maria Ellenburg
Lorie Walters

REGION VII
Marie Ellenburg
Lorie Walters

REGION VIII
Teresa (Teri) Fabry

REGION IX
Christine Elliott Gleason

REGION X
Susan Carter
Chayla Deitz
Rima Ghandour
Jamie Harding
Dawn Harris
Crystal Jones
Angela Korver
Stacey Matteson
Debbie Mills
Theresa Peery
Kacie Salois
Helen Smith
Cynthia Steele
Carlissa Williams

CONGRATULATIONS TO
NEW CPIWs AND CIIPs
Recipients from February 20, 2013 through July 10, 2013

REGION I
Joyce McCutcheon
Francine Yotsko

REGION II
Kelly Bryant

REGION III
Denise Godwin
Roxanne Sima

REGION IV
Michelle Ackermann
Pam Allen
Cherri Harris
Cheryl Hoffer
Marcella Shinabery
Natalie West

REGION V
Jennifer Murphy
Jennifer Weiterman

REGION VI
Marie Ellenburg
Lorie Walters

REGION VII
Maria Ellenburg
Lorie Walters

REGION VIII
Teresa (Teri) Fabry

REGION IX
Christine Elliott Gleason
Jane Densch
CPCU, AIC, ARP, ARe, CPIW, AIS
President

Jane has been an active member of the Denver Association of Insurance Professionals since joining the association in 1989. Jane has had the opportunity to serve at all levels of the association including, President of IWOD (1994-95); Council Director of Colorado (1996-97); Region VII RVP (1998-99), and on most of the committees on the local, council and Regional levels. Jane’s NAIW Committee service includes Nominating, Organization Interface Advisory Panel, TIW/NAIW Now! Editorial Advisory Panel, Non-Dues Revenue Task Force, Communications Task Force and Student Member Task Force. Four years ago she was successful in securing Allianz Life and Fireman’s Fund, both companies of Allianz as corporate sponsors for NAIW. Jane was recognized by NAIW as Claims Professional of the Year in 1995 and Insurance Professional of the Year in 2000. In 2004 Jane received the AAMGA award from Region VII. Jane is a Founders Club member of ISFA and Pacesetter with the NAIW Legacy Foundation.

In November, 2011, Jane accepted a voluntary early retirement offer from Fireman’s Fund, a company of Allianz. Prior to that, she was the Claims Auto/General Liability Product Director, which involved leading the A/GL Technical Directors in a cohesive approach to technical insurance issues. Coordinating the team’s responsibilities with the claims operational staff and participating in innovative product development with her business partners were part of her responsibilities. She initiated Technically Speaking, a quarterly technical newsletter and the A/GL Advisory Council, a monthly meeting between operational and technical leaders, plus she coordinated monthly technical webinars on emerging claim issues as well as the Advanced Casualty Seminar, a two-day webinar program with CE and CLE. Retirement has given Jane more time to focus on IAIP!

A graduate of the University of Oklahoma, Jane received the CPCU designation in 1989. Other designations include AIC in 1985, ARP in 1989, ARe in 1995, AIS in 2001 and CPIW. As a member of the Society of CPCU and the Society of CPCU Claims Section, Jane has held various offices with Colorado Chapter of CPCU, including local president (2001-02). The Colorado Chapter of CPCU recognized Jane with the President’s Award for Outstanding Leadership in 1993. She co-chaired the Host Chapter Committee, which assisted the CPCU Annual Meetings and Seminars’ successful meeting in Denver in 2009 and was a member of the Claims Section Committee from 2008-2011. She has been on the Colorado Insurance Education Foundation Board since 1996.

Camping and hiking are two of the activities that Jane enjoys with her husband, Dick. They live in the foothills outside of Denver. They can always be found attending sporting and school events of Hanna, their granddaughter.

roz horton
CIC, CPIW, DAE
President-Elect

Rosalyn - “roz” - joined the association in 1992 when she changed careers from running a family-owned business to entering the insurance industry. She is a Member-At-Large in the Tennessee Council of Region III. During her membership, she has served on or chaired committees on all levels of the association (some on numerous occasions). In 1999/2000, she served as Tennessee Council Director and Region III Vice President in 2004/2005.

