January 2016 • Vol. XXIX • Number 1

Inside This Issue

PLUS
PROFESSIONAL LIABILITY UNDERWRITING SOCIETY
Journal
YOUR SOURCE FOR PROFESSIONAL LIABILITY EDUCATION AND NETWORKING

It's Not All About the Data: The Energy Industry and the Critical Infrastructure Threat

By Tanya Forsheit, Esq., CIPP/US

Tanya Forsheit *is a partner at Baker & Hostetler LLP in Los Angeles, CA. Tanya is a career litigator and trusted counselor who works with clients to address legal requirements and best practices for protection of customer and employee information. Tanya brings to bear more than 18 years of experience litigating complex disputes, as well as her cloud computing and social media knowledge, in counseling clients on thorny issues in data management and information protection. She can be reached at tforsheit@bakerlaw.com.*

It has been nearly three years since President Obama issued Executive Order 13636, "Improving Critical Infrastructure Cybersecurity" ("EO 13636") starkly declaring that "[r]epeated cyber intrusions into critical infrastructure demonstrate the need for improved cybersecurity" and calling for a "partnership with the owners and operators of critical infrastructure to improve cybersecurity information sharing and collaboratively develop and implement risk-based standards." EO 13636 required that the National Institutes of Standards and Technology ("NIST") lead the development of a framework to reduce cyber risks to critical infrastructure (the "Cybersecurity Framework"), including standards, methodologies, procedures, and processes that "align policy, business, and technological approaches to address cyber risks." EO 13636, ¶ 7(a). NIST released the final voluntary Cybersecurity Framework in February 2014.

Whatever else critical infrastructure might mean under the broad definition set forth by EO 13636 ("systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters," EO 13636, § 2), it clearly encompasses systems and assets in the energy industry, including but not limited to the nation's electrical grid and oil pipelines.

The Risks

There is no doubt that a cyberattack on such assets could be disastrous to the economic, physical and public health and safety of this country. And yet, the focus in daily headlines and in the security community continues to be data security breaches involving the compromise of credit card numbers, social security numbers, or other forms of sensitive information. Indeed, even in the energy sector, tremendous resources, time and attention have been devoted to the concerns of Public Utilities Commissions in numerous states with respect to the treatment and sharing of consumer personally identifiable information in the smart grid.

By contrast, the discussion of the threat to our physical critical infrastructure seems to happen in hushed tones, often behind closed doors, perhaps because the potential consequences are simply too terrible to fathom. In the meantime, one consultant from the nuclear power sector claims to have identified almost 400 control system cyberincidents—i.e., situation in which a failure in electronic communications leads to a loss of confidentiality, integrity, or availability—including accidents such as the deadly San Bruno, California, pipeline explosion in 2010 that resulted, at least in part, from failures in the Supervisory Control and Data Acquisition (SCADA) software that manages critical infrastructure (See Paul F. Roberts, *How cyberattacks can be overlooked in America's most critical sectors*, The Christian Science Monitor, March 23, 2015). The Department of Homeland Security's Industrial Control System Cyber Emergency Response Team (ICS-CERT), which works with private industry to reduce risks

continued on page 10

PLUS Perspective:
Incoming President's Message

Heather Fox *2016 PLUS President.*

The New Year is officially here, and with its arrival my term as president of PLUS has begun. I am very excited to continue my service to PLUS in this new capacity. I fully expect 2016 to be a great year for PLUS, an organization that means so much to so many professional liability insurance professionals.

2016 is poised to be an interesting year for the insurance industry. From ongoing industry consolidation to the constantly evolving legal landscape impacting many professional lines, staying current on the latest in our industry has never been more important. Your membership in PLUS is a great start, since PLUS offers many resources for its members to stay current and excel in this exciting and challenging insurance market.

One of my primary goals for 2016 is to make communication with you, the PLUS membership, more effective. There are so many awesome things that PLUS does, but many members simply aren't aware what those things are and how to utilize them to benefit their careers. For example, did you know that all PLUS members can opt-in to receive a daily news email containing the latest headlines, opinions and discussion of the issues that impact professional liability insurance? It's free with your PLUS membership and almost 1,000 PLUS members have already signed up to receive this valuable information in their inbox each business morning. If you'd like to sign up for the daily PLUS News Feed, simply email Lance Helgerson (lhelgerson@plusweb.org),

PLUS' director of strategic marketing, from the address at which you'd like to receive the daily news email and you will be enrolled—it's that easy!

Another tremendous educational resource is the PLUS Multimedia Library. This members-only video library contains all of the educational sessions from the PLUS Conference and PLUS Symposia from the past four years, plus Webinars, international event sessions, select chapter events and much more! All told there are more than 241 hours of industry content available from your computer or mobile device. I encourage you to discover the value of this service on your next "working" lunch by clicking on the Multimedia Library link under the Education tab on the PLUS website.

Diversity and inclusion efforts have been at the forefront of PLUS' priorities for several years, and in 2016 I'm very excited to see the progress we'll make with our inaugural class in the Diversity Leadership and Mentoring Program (LAMP). LAMP offers 15 members from traditionally underrepresented groups the opportunity to attend PLUS national level events, connect with PLUS leaders, and work with an industry mentor to help advance their careers. Having met many of the eager LAMP participants at the recent PLUS Conference in Dallas I was very impressed with these individuals and look forward to seeing what they can achieve in our industry in the years to come. As our inaugural LAMP group, their success will define the success of the LAMP program.

As we enter the New Year, I want to challenge you to move beyond your membership in PLUS and become a volunteer with the organization and bring your ideas about how PLUS can provide even more value to its members. PLUS is fortunate to have more than 300 industry professionals who already donate their time and talents to make the organization work, but we are always looking for new volunteer talent and new ways to engage with members who want to connect. People often say to me that they don't know how to get involved, so here it is… contact PLUS' new executive director, Robbie Thompson, and mention to him that you want to volunteer! He will work with the team at PLUS to find a way for you to get connected with a committee, task force, or other volunteer opportunity to help keep PLUS at the forefront of our industry. Once you discover the value of volunteering with PLUS I guaranteed you'll want to stay connected throughout your career, so start today! Robbie can be reached directly at 952-746-2585.

I am incredibly excited to be president of PLUS this year, and I look forward to building on the many successes of my predecessor, James Skaryznski. Finally, I wish to extend my thanks to the more than 7,000 PLUS