THE REGULATOR®
SPRING 2015
INSURANCE REGULATORY EXAMINERS SOCIETY

TRIA Renewed … at Long Last

By Eric Nordman, Director of Regulatory Services and CIPR

As I began to write this article in early January, I was not sure what to make of the unbelievable politics getting in the way of implementing a practical and cost-effective solution to address a major risk. I am talking about the failure to reauthorize the Terrorism Risk Insurance Program. As the ball dropped in Times Square, many businesses in the Eastern Time Zone experienced a significant change in insurance coverage for the risks they face. At the stroke of midnight the Terrorism Risk Insurance Program went away leaving many unsuspecting businesses with a gap in their risk-management toolkit.

Luckily, the dawn came without a major terrorist attack so everything on the surface seemed bright. However, people quickly came to realize Congress was playing with fire by failing to renew the program. When the World Trade Center buildings collapsed on Sept. 11, 2001, the insurance industry's perspective about the risk of loss from acts of terrorism changed dramatically. It became apparent a determined terrorist could cause substantial damage under the right circumstances. The definition of substantial damage shifted from millions of dollars to billions of dollars.

After the Twin Towers fell, the reaction of the insurance industry was predictable. They moved to limit their exposure to losses caused by terrorists. The nation's airlines received notices of cancellation within a week. Other business owners were soon to follow as the insurance industry tried to figure out what to do.

State insurance regulators reacted to the looming coverage crisis by meeting to discuss a common solution. As a result of the conversations, an uneasy truce was reached. In December 2001, the NAIC published a model bulletin for states to use to provide at least some level of terrorism coverage in light of Congressional failure to act at the time.

The solution outlined in the model bulletin provided for insurers to cover acts of terrorism as long as they did not reach a catastrophic level. For property insurance, the exclusion for acts of terrorism would only apply if the acts of terrorism resulted in industry-wide insurance losses in excess of $25 million for related incidents occurring within a 72 hour period.

The solution outlined in the model bulletin provided for insurers to cover acts of terrorism as long as they did not reach a catastrophic level.

Also allowed were exclusions for nuclear, biological, chemical or radiological events (NBCR). The allowed exclusion for commercial liability insurance was a bit more complicated. It kept the $25 million and 72 hour thresholds, but added an alternative of 50 or more people sustaining death or serious physical injury.

□ continued on page 2

WHAT'S INSIDE

MARK YOUR CALENDAR

May 13-15, 2015
MCM® Designation Course
Des Moines, IA

July 19-22, 2015
IRES CDS & Regulatory Skills Workshop | Charleston, SC

□ *Upcoming Events* - continued on page 14

TRIA Renewed – continued from **page 1**

In 2002, Congress reacted to the lack of a robust market for insuring acts of terrorism by creating the Terrorism Risk Insurance Program. The successful common sense program was renewed twice (2005 and 2007). While the program reauthorizations occurred late in the year, neither time did the program authorization expire as they did when 2014 drew to a close.

On Dec. 30 2014, a Treasury spokesperson had this to say about the Terrorism Risk Insurance Program, "The Terrorism Risk Insurance Act is important to our national security and essential for continued economic growth. When Congress returns next year, we hope it acts swiftly to pass a long-term reauthorization consistent with the bipartisan, bicameral TRIA (Terrorism Risk Insurance Act) compromise to maintain a functioning and affordable insurance market for terrorism risk. While we hope for a speedy renewal, until Congress acts, Treasury will wind down the program consistent with its expiration."

It seems incredible one departing Senator (Tom Coburn (R-OK)) was able to prevent the enactment of a bill with such broad bipartisan consensus. However, his parting shot was to block the passage of the bill, not because he was opposed to the Terrorism Risk Insurance Program, but rather he was opposed to Title Two dealing with the National Association of Registered Agents and Brokers (NARAB).

When the new Congress convened, passage of the TRIA was top of the list for bipartisan consideration. H.R. 26—The Terrorism Risk Insurance Program Reauthorization Act of 2015—passed the House of Representatives by a vote of 416-5 on Jan. 7, 2015. The next day, the Senate voted 94-4 to adopt the bill. It went to President Obama's desk where he signed it into law on Jan. 12, 2015. With the signing one would think everything was once again right with the world. However, there were some loose ends needing attention.

When the new Congress convened, passage of the TRIA was top of the list for bipartisan consideration.

The revised Terrorism Risk Insurance Program does contain some changes. The following list identifies several of the more important changes to the program:

- The program was extended through Dec. 31, 2020.
- The Insurer Deductible was set at 20% of an insurer's direct earned premium of the preceding calendar year and the federal share of compensation was set at 85% of insured losses that exceed insurer deductibles until Jan. 1, 2016. Then the federal share is decreased by one percentage point per calendar year until it reaches 80%.
- The certification process was changed to requiring the Secretary of the Treasury to certify acts of terrorism in consultation with the Secretary of Homeland Security instead of the Secretary of State.
- The program trigger was amended to apply to certified acts with insured losses exceeding:
  - $100 million for calendar year 2015,
  - $120 million for calendar year 2016,
  - $140 million for calendar year 2017,
  - $160 million for calendar year 2018,
  -$180 million for calendar year 2019,
  and $200 million for calendar year 2020 and any calendar year thereafter.
- The mandatory recoupment of the federal share through policyholder surcharges increased to 140 percent from 133 percent.
- The insurance marketplace aggregate retention amount was established at the lesser of $27.5 billion, increasing annually by $2 billion until it equals $37.5 billion, and the aggregate amount of insured losses for the calendar year for all insurers. In the calendar year following the calendar year in which the marketplace retention amount equals $37.5 billion, and beginning in calendar year 2020, it is revised to be the lesser of the annual average of the sum of insurer deductibles for all insurers participating in the program for the prior three calendar years, as such sum is determined by the Secretary of the Treasury by regulation.
- The Secretary of the Treasury is required, not later than nine months after the date of enactment of the Act, to conduct and complete a study on the certification process, including the establishment of a reasonable timetable by which the Secretary must make an accurate determination on whether to certify an act as an act of terrorism.
- Insurers participating in the program are required to submit to the Secretary of the Treasury for a Congressional report to be submitted June 30, 2016 and every June 30 thereafter, information regarding insurance coverage for terrorism losses in order to evaluate the effectiveness of the program. The information to be provided includes: lines of insurance with exposure to terrorism losses, premiums earned on coverage, geographical location of exposures, pricing of coverage, the take-up rate for coverage, the amount of private reinsurance for acts of terrorism purchased and such other matters as the Secretary considers appropriate. This information may be collected by a statistical aggregator and in coordination with State insurance regulatory authorities.
- The Comptroller General of the United States is required to complete a study on the viability and effects of the federal government assessing and collecting up-front premiums and creating a capital reserve fund.
- The Secretary of the Treasury is required to conduct a study not later than June 30, 2017 and every June 30 thereafter to identify competitive challenges small insurers face in the terrorism risk insurance marketplace.

continued on page 3

TRIA Renewed – continued from **page 2**

- The Secretary of the Treasury is required to appoint an Advisory Committee on Risk-Sharing Mechanisms to provide advice, recommendations and encouragement with respect to the creation and development of nongovernmental risk-sharing mechanisms. The Advisory Committee will be composed of nine members who are directors, officers, or other employees of insurers, reinsurers or capital market participants.
- The terms "program year" and "transition period" are changed to "calendar year" throughout the law.