During her membership with the Nashville Insurance Professionals, roz received local awards as Rookie of the Year, Claims Professional of the Year (twice), Insurance Woman of the Year and represented her local in the council CWC contest four times. She continued by winning the Tennessee contest in 1996, 1998, 2000 and 2008 and was Regional runner-up in 1998. roz was selected as Tennessee Insurance Woman of the Year in 2000 and received the AAMGA Tennessee Council Award in 1997 and 2003. At the Regional Conference in 1993, she was selected as their Rookie of the Year. In 1999, she was also the recipient of the T. J. Mims Award of Excellence given by Canal Insurance to a member of Region III. During the 2008 International Convention in Scottsdale AZ, she received the AAMGA/Presidential Award. roz is a Gold Member of ISFA’s Founders Circle and a sponsor of their annual Golf Tournament. She is also a Trendsetter contributor to the Legacy Foundation.

roz has been employed by AGCS Marine Insurance Company (a division of
Debra Kuhne
AAI, AIC, AIS, CIIP, DAE, CELS
Vice President

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, and most recently Region I RVP serving from 2010 to 2012. Debbi is an avid supporter of the NAIW (International) 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, COBRA, 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, CPIW, DAE, and CELS designations. She has taken several of IAIP’s courses, competed in 2 Regional CWC Speak-Offs and, this year, became an Instructor for IAIP courses.

Tish Riley
CIIP, DAE
Secretary

Tish Riley’s career in insurance spans 30+ years with three different P & C companies. Like many in the industry, she had not intended to make insurance her career but in 1974 she landed a job as a file clerk for a St. Paul Fire & Marine Insurance in the 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 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 7 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 roles from Underwriting Manager to Underwriting Specialist to Allianz Global Corporate and Specialty) for 20 years. She works from her home, in historic East Nashville, close to Titan Stadium. Her current assignment is Underwriting Manager for their Small Business Unit in the Southern States Region. In this position she oversees a staff of employees in Dallas and New Orleans, and is responsible for processing renewal accounts $50,000 and under in premium. In addition to these duties, she has, over the years, served in an advisory / training committees.

roz holds the CIC, CIIP, DAE, PIAM designations and is currently working towards her CPII (Certified Professional in Insurance). She is a member of the CIC Society of the National Alliance. She also holds a Certificate in Convention and Meeting Planning from Calhoun College (GA) and attended Elkins Institute where she received her FCC Broadcast License.

She is a member of Delta Master Chapter of Beta Sigma Phi Sorority where she served as Co-Chair/ Treasurer for the June 2012 TN State Convention. In 2011, she served as Co-Chair for the American Cancer Society/ Nashville Relay for Life, which raised over $80,000 for cancer research. She is also active with her East Nashville High School alumni association.

roz is a widow and has three children, five grandchildren and two great-grandchildren. Her interests include: reading, traveling, annual Birthday Girl(s) celebrations, attending Broadway shows with her friends, family outings, and cruising in her SmartCar.

In February of last year, roz fulfilled one of her “bucket list” items by jumping off the top of the Stratosphere Hotel in Las Vegas. The hotel is 108 floors and the drop is 855 feet (free fall). She says it was one of the most thrilling things she has ever done and looks forward to doing it again, at night, so she can see the lights of Vegas.

Debbi loves to garden, perform home renovations, read and spend time with her two cats – Sarah and Phoebe.
2013-2014 Board of Directors

Donna Varin
AIT, CIIP
Region I Vice President

Donna retired on December 1, 2012 after serving 35-1/2 years with Amica Insurance in Lincoln, RI. 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 Associates Degree in Computer Science. In 2003, she obtained both the Associate in Information Technology (AIT) and Certified Professional Insurance Woman (CPIW) designations.