Insurance regulators tracked the progress of H.R. 26 as it was being considered and issued a model bulletin for regulators to communicate a consistent message to insurers about changes to the program and steps needed for insurers to comply with disclosure notices and changes to policy forms.

On Feb. 4, 2015, the Treasury published interim guidance concerning the Act. The interim guidance helped calm frayed nerves. It provided an extension of the deadline for providing disclosures and offers of coverage to Apr. 13, 2015. This allowed insurers some breathing room to comply with the requirements in the Act. The Treasury also advised the model disclosures in the NAIC Model Bulletin are consistent with the disclosure requirements of the Terrorism Risk Insurance Program. The Treasury provided additional guidance to assist insurers with understanding the changes made to eliminate the required disclosure at time of purchase and what to do under various coverage and offer scenarios.

The interim guidance helped calm frayed nerves. It provided an extension of the deadline for providing disclosures and offers of coverage to Apr. 13, 2015.

With the legislation on the books, insurers are working through the backlog of pending disclosures, offers and explanations to policyholders. Next on the horizon is working with various federal agencies on studies of several topics. Included on the list are: the study of the certification process by the Treasury; the collection of data to evaluate the effectiveness of the program; conducting a study on the viability of collecting up-front premiums and creating a capital reserve fund; and conducting a study on competitive challenges small insurers face in the terrorism risk insurance marketplace. As you can see, there is much work before us. ■

Eric Nordman, CPCU, CIE, is the director of the NAIC Regulatory Services Division and the CIPR. He directs the Regulatory Services Division staff in a wide range of insurance research, financial and market regulatory activities, supporting NAIC committees, task forces and working groups. He has been with the NAIC since 1991. Prior to his appointment as director of the Regulatory Services Division, Nordman was director of the Research Division and, before that, the NAIC's senior regulatory specialist. Before joining the NAIC, he was with the Michigan Insurance Bureau for 13 years. Nordman earned a bachelor's degree in mathematics from Michigan State University. He is a member of the CPCU Society and the Insurance Regulatory Examiners Society.

TNC Insurance Regulation: A Snapshot

By Joel Laucher

This article on Transportation Network Companies (TNC's) –Uber. Lyft, Sidecar, etc. – is already out of date. That's right; developments in the insurance arena for the ride-sharing technology companies have been evolving so quickly over the last few months that it's hard to keep up.

What would you expect from a business model that is labeled a "disrupter" by so many articles in the media because it upends a traditional business activity? In this case, the business paradigm being interrupted is an iconic one, the yellow taxicab. A taxi is an image virtually everyone can bring to mind. And I think that's what makes this particular market shift so interesting. While other disruptive business models may be taking on how marketing is conducted or how data is stored, this one is playing out right in front of us on the streets.

That's right; developments in the insurance arena for the ride-sharing technology companies have been evolving so quickly over the last few months that it's hard to keep up.

It's likely that you may have participated by taking a ride in a TNC vehicle. Or maybe your cousin drives for one of the TNC's to earn a little extra money. Or a

living. And if he is, does he have insurance coverage? How exactly is that livery exclusion in his personal auto policy worded?

Which is how we are drawn in as regulators and insurance professionals. There have been gaps in coverage for TNC drivers, passengers and pedestrians. There still are gaps in coverage. Because regulation of livery operations like taxis is fragmented - often involving municipalities, sometimes states, sometimes

continued on page 4

Meet Randy Helder

By Kelly Ann Helder

It's not every day I get to introduce my husband to members of our insurance family. After 25 years of marriage, job transfers, business travel and the highs and lows that come with any life, I am pleased to give you the highlights of a life well-lived by a man who is honest, kind and, well, tall.

Randy Helder CPCU, AIE, ARe, AIC, AU joined IRES in 2009, while working as a Market Analysis Manager. He was voted onto the IRES Board of Directors in 2014 and was asked to serve on the Executive Committee as Chair of the Education Committee.

He graduated from Cal State Fullerton with a BA in Political Science and immediately began work for a personal lines carrier. Randy has had a long and varied career in the insurance industry working in every aspect from claims, compliance, Re-insurance and is currently working as the Assistant Director of Market Regulation at the NAIC in Kansas City.

With a strong view of ethics in the industry, Randy believes continuing education is a vital component of any professional career. He has enjoyed being involved in the insurance industry and providing his expertise to a way of life he was born in to being the son of William AC Helder CPCU, former president of Bayside Management Company.

Randy's hobbies include spending time with his family and Astro-photography. He is an avid baseball fan and has been spending the last several years visiting baseball fields around the country with his son, Nate. On warm summer weekends, he can be found floating on his boat with family and friends. ■

TNC Insurance Regulation – continued from **page 3**

countries - the regulatory response is fragmented. But there is a flurry of regulatory activity going on right now across the nation and across the world.

Most recently, the NAIC's "Sharing Economy Working Group" under the leadership of California Insurance Commissioner Dave Jones (my boss!) created a "white paper" on Transportation Network Companies. It is an informative piece and a snapshot in time of the state of affairs of TNC regulation. Since that snapshot is still relatively fresh, I'll refer you to that: http://naic.org/store/free/TNC-OP-15.pdf

While other disruptive business models may be taking on how marketing is conducted or how data is stored, this one is playing out right in front of us on the streets.

For those that don't want to delve into that much detail, I'll provide this simple summary. Coverage for the TNC's themselves has been written by surplus lines insurers. A $1,000,000 liability limit is about where that coverage has generally been pegged. That coverage may include Underinsured/Underinsured Motorist coverage and it may include Collision coverage – these possibly may be dependent on whether the driver's own policy includes such coverage. Although many personal auto policies exclude coverage for those driving for TNCs, some personal auto coverages have livery exclusions that arguably may be read to not exclude the time a driver has the application on but has yet to pick up the passenger.

As the TNC exposure has become clearer to personal lines insurers, they are now choosing more deliberately whether they want to be involved in this hybrid of personal and commercial use of the car. Most don't, but some are starting to write coverage for what is commonly called period 1 – the time from when the TNC app is turned on until a match is made with a prospective rider.

In fact, the major TNCs and a number of major insurers have recently proposed a model legislative piece that would specify limits of liability limits of $50,000 per person, $100,000 per occurrence, and $25,000 or $30,000 for property damage for period 1 depending on the state. This model also suggests that TNCs maintain primary coverage during Period 2 (match-made until pick-up of the passenger) and Period 3 (pick-up to drop-off) with liability limits of at least $1 million. These limits are in-line with those adopted by some of the states that already have had legislation on this issue.

What to expect: further legislation, forms filings (tightening exclusions for some insurers, expanding the coverage for others), and a number of experiments in rating plans as insurers figure out how to meld the pricing for TNC driving with personal driving. There will be many practical questions to resolve: How to separate and verify personal miles from TNC mileage for rating purposes? Will there be sufficient cooperation during the claims handling process to determine when the personal auto coverage terminated and the commercial TNC initiated? And what if there were multiple TNC apps engaged?

What to ponder – will we be going through this exercise for homeowners coverages soon with the advent of similar apps that allow homeowners to rent out rooms in their homes like hotels?

So, I think I can leave it at that for now. Or I can start the article over and find out what has changed since I wrote that first line ... . ■

Joel Laucher joined the California Department of Insurance in 1985 as a market conduct examiner. Previously, he had worked as a commercial lines underwriter.

At the Department he has served as a Division Chief for the Market Conduct Division and Consumer Services Division and is currently Deputy Commissioner of the Rate Regulation Branch. Joel is a 1978 graduate of UC Santa Cruz with a degree in Literature. Which explains everything else.

The Effects of Cyber Attacks on the Insurance Industry

By Thomas E. Hampton, Senior Advisor, Dentons US LLP

Introduction

In the past few years, there has been a significant increase in the number of cyber-attacks affecting the personal information and in some cases the credit card data of customers. Major retailers such as Target, Home Depot, Neiman Marcus and Staples have reported computer breaches, with the cyber-attack on Target being the largest in terms of financial loss. In its Second Quarter 2014 financial filing with the SEC, Target reported that the cost of the cyber-attack had reached $182 million in breach-related costs, with only $70 million of those costs being covered by insurance. It is estimated that ultimate cost of the Target cyber-attack may reach approximately $1 billion. These cyber-attacks have caused reputational damage to these companies and have indirectly translated into loss of revenues. The cyber-attack against Target ultimately resulted in the resignation of the Company's CEO and Chairman of the Board as well as the Senior Information Technology Officer.

These cyber-attacks have caused reputational damage to these companies and have indirectly translated into loss of revenues.

As we move into 2015, a number of significant cyber-attacks are continuing to occur. Recently, Anthem Inc., revealed that a data breach had exposed personal information of approximately 80 million customers and employees. Cyber-security threats should be a concern to all companies that have internet connections. As former FBI Director Robert Mueller states, "There are only two types of companies: those that have been hacked, and those that will be. Even that is merging into one category: those that have been hacked and will be again."

Experiencing a cyber-attack can be a very costly to a company. In situations where companies have experienced a data breach involving personal information, a majority of states have enacted statutes requiring a notification process. In some 46 states and the District of Columbia, the law authorizes a private rights of action for failure to comply with the notification requirements. There are also laws enacted in states that are similar to the Federal Trade Commission's Safeguard Rule. These standards are intended to: insure the security and confidentiality of customer records and information, protect against any anticipated threats or hazards to the security or integrity of such records and protect against unauthorized access to or use of such records or information that could result in substantial harm or inconvenience to any customer.[1] These types of consumer notification laws as well as rules from the US Securities and Exchange Commission and Health Insurance Portability and Accounting Act of 1996, regarding the release of confidential information, have encouraged companies to implement a risk management plan to safeguard information for the protection of their customers.

1 Description of Federal Trade Commission's Safeguard Rule as shown on the FTC website.

Some of the other direct expense involved with a cyber-attack includes hiring an independent information security forensic firm, sending out required notices to customers, providing identity theft and credit monitoring services to customers, establishing or hiring call center staff to assist customers as well as dealing with crisis management services. One cost included in data remediation process is the cost companies may be forced to pay the hacker to have their data returned or to gain access to their computer system.

Establishing a Cyber-Security Risk Management Process

In accordance with provisions included in the Sarbanes-Oxley Act, publicly-traded companies are required to establish an Enterprise Risk Management framework, which should include cybersecurity risks. However, there were no industry standards or best practices established for cybersecurity risk management programs.

In February 2014, the National Institute of Standards and Technology ("NIST") issued the first version of the "Framework for Improving Critical Infrastructure Cybersecurity" pursuant to Executive Order 13636 issued by President Barak Obama. The establishment of the prescribed voluntary set of standards for developing a cybersecurity risk management type framework may be the first step in mitigating cyber-attack risks. The three main elements described in the document are the Framework core, tiers and profiles. The core includes five functions; identify, protect, detect, respond and recover, which when used in concert allows any company to understand and shape its cyber-security program. The tiers describe the degree

continued on page 6

The Effect of Cyber Attacks – continued from **page 5**

to which a company's cybersecurity risk management meets the goals detailed in the framework. The profile helps companies progress from a current level of cybersecurity knowledge to a target improved state that meets business needs. When considered together, this Framework provides a high-level, strategic view of the lifecycle of an organization's management of cybersecurity risk[2].

An effective cybersecurity risk management core requires a company to establish an on-going process of identifying information assets, protecting, assessing, and responding to cybersecurity risk. For many companies, this initial risk assessment will include (1) Identifying Information Assets, (2) Locating where Information Assets are being housed in the Company, (3) Assign a rating to your Information Asset List based on the amount of damage caused if the information is disclosed, (4) Develop a Threat Model, and (5) Finalize Plan.

With the increased number of cyber-attacks, you would think that most if not all cyber breach incidents are being reported and process through some type of cybersecurity risk management program to determine the program effectiveness. However, some cyber breaches simply go unreported especially if the breach did not cause a loss of customer personal data or proprietary information. A cyber breach may be as little as an employee losing a laptop computer or flash drive with stored company information. Some of these incidents are resolved without any report being sent to the Chief Information Officer ("CIO"). This is not the case with security hacks of a company system, which are considered an elaborate penetration where information assets have been compromised. One of the latest computer hack incidents occurred against Sony Pictures Entertainment Inc. The hackers stated that the impetus of the cyber- attack was the release of the controversial movie, "The Interview," which depicted the North Korean Supreme Leader Kim Jong Un in this comedy. Even when the latest generation of safeguards and protections are implemented, data security can be undermined when employees or contractors fail to follow those safeguards. The major point is not all cyber breaches reach the magnitude of a computer hack, but identifying all cyber security breaches – whether intentional or unintentional – are important in developing an effective Cybersecurity Framework.