Donna joined NAIW/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 served/chaired committees at every Council Meeting, Regional Conference and International Convention she’s attended since 2001. Donna has also represented the Council as a member of 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 8 years in Greenville. She has one child, Keith, who is a member of the RI Army National Guard and has served in Kuwait. Keith and his fiancée are currently expecting their first child – Donna’s first grandchild. 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 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

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 and she’s looking forward to working on the Executive Board.
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. She holds her agent’s license and was employed (until retirement) as the Operations Manager at Lutgert Insurance, where she oversaw their five offices and eighty plus employees. She recently celebrated her 20th anniversary with the agency. 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 June and is looking forward to enjoying her free time.
2013-2014 Board of Directors

Cindy Prud’homme
AINS, CPIA, CIIP
Region IV Vice President

Cindy Prud’homme is an IT Supervisor for Meadowbrook Insurance Group in Southfield, Michigan. She manages system implementations, large projects, and provides post-implementation support to Meadowbrook’s self-insured and wholesale operations throughout the United States. Cindy manages a team of programmer/analysts. Prior to that, Cindy worked on Meadowbrook’s Business Process Improvement initiative, where she visited Meadowbrook branches around the country, for enhancement and efficiency opportunities in their business process. Cindy has 30+ years of experience in the insurance industry, with an accounting, systems, and operations background. She holds the AINS, CPIA, and CIIP designations and is a licensed P&C producer in the state of Michigan.

Many IAIP members know Cindy from her 2005-2006 service on the National Board of Directors of AMS Users’ Group (now NetVU), chairing the Sagitta Education Committee. There she received the President’s Citation for service in 2007 and the James M. Gibson Service Award in 2008. Cindy was a regular fixture at NetVU conferences, conducting educational presentations on technical subjects and business skills, including Business Presentation Skills and Business Process Improvement. She was a founding member of the Midwest Sagitta Users’ Group, and during her Charter Presidency expanded this ‘local chapter’ to include a territory of seven states.

Cindy is a founding member of the Mid-Michigan Association of Insurance Professionals, where she was the group’s Charter President in 1997. She holds dual membership in the Insurance Association of Metropolitan Detroit, where she also served as President. She has held office and chaired committees for both associations over the years, and was the Insurance Professional of the Year for Insurance Association of Metropolitan Detroit in 2008. She is Past Council Director for the Michigan Council of IAIP, having served 2 terms from 2008-2010 and is now serving IAIP members as the Regional Vice President for Region IV for a second term.

In addition to being a member of the IAIP Board of Directors, Cindy is serving a second year on the Budget & Finance Committee and the Marketing Task Force. During Cindy’s first year on the Board of Directors, she also co-chaired the Conference Review Task Force and served as a member on the Renewal Incentive Task Force, the Benchmarking Study Task Force, and the Website Redesign Task Force.

Cindy has taken Confidence While Communicating two times and has represented the Michigan Council in the Regional competition three times. She now teaches CWC as well as the new Certified Leadership Program. Some members know Cindy from attending her workshop, ‘Bridging the Membership Gap’, which she presented at the New Orleans IAIP Convention; it explored the impact of membership diversity on IAIP local associations. Cindy is a Founders’ Circle member of the Insurance Scholarship Foundation of America and a regular contributor to the NAIW Legacy Foundation.

Cindy doesn’t often know what free time is, but when she finds it, it’s usually spent with her family. Cindy enjoys spoiling her first grandchild, Kennedy, and enjoys cooking, watching NASCAR races, camping, and traveling.

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

Danny has been a member of IAIP for five 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. 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 new role, he is responsible for transitioning several existing books of business to a new policy maintenance system. In November 2013, he will celebrate his fifteenth anniversary with ANPAC.

Danny holds the AINS, AIS, API, ACS, and CIIP 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 has been a member of IAIP for five 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. 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 serves on the Community Investment Panel of the United Way of the Ozarks, volunteers for various events hosted by Big Brothers / Big Sisters, and runs marathons as a member of Team World Vision. 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, travelling, sampling new wines, and watching movies.
Sonya Embry
CISR, CPIW, DAE
Region VI Vice President

Sonya Embry has been a member of NAIW/IAIP for 19 years, and is a member of the Insurance Professionals of Tulsa. Sonya received the Insurance Professional of the Year award from her local association in 2010 and won at the regional level in 2011. She served as Oklahoma Council Director in 2010-2011. Sonya has served in a variety of positions at the Regional, Council and Local levels. She currently serves as Region VI Vice President and will serve again during the 2013-2014 term.