Growth of the Cyber Insurance Market

With the risk of cyber-attacks increasing, the cyber insurance market has grown exponentially as well. Marsh & McLennan Companies estimates that the U.S. cyber insurance market had estimated gross premiums of $2 billion in 2014 and the premiums from cyber insurance policies should continue to grow at 20 to 50% a year. It is estimated that over 50 insurers are currently offering specialized cyber-security insurance policies. Insurers that are providing this coverage have commenced the process of better understanding cyber risk data exposures by engaging computer experts to test the computer systems of policyholders for breach penetration weaknesses. As insurers gain more information on the appropriateness of pricing models of their cyber-security insurance policies, they have been using a couple of methods to limit their loss exposures; one is to market specialized cyber-security policies that underwrite one or two the cyber-security risks.

Even with this increase in insurance capacity, there has been a challenge for companies attempting to transfer their cyber-attack risk. Insurers that are marketing cybersecurity insurance coverage are limiting their products to a particular cyber risks or to a particular industry. It is analogous to going to a restaurant and buying your dinner a la carte. Breach remediation coverage is sold separately from loss of income due to a company's website being inoperable or some other business interruption risks. Therefore, if a company decides to insure its breach remediation risks, such as the cost of increasing its call center to respond to customer inquiries or provide credit monitoring services to customers, or the cost of having its network brought back to operational status, the cost for each risk will be quoted separately. This practice has caused companies to purchase several policies in order to buy insurance coverage for the preferred amount of cybersecurity risk the company would like to insure. Insurers are providing policies with coverage for losses resulting from reputational risk, using the business interruption policy mantra, even though these risks are somewhat different. As more cyber-attacks occur and the risk exposures are identified by companies, you can anticipate that more insurance products will be developed.

The other method used to transfer the cybersecurity risk is to have the Company's risk managers or brokers review the language embedded in some of the company's current policies to determine if these policies include language that may provide coverage for particular type of cyber-attack incidents. Some of the policies, due to ambiguous provisions, may provide a company protection from cyber-attack risks. These policies include the Commercial General Liability (CGL) Policy, which in some cases provide coverage for leaking of private or confidential information when a company had a computer breach, Crime Insurance policies and possibly policies covering Employment Liability. Other policies, like Fiduciary Liability insurance coverage, provide coverage to protect and defend companies that are administering employee benefit plans. This coverage indemnifies companies for notifying employees of a data security breach and it covers the cost of any civil money penalties involved.

It should be noted that although some insurers have honored some of these claims, other insurers have denied coverage and have used the courts to determine if the cybersecurity risk claims

continued on page 7

2 Framework for Improving Critical Infrastructure Cybersecurity, Version1.0, Section 1.1 Overview of Framework dated February 12, 2014

The Effect of Cyber Attacks – continued from **page 6**

were intended to be covered by these policies. One of these lawsuits filed in New York State involved Sony and two insurance companies that provided CGL policies to the company. These two insurers argued that the cyber data breach that occurred against Sony PlayStation network should not be covered since Sony did not have any intentional or affirmative involvement with the hackers involved with the data breach. The Coverage B "personal and advertising injury" provisions included in the CGL policy would only apply if Sony was involved in the data breach.

Conclusion

Cybersecurity is a major risk for all companies with an internet infrastructure, regardless of the company's size. With the increase in cyber-attacks and the belief that no company is entirely safe from breaches, it is imperative that companies include cyber-security risk management processes in their ERM framework. The NIST Cybersecurity Framework is a good process to implement.

Cybersecurity is a major risk for all companies with an internet infrastructure, regardless of the company's size.

One of the key components in developing a Cybersecurity Framework is identifying the company's information assets and risk exposures to determine the company's risk tolerance and risk retention appetite levels. In this current environment, the transfer of cybersecurity risk through an insurance contract should be a key component in any risk management strategy. The use of insurance policies should not be limited to large companies. At the February 10th, 2015, Federal Advisory Committee on Insurance (FACI) meeting in Washington, DC, Deputy U.S. Treasury Secretary Sarah Bloom Raskin stated, that although cyber risk insurance market is growing tremendously, "Cyber insurance take-up rates at smaller companies have not grown." Secretary Raskin asked FACI to respond to issues on why small companies are not buying the much needed cyber insurance at the similar rate of large companies.

Insurance companies are not immune to cyber-attacks, and this fact is becoming more of a challenge to insurance regulators. States insurance regulatory agencies have begun to develop a process to regularly assess the cybersecurity preparedness of their licensed companies. Also, the National Association of Insurance Commissioners (NAIC) have established a new 2015 National Cybersecurity Task Force that will focus its efforts on monitoring developments in the area of cybersecurity, and collecting information on cyber-liability being issued in the market. The Task Force will identify critical infrastructure assets at the NAIC and state insurance agencies.

As insurance regulators get more involved in assessing the cybersecurity preparedness of insurers, the monitoring of a company's cyber-security risk management program should be incorporated in the examiners financial analysis and market conduct examination profiles. Examiners are responsible for monitoring and assessing the financial and market conduct activities of licensed companies. With the tremendous financial loss that could be experience by an insurer due to a data breach, examiners should be responsible for reviewing a company's Cybersecurity Framework, determine what type of procedures a company has in place to mitigate any cyber-attacks and review the company's remediation plans. Although sending statutory notices to customers and employees concerning a data breach is important, the best strategy is verifying whether a company's framework is sufficient to limit data breaches in the first instance. ■

Thomas E. Hampton is a Senior Advisor in Dentons Insurance Regulatory Practice. He works with clients on Financial Regulatory and Captive Insurance projects. He is located in the Washington, DC office. thomas.hampton@dentons.com.

Member News

Announcing: Featured IRES Member Mr. Sandy P. Fay

Sandy is a partner at the law and governmental consulting firm of Colodny Fass. They are based in South Florida, with the Tallahassee office just one block from Florida's capitol. Sandy practices insurance regulatory law, which includes providing counsel in corporate transactions, administrative procedures and a variety of issues such as insurance licensing, compliance and solvency issues.

Sandy joined IRES in July 2011. He said the reason he joined was IRES' mission to ensure professionalism and integrity is a fundamental cornerstone of the insurance industry, which is a major economic driver. With all the educational and training opportunities afforded by IRES, this organization presents a unique networking opportunity to learn more about the high standards imperative to our nation's top regulators and fellow IRES members.

Through IRES, Sandy has expanded his knowledge of examination processes and procedures, and certainly learned more about the industry as a whole.

When asked about what he likes about being an IRES member, Sandy said that particularly with the advent of global regulatory convergence, he likes the broad scope of information and news available to IRES members.

Sandy is married, with two sons. They enjoy travel and sports, and are involved in Scouting.

Thank you, Mr. Sandy Fay, for being our Featured IRES Member, and sharing some of your story.

Contact information for Mr. Fay is available in the IRES Member Directory.

Cyber Security Enterprise Programs: The Devil is in the Details

By Alan Gutierrez-Arana

Background

On almost a daily basis, we see and hear about a new data breach in all the industry verticals. While not so long ago, this type of illegal activity was mostly observed in the financial institution realm and conducted against payment instruments like credit and debit cards, today we see more and more attacks directed against companies that conduct business around Personally Identifiable Information (PII) or electronic Protected Health Information (ePHI); this targeted activity directly impacts the insurance industry in all its modalities (Life, P&C, Healthcare, etc.) and, as we have all seen in recent cases, it has only shown signs of growth. While the common tendency is to believe that hackers' priority is mainly financial information that provides a quick return, PII and ePHI value in the black market of information is on the rise. According to recent studies on the trends of sites that are used to sell and exchange stolen data, information like social security numbers, full names and addresses are trading at higher prices than credit and debit cards.

Are the IT controls truly pervasive?

It is a common procedure (and part of the financial and market conduct examination handbooks published by the NAIC) to request information around information security policies and procedures, business continuity and disaster recovery plans as part of the field activities conducted by the States during exams; information technology specialists assist the lead examiners in reviewing the documentation that provides details around the controls that the insurers has implemented to protect its costumers PII and ePHI, depending on the line of business. While we can feel comfortable from a control objective perspective that the company has designed security and privacy controls in an effective manner, why do data breaches continue to occur? If companies present documentation that is satisfactory from a compliance perspective and during walkthroughs and interviews staff appears to have a good grip around the systems and the company's data repositories, why is a common scenario the fact that data breaches take a significant amount of time to be discovered?

According to recent studies on the trends of sites that are used to sell and exchange stolen data, information like social security numbers, full names and addresses are trading at higher prices than credit and debit cards.

It is common to notice during audits and exams that attention is paid to design controls that address objectives established by well-known frameworks like COSO and COBIT, but when we jump into the operational effectiveness of such controls, are we looking to the entire landscape, or are we focusing on the "logical reach" of these controls? I'll explain myself with a simple example: user access management policies and procedures, when designed in an effective manner, address the processes on how users must be on-boarded, modified or terminated in a specific system or application. Common audit and examination process is to observe samples of user authorization forms or other type of evidence that could demonstrate that the policies and procedures are being followed by the insurers' employees; when we feel that accountability is demonstrated, we tend to consider that the controls were designed in good fashion and are operating effectively.

Looking at the "Rabbit's Hole"

Perfect. We reviewed our policies and procedures, interviewed the process owners and inspected our samples; we feel confident that the right due diligence has been conducted…do we? Have you asked about how the information security policies and procedures apply and are enforced over vendors and third party service providers that have access to the company's systems? Did you gain comfort around how remote users are logging and accessing critical information in the company's systems? Is the company outsourcing and/or off-shoring some of its information technology functions or business processes? Were the risks associated with these activities taken in consideration in the controls deployed by the insurer?

Yes, you are now looking at the rabbit's hole … .

Effective Cyber Security Programs

In today's world, cyber security is the term of the day for all industry verticals; companies are revamping their information security policies and procedures, senior management and boards of directors are asking the "uncomfortable questions" (are we REALLY secure?) to their information technology and security groups. As auditors and regulators, we must join the chorus and ask questions like:

- Have you established malware and virus controls?

continued on page 9

Cyber Security Programs – continued from **page 8**

- Do the company's systems development and change management process to consider secure code development measures and standards?
- Is the staff trained and aware of the latest techniques and weaknesses exploited by hackers?
- Is the company conducting *effective* monitoring and review of the logs generated by critical systems and any security tools? (Please note the emphasis in EFFECTIVE.)
- Are penetration testing and vulnerability scans conducted in a periodic and pervasive manner to test the company's systems defenses?
- Is there a mature third parties' access management program in place?
- Does the company know all the ingress and egress points of PII and ePHI?

One Last Thought

While the list of questions above could be way more extensive than what I provided above, my objective with this short article is to plant the "bug" in the readers minds on how to "look beyond the trees" and ask questions that could provide you as an examiner with a broader perspective of the strength of the insurers' cyber security measures around critical data, use your experience and develop your own set of inquiries. My last advice: think outside the box…that is what the bad guys do to successfully achieve their goals. ■

Alan Gutierrez-Arana, a consulting director with McGladrey LLP, has over 15 years of experience providing IT security and controls assessments, regulatory compliance consulting services for a broad range of insurance, banking, finance and high technology entities. He specializes in IT controls assessment and compliance, federal and state IT regulatory compliance (NAIC, SOX, PCI-DSS, HIPAA-HITECH, BASEL II, FFEIC), controls design and implementation, disaster recovery, IT outsourcing and off-shoring, IT governance, business continuity, change management, information security, and e-business; his clients' portfolio includes several insurance departments, Fortune 100 and Fortune 500 companies.

From the President's Desk

By Parker Stevens

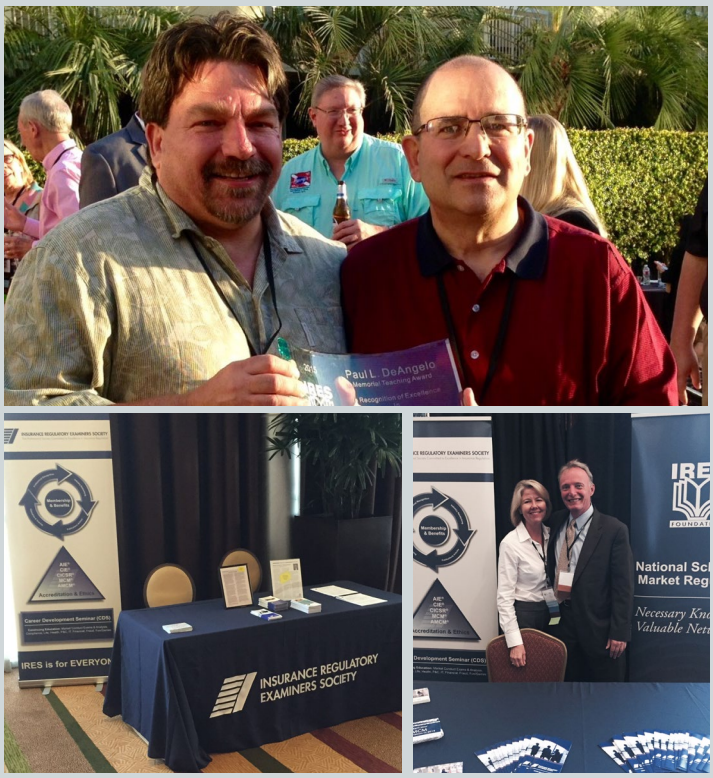
I, along with the rest of IRES, would like to congratulate Jim Mealer who is the 2015 Paul L. DeAngelo Memorial Teaching Award winner given by the IRES Foundation. Jim is a long time IRES member and the Chief Market Conduct Examiner for the Missouri Department of Insurance, Finance and Professional Registration. He has served on a number of committees, panels, Boards of Directors, and is an all-around great guy. IRES is very proud of Jim!