Sonya has worked at Mid-Continent Group for 22 years, and is the AP/AR Manager in the Agency Accounting department at the main office in Tulsa, Oklahoma. Her management experience includes overseeing the monthly account current and closing process; monthly reports to senior management; premium taxes, sign checks, agent portal administrator; and managing 4 employees. Her current responsibilities include assigning new Agents, when applicable; administration duties for CFO, assisting staff when needed, gathering information for auditors for her department, and training staff on premium taxes.

Sonya plans to start working on her CIC designation this year. She has taken a variety of NAIW/IAIP courses. Sonya has taught three NAIW classes locally -- Confidence While Communicating (CWC), Leadership Development and Making a Difference: Ethics and the Insurance Professional and two NAIW I Can! Series classes at regional, LTC: 101 and The Facts of “Life.”

Sonya has an Associate Degree in Accounting from Tulsa Community College and is currently taking an online degree program with one class (Auditing) left in the Fall. She plans to graduate in the Fall 2013 with a Bachelor’s Degree in Accounting and Minor in Management from Northeastern State University at the Broken Arrow, Oklahoma campus.

Sonya loves to cruise on ships to warm places, go to the lake, and watch movies. Sonya enjoys local runs/walks and hopes to get involved in more after completing college. She volunteers to help setup for the Tulsa Boys Home “Run for the Roses” event, Eastern Oklahoma Food Bank, and local Redefine program to build 6th grade girls’ self-esteem at Edison Middle School in Tulsa, OK. She coordinates donations for other non-profit charities, such as United Way at work and IPT events. Sonya plans to go on another cruise in March 2014 with her family. Also, she enjoys taking Sign Language classes.

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 in a six-state area (WI, MN, ND, SD, IA and NE). She created, developed, facilitated / trained various educational programs for agents and their team members, as well as operations center employees in the insurance field. She has worked with various leaders of the insurance industry from service levels up to senior vice presidents on personal and professional development and goal setting programs.

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 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, 4 parts of the LUTCF, and 4 parts of the CPCU. Angie was variable licensed for her company, holding the Series 6 and 63
2013-2014 Board of Directors

Katharine Nohr
J.D.
Region VIII Vice President

Katharine M. Nohr, J.D., the author of Managing Risk in Sport and Recreation: The Essential Guide for Loss Prevention, is a principal for Nohr Sports Risk Management, LLC and Claim Crazy, Inc. After serving as a name partner in a prominent Honolulu insurance defense litigation firm for 19 years, she began her own law practice, the Law Offices of Katharine M. Nohr, LLC in 2007. Ms. Nohr is a former Honolulu District Court Judge (per diem), is a trained mediator and currently serves as an arbitrator for Hawaii’s Court Annexed Arbitration Program. Ms. Nohr, a former triathlete, served as Regional Coordinator of Officials for USA Triathlon (“USAT”) from 2004 to 2012 and was previously an appellate hearings officer for USAT. Ms. Nohr earned a Bachelor of Arts degree in political science from the University of Washington in Seattle and her Juris Doctor from the University of Utah College of Law in Salt Lake City.

Ms. Nohr has been a member of Honolulu Association for Insurance Professionals (“HAIP”) since 2002, serving as president and Hawaii State Council Director in 2006-2007. She was awarded International Insurance Professional of the Year and Insurance Professional of the Year for Region VIII in 2012. She earned Rookie of the Year in 2003-2004 and the AAMGA award in 2005 from her local association. She won the CWC contest and represented Hawaii at the Region VIII Conference in Dublin, CA in 2003. Ms. Nohr has been very active with the start up of the Healthy Insurance Professionals program, starting with programs at the Region VIII conferences in Honolulu and in Las Vegas in 2012. She was a member of the Healthy Insurance Professionals task force in 2013 and assisted with the programs offered at the IAIP Convention in Orlando in 2013.