For months now you have heard me talk about our new IRES booth. Well we were able to finally roll it out at the Spring NAIC meeting and the IRES Foundation School last month. Personally, I think it is a major improvement and really stands out, compared to our old one. See below for a few pictures of our new pride and joy.

Finally, I want to take a minute to just say thank you to all the dedicated women and men that make up all the IRES Committees, the State Chairs, the Board of Directors, and the Executive Committee. Many don't realize just how much time and effort they put in to help make IRES run smoothly. They are the backbone of IRES with one goal in mind, to keep growing IRES. For me personally, it has been an amazing year, quick, but an absolute pleasure to work with such wonderful professionals. So if you happen to see an IRES volunteer at work, at a conference, or just out and about please take a minute to say thank you.

The CDS is just around the corner and I can't wait to see you all there. ■

Parker Stevens, IRES President
parkerstevens@examresources.net



Clockwise from Top: Jim Mealer recieves the 2015 Paul L. DeAngelo Memorial Teaching Award; Robin Clover and Mark Hooker with the IRES Exhibit Booth at the IRES Foundation School; The new IRES display at the Spring NAIC event.

Back to Basics

Highlights of the IRES Foundation National School on Market Regulation

By Christine Palmieri

Industry and regulatory compliance personnel once again came together for the distinguished IRES Foundation National School on Market Regulation April 12-14, 2015. The backdrop: picturesque La Jolla, California.

As customary, the Foundation's pre-conference event, the "Welcome Reception" was held on Sunday evening. During the festivities, Jim Mealer from the Missouri Department of Insurance was awarded with one of the Foundation's two prestigious awards, the 2015 Paul DeAngelo Memorial Teaching Award, for his continued commitment to market regulatory initiatives.

As the host state, the California Department of Insurance (CDI) provided tremendous support throughout the School.

Commissioner Dave Jones commenced the two day event with a thoughtful keynote address to more than 225 industry attendees and regulator faculty, touching upon various emerging insurance topics and highlighting the importance of collaboration between regulators and industry. Three representatives from the CDI's Fraud Division provided a comprehensive overview of their SIU oversight and interaction with insurance carriers, other law enforcement and prosecutors as well as a recap of several case files and what it takes "To Catch a Thief." In addition, three of the 21 who served as the 2015 faculty represented CDI's Market Conduct Division.

While traveling abroad, Director John Huff from Missouri highlighted his commitment to this annual event by delivering a fitting video message about the importance of IRES and the IRES Foundation. Two representatives from the Missouri DOI joined other senior regulators from California, Connecticut, Florida, Iowa, New Hampshire, Ohio, Virginia, Washington, West Virginia, Wisconsin, the NAIC and the Interstate Insurance Product Regulation Commission in serving as faculty members.

Commissioner Nick Gerhart from Iowa served as the keynote lunch speaker and provided his views on market regulation and, continuing with the theme of anti-fraud, offered insight into current initiatives by his organization.

Carol Newman, former general counsel for the California State Compensation Insurance Fund and presently with her own practice, was awarded the 2015 Gary A. Hernandez Memorial Insurance Education Leadership Award. Carol was with the Sonnenschein firm (now Dentons) and Fireman's Fund previously, and served as Chair of the IRES Foundation.

The 2015 school introduced a panel discussion focusing on perspective from the "C Suite". Chief Compliance Officers from Zurich, Nationwide and Guardian Life provided "A View From the Top" during this must-attend dialogue. This distinguished group of executives offered insight into what keeps them up at night and how they maintain a culture of compliance within their companies.

An IRES Foundation School would not be complete without the culminating game show, hosted by Alex Trainwreck. A team of regulators competed against teams of former regulators and industry in the "Not Jeopardy" game show, revealing their knowledge, or lack thereof, of insurance trivia.

The IRES Foundation slogan, "Necessary Knowledge, Valuable Networking," has once again proven to be a fitting depiction of this annual event. Save the Date for next year's event! April 17 -19, 2016, in San Antonio, Texas. ■

Chris Palmieri is the Vice President of Corporate Compliance & Market Regulation at Travelers where she oversees external market regulation activities and consumer complaint handling. Chris and her team also facilitate many internal compliance functions, working closely with business and corporate areas on a variety of matters, including implementation of news laws and regulations and establishment of protocols in support of market regulation.

IRES Foundation Awards Presented at 2015 National School

Paul L. DeAngelo Memorial Teaching Award

This year's recipient is Jim Mealer (MO).

Jim Mealer poses with John Mancini as he receives the 2015 Paul L. DeAngelo Memorial Teaching Award.

Gary A. Hernandez Memorial Insurance Education Leadership Award

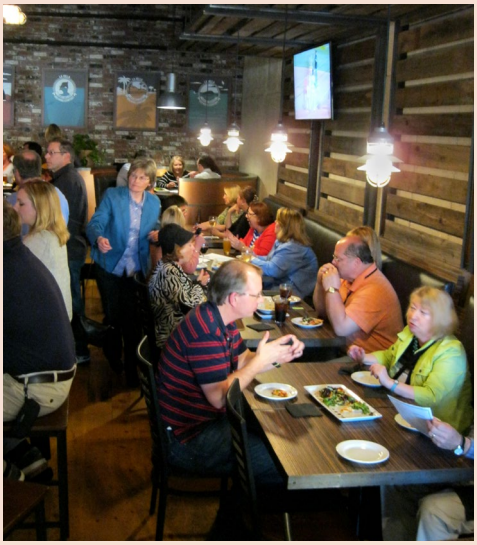
This year's recipient is Carol Newman – General Counsel, State Compensation Insurance Fund.

Carol Newman poses with John Mancini as she receives the 2015 Gary A. Hernandez Memorial Insurance Education Leadership Award.

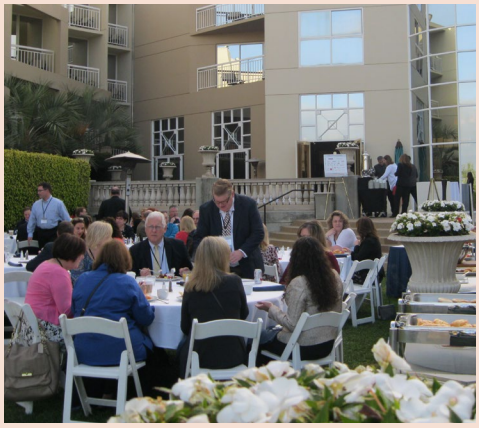
Surfin' the Waves of Regulation

Photos from the 2015 IRES Foundation National School on Market Regulation

Mike Hailer and Cheryl Davis with first-time attendee William Yarbrough at the First-Timers Reception.



On Tuesday night, attendees gathered for the networking event held at La Jolla Brewery.



Attendees took advantage of the sunshine as they ate breakfast in the garden.

Commissioner Jones from California was the Keynote speaker Monday morning.

Robin Clover and John Mancini help out with the Game Show.

Exhibit Hall at the Hilton La Jolla.

'Zoning In'

By Kathy Donovan

Northeast Zone

Maine Adopts Long-term Care Insurance Claims Rules

Effective March 30, 2015, new claim practice standards were established for long-term care insurers under Maine Insurance Rule Chapter 420. Significant new provisions involve claim payments, timeframes, appeals, external review, as well as filing requirements for new or revised contract provisions and forms.

New Jersey Adopts "Homeowners Insurance Consumer Information Brochure" Requirements

New insurance regulations, adopted under NJAC 11:2-41, establish the "minimum standards for a one-page summary of a homeowner's policy, including notable coverages and exclusions, required to be provided to policyholders." Insurers may use the rule's five model summary templates or their own company-specific forms. Filing timeframes apply to company-specific forms, which must be filed 30 days before use. Insurers must implement the rules by May 31, 2015, with forms filed for review on or before May 1, 2015.

New York Sets Cyber Security Exam Framework

New York's Department of Financial Services announced its IT/cyber security examinations will now include, but not be limited to, the following topics:

- Corporate governance, including the organization of and reporting structure for cyber security related issues;
- Management of cyber security issues, including the interaction between information security and core business functions, written information security policies and procedures, and the periodic reevaluation of such policies and procedures in light of changing risks;
- Resources devoted to information security and overall risk management;
- The risks posed by shared infrastructure;
- Protections against intrusion, including multi-factor or adaptive authentication and server and database configurations;
- Information security testing and monitoring, including penetration testing;
- Incident detection and response processes, including monitoring;
- Training of information security professionals as well as all other personnel;
- Management of third-party service providers;
- Integration of information security into business continuity and disaster recovery policies and procedures; and
- Cyber security insurance coverage and other third-party protections.

The Department further indicated in its press release, dated March 26, 2015, that "company IT/cyber security examinations will be scheduled after conducting a comprehensive risk assessment of each institution." The Department requested specific companies to complete the "Platform Data Sheet" referenced in the press release, with responses to be submitted via the secure portal application no later than April 27, 2015.

Southeast Zone

Mississippi enacts "Property Insurance Clarity Act"

This Act requires homeowners insurers to provide certain information to the Mississippi Insurance Department, beginning or before Oct. 1, 2015. Specifically, once every three years each insurance company, as well as the Mississippi Windstorm Underwriting Association, must submit "computations of the total amount of direct incurred losses, direct earned premiums, policy limits, reinsurance, allocated loss adjustment expense and the number of policies in force by earned house years for the prior calendar year." The data must be submitted by zip codes and be provided for each of the following policy categories: (1) all homeowners policies that include windstorm coverage; (2) all homeowners policies that exclude windstorm coverage; and (3) all policies that only include windstorm coverage. Provisions to request filing exemptions or extensions, as well as monetary enforcement penalties, are also addressed.

West Virginia enacts changes in financial responsibility and named driver exclusions

Effective Jan. 1, 2016, HB 2790 increases the minimum amounts of financial responsibility. The bill also clarifies that "insurers are not required to offer new or increased uninsured or underinsured motor vehicle coverage when coverage is increased to meet the increased requirements of proof of financial responsibility" and further addresses named driver exclusions and coverage, indicating that the legislature finds the following:

- The explicit, plain language of a motor vehicle liability policy between an insurer and its insureds should control its effect.

continued on page 13

'Zoning In' – continued from **page 12**

- Where insurers are required by the common law to provide minimum financial responsibility limits coverage for excluded drivers, consumers not excluded by restrictive endorsement are negatively impacted.
- The decision of the Supreme Court of Appeals of West Virginia in *Jones v. Motorists Mutual Insurance Company*, 177 W.Va.763 (1987) interpreted chapter seventeen-d of this code to require insurers to provide minimum financial responsibility limits of coverage to excluded drivers; and
- It is not the intent of the legislature to require insurers to provide minimum financial responsibility limits of coverage to excluded drivers.

Midwest

Prior Authorization form in focus in Indiana

Indiana's Department of Insurance Bulletin 214 encourages "all entities involved in the prior authorization process to use a common form for prior authorization, thereby reducing costs to insurers and health care providers, and avoid unnecessary delays for patients." In the interest of achieving a level of uniformity, the Department included a prior authorization form in its Bulletin which is similar to one currently used in Texas.

Oklahoma

The Oklahoma Insurance Department issued guidance in its Bulletin No. PC 2015-02 on three issues regarding earthquake insurance:

- "Man-made" earthquake exclusion
- Preexisting damage exclusion and
- Specialized training of earthquake adjusters

Regarding the topic of the "man-made" earthquake policy exclusion, the Commissioner expressed concern "that insurers could be denying claims based on the unsupported belief that these earthquakes were the result of fracking or injection well activity." The Commissioner further indicated, "If that were the case, companies could expect the Department to take appropriate action to enforce the law. I am considering market conduct examinations to ascertain the facts surrounding the extraordinary denial rate of earthquake claims that the preliminary data seems to indicate." Denials based on "pre-existing" damage are also in focus by the Department, as the Commissioner indicates there is a regulatory expectation "that the insurer has inspected the property prior to inception of the coverage and maintained reasonably current information as to the condition of the insured property, prior to loss." With respect to adjuster training, the Commissioner expects that insurers "will take steps to ensure that claims adjusters receive training as necessary to address the concerns."

Western

Montana Allows "Military Discount" Exception to Rebate and Discount Prohibition

Effective March 20, 2015, HB 53 provided for a military discount exception to the general rebate and discount prohibition for property or casualty insurance. Essentially, the general prohibition against rebates or discounts provided under Montana law does not apply with respect to property or casualty insurance sales to: an active, retired, or honorably separated member of the U.S. Armed Forces, including a member of a reserve component; or a spouse, surviving spouse, dependent, or heir of a U.S. Armed Forces member.

Montana Enacts Additional Security Breach Requirements

Effective Oct. 1, 2015, Montana's definition of "personal information" will be expanded to also include medical record information, a taxpayer identification number or an identity protection personal identification number issued by the IRS. HB 74 additionally mandates that any licensee or insurance-support organization that is required to issue a notification pursuant to 33-19-321 "shall simultaneously submit an electronic copy of the notification and a statement providing the date and method of distribution of the notification to the commissioner, excluding any information that personally identifies any individual who is entitled to receive notification. If a notification is made to more than one individual, a single copy of the notification must be submitted that indicates the number of individuals in the state who received notification."