Ms. Nohr frequently provides training to insurance carriers, primarily regarding Hawaii no-fault law. She has taught numerous seminars for HAIP on sports and recreation risk management and other insurance topics. From 2010 to 2012, Ms. Nohr traveled to the UK to speak at The Conference on Law Policy and the Olympic Movement at Ithaca College London and in 2012 to speak at the University of Cambridge at the Sport & Society Conference. Ms. Nohr spoke regarding risk management topics as they relate to the Olympic Games in London 2012 and Rio de Janeiro 2016. In May of 2013, Ms. Nohr was invited to speak at a Sport Congress at the University of Erciyes, Turkey on the topic: “Boston Marathon Bombings: Sporting Event Risk Management.” She has also been a keynote speaker at the Midwest USA Triathlon Conference in Chicago, speaking about the topic: “Triathlon Law and Risk Management.”

In her spare time, Ms. Nohr writes novels (“Tri-Angles” and “Free-wheel”—both pending publication), swims laps at the YMCA, hikes, travels, reads, and herds her Siamese cats (Tashi and Bucky). She is a “super-connector” on Linkedin.com, with over 5,000 connections.
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, 4 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 1980’s 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.

Photo credit for Board of Directors photos: Justin Werner
The International Association of Insurance Professionals 72nd Annual Convention commenced on Thursday, June 6, 2013 with more than 400 members and industry professionals in attendance. The 72nd Annual Convention was held at the Caribe Royale in Orlando, Florida.

Throughout the convention, attendees had the opportunity to participate in 17 different educational workshops, a trade show, several networking events, a keynote address, and two business meetings.

The convention kicked off on Thursday with 11 educational workshops held throughout the day. Workshops included insurance industry topics, as well as workshops on building relationships and professional development. Courses from the Certified Leadership program were offered, along with topics on social media, personal strategies, and local association planning, which completed the day. The exhibit hall provided attendees the opportunity to meet with the exhibitors and network. Following the education workshops, the Convention Briefing was held, which included Corporate Partner recognition, Task Force and Committee reports, Delegates Briefing, and the Meet the Candidate session for International Secretary. A Welcome Party with the exhibitors was held that evening where attendees continued to network. During the Welcome Party, nearly $1,000 was raised for the Legacy Foundation, which supports education programs.

Friday continued with five educational workshops throughout the morning. A lunch was held for attendees in the exhibit hall, followed by exhibitor recognition and prize drawings. Friday afternoon, the CWC Speak-off competition was held. Nine regional contestants competed and all gave excellent presentations. Afterward, the First Business Meeting convened where Tish Riley, CIIP, DAE, from Stockton, CA was elected International Secretary. To conclude the meeting, various Task Force and Committee reports were given, and items presented and approved by the Recommendations Committee were discussed and voted on by the delegates.

On Saturday, Erick Burton provided the keynote address on being a “Future Leader,” which was enthusiastically received by the audience. The Second Business Meeting convened thereafter, with various Task Force reports and additional motions presented and voted on by the delegates. After conclusion of the meeting, the Annual Recognition Luncheon was held. During the luncheon, the international award winners and POC scholarship recipient were announced as follows:

**Professional Underwriter of the Year**
Susan Reichardt -- Region V

**Claims Professional of the Year**
Donna Lynn Wiik -- Region I

**Insurance Professional of the Year (co-winners)**
Lara Nelson Miller -- Region III
and
Linda Luka -- Region V
Risk Management Professional of the Year  
Sara K. Skirvin -- Region IV

Rookie of the Year  
Martha Elliott -- Region VII

Confidence While Communicating Speak-Off  
Brenda McDermott -- Region V

POC Scholarship  
Rachel Shubert -- Region V

Scholarship recipients from National Alliance, The Institutes, and the International Risk Management Institute (IRMI) were also announced and those in attendance were recognized.

Following the award and scholarship presentations, the 2012-2013 Board of Directors were recognized for their leadership during their term. Outgoing President, Penny Haworth-Rich, thanked the board members for their service and also thanked attendees for their support throughout the year. Past President Cheryl Bailey then installed the 2013-2014 officers as follows:

President - Jane Densch, CPCU, AIC, ARP, ARe, CPIW, AIS -- Denver, Colorado.
President Elect - Roz Horton, CIC, CIIP, DAE -- Nashville, Tennessee.
Vice President - Debbi Kuhne, AAI, AIC, AIS, CIIP, DAE, CEIS -- Torrington, Connecticut.
Secretary - Tish Riley, CIIP, DAE -- Stockton, California.
Region I Vice President - Donna Varin, AIT, CIIP -- Greenville, Rhode Island.
Region II Vice President - Brenda Lawhorn, CIC, CPIW, AINS -- Waldorf, Maryland.
Region III Vice President - Betty Curry, CPSR, CPIA, CPIW, DAE -- Naples, Florida.
Region IV Vice President - Cindy Prud’homme, AINS, CPIA, CIIP -- Grand Blanc, Michigan.
Region V Vice President - Danny Douglas, AINS, AIS, API, ACS, CIIP -- Springfield, Missouri.
Region VI Vice President - Sonya Embry, CISR, CPIW, DAE -- Tulsa, Oklahoma.
Region VII Vice President - Angie Sullivan, AIC, CPIW -- Lincoln, Nebraska.
Region VIII Vice President - Katharine Nohr, J.D. -- Kaneohe, Hawaii.
Region IX Vice President - Gail Welfringer, CPIW -- Bothell, Washington.

After being installed, Densch gave credit to those leaders who came before her and inspired her. She encouraged all members in attendance to look toward the future and help make the association successful. Each member of the Board of Directors then spoke about their goals for the upcoming year. A dessert reception followed the luncheon with fellowship and networking.

The International Association of Insurance Professionals would like to extend our sincerest thanks to all attendees, sponsors, exhibitors, and guests for their support during this event. We look forward to the upcoming year and hope you will make plans to join us in San Diego, California at the Doubletree Mission Valley, June 5-7, 2014 for yet another convention to remember.
The Young New Professionals meet to discuss plans for the upcoming year.

Members visit with exhibitors.

Carla Huddlestone from Wells Fargo accepts a Corporate Partner appreciation award.

Danny Douglas holds a workshop to discuss creative ways to market the association.

Members listen attentively to a workshop presentation.

Guest speaker Erick Burton motivates the group with tips on becoming a leader.

Members enjoy a discussion led by Emily Huling.

Communicating with Confidence Speak-Off contestants.
The Young and New Professionals group show their enthusiasm.

Members attend the Annual Recognition Luncheon.

Angelia Poyner presented a class on the Certified Leadership Program.

Members enjoy the Young and New Professionals mixer.

Presenter James McCartney, from Accurate Data Partners, speaks to members.

Members listen attentively to presenter Byron Sabol.

Members in the lobby walk to workshop sessions.

The Young and New Professionals group show their enthusiasm.

Photo credit for convention photos: Justin Werner
International Award Winners

Professional Underwriter of the Year
Susan Reichardt - Region V

Claims Professional of the Year
Donna Lynn Wiik - Region I

Insurance Professional of the Year
Co-winners - Linda Luka - Region V & Lara Nelson Miller - Region III

POC Scholarship
Rachel Shubert - Region V

Risk Management Professional of the Year
Sara K. Skirvin - Region IV

Rookie of the Year
Martha Elliott - Region VII

Confidence While Communicating
Brenda McDermott - Region V
At Paul Davis, the trust you put in us every day is fundamental because we recognize that the work we do reflects on you. Your customers are treated as our own, so you’ll know they are always taken care of. And we work with adjusters with a commitment to ensure a smooth process throughout every loss, every time.

Why do 20,000 agents trust their policyholders to us? Because the difference is not in what we say, but in how we perform.