Changes in Renewal Notices Enacted in Utah

With the passage of HB 76, renewal notices issued by insurers for certain property and casualty lines of business will be required to include additional content. In addition to maintaining the current mandates requiring insurers to clearly state the renewal premium and how the renewal premium may be paid, insurers must also include the due date for payment of the renewal premium and state that failure to pay the renewal premium extinguishes the policyholder's right to renewal. New provisions also clarify how deadlines are measured and address payment delivery methods. ■

Kathy Donovan is Senior Compliance Counsel, Insurance with Wolters Kluwer Financial Services. Kathy has more than two decades of experience in insurance compliance. Her expert commentary on legal and regulatory issues affecting the insurance industry is widely published and she is a regular presenter at various industry events.

New Members

Welcome!

The following members have joined IRES since the last issue of *The Regulator®*. Visit the online member directory to learn more about them—and please join us in welcoming them!

GENERAL MEMBERS

- ★ Mary Frances Butler
- ★ Cari Clauss, AIE
- ★ Barbara Ann Hudson
- ★ Terra Mason
- ★ Stephen McDaniel
- ★ Monique Miller
- ★ Sumen Roy
- ★ Rhonda Irene Saunders-Ricks
- ★ Sharon Shipp
- ★ Julie Stuart
- ★ Gilda Thompson

SUSTAINING MEMBERS

- ★ Keri Olson
- ★ Mary E. Taylor

ORGANIZATIONAL MEMBERS

- ★ Barbara Caruso

New Designees

Congratulations!

The following members have received their Accredited Insurance Examiner (AIE™), Advanced Market Conduct Management (AMCM™), Certified Insurance Examiner (CIE™), Certified Insurance Consumer Service Representative (CICSR), or Market Conduct Management (MCM™) designation since the last issue of *The Regulator®*. Please join us in congratulating them!

AIE®

- ★ Patricia Gabriel, AIE, MCM
- ★ Ventura Efrain De La Rosa, AIE (TX)
- ★ William George Fifer Sullivan, AIE, MCM
- ★ Julie Hesser, AIE
- ★ Amy Liston, AIE
- ★ Cari Clauss, AIE

CIE®

- ★ Marc S. Springer, AIE, CIE, MCM (unaffiliated)

MCM®

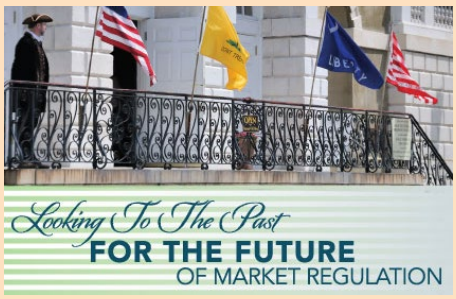
- ★ Susan Boyd, MCM
- ★ Matthew Brasch, MCM
- ★ Timothy Butler, MCM
- ★ Tangela Byrd, MCM (LA)
- ★ Kendra L. Coates, CIE, MCM (ME)
- ★ Beverly A. Dale, CIE, MCM (unaffiliated)
- ★ Mary Firmin, MCM (LA)
- ★ Cynthia M Fitzgerald, AIE, MCM, CICSR
- ★ Craig A. Gardner, CIE, MCM (unaffiliated)
- ★ Jamie Gehling, MCM (LA)
- ★ Jeffery Gorham, MCM
- ★ Angelle Hayes, MCM (LA)
- ★ Terry Henschel, MCM
- ★ Teresa Howell, MCM
- ★ Runfeng Hu, MCM
- ★ Steve Kinoyan, MCM
- ★ Nora Lemonds, MCM
- ★ Katherine Linster, MCM
- ★ John C. Mancini, CIE, MCM (unaffiliated)
- ★ Marcelo Martinez, MCM
- ★ Laura Matuszak, MCM
- ★ Daniel Pittman, MCM (LA)
- ★ Greg Reents, MCM
- ★ Karen Elizabeth Slebodnick Wright, CIE, MCM (TX)
- ★ Jason Sloper, MCM (LA)
- ★ Kallie R. Somme, MCM (LA)
- ★ Alana Viertel, MCM

Upcoming Events

2015 IRES Career Development Seminar and Regulatory Skills Workshop

July 19-22 | Charleston, SC

For more information on 2015 CDS visit the CDS Webpage at go-ires.org/CDS/2015



2015 MCM® Programs

May 13-15 | Des Moines, Iowa

July 22-24 | Charleston, South Carolina

Oct. 19-21 | Atlanta, Georgia

For more information visit the MCM® Program page at http://www.go-ires.org/mcm

Watch the calendar at www.go-ires.org for more upcoming events. ■

INSURANCE REGULATORY EXAMINERS SOCIETY
The Professional Society Committed to Excellence in Insurance Regulation

www.go-ires.org | info@go-ires.org

To submit articles, photographs, or calendar items, contact: IRES, 1821 University Ave W, Ste S256, St. Paul, MN 55104; email TheRegulator@go-ires.org; phone 651-917-6250; fax 651-917-1835.

Editor's Corner

By Kara Baysinger

In this issue of The Regulator® we focus on the new (ride-sharing companies), the scary (terrorism coverage) and the newest big scary (cyber attacks). Thank you to Mr. Thomas Hampton for his thoughtful piece on how cyber attacks have affected the insurance industry, including the growth and challenges in the cyber insurance market. Mr. Alan Gutierrez-Arana provides us with an insightful look into the questions examiners should be considering when evaluating an insurer's cyber security program. Mr. Eric Nordman keeps us up-to-date on the renewal of the Terrorism Risk Insurance Act, including several important changes to the program. Finally, Mr. Joel Laucher takes us on a "ride" through the issues surrounding insurance coverage for transportation network companies like Uber and Lyft.

We are also happy to report on the success of the IRES Foundation National School on Market Regulation held April 12-14 in La Jolla, California. A heartfelt congratulations to Mr. Jim Mealer, winner of the Paul L. DeAngelo Award, and Ms. Carol Newman, winner of the Gary A. Hernandez Memorial Insurance Education Leadership Award. We look forward to seeing you at the upcoming CDS July 19-22 in Charleston, South Carolina.

Please let me know if you have any feedback on this issue, or ideas for upcoming issues. It's your organization: make sure your voice is heard - right here in The Regulator®. ■

NEXT ISSUE

We always have room for another article, so submit your ideas to www.go-ires.org/newsletter/submit.

Contact us at TheRegulator@go-ires.org.

– Your staff at The Regulator® (Kara, Stephanie, Bella, and Heather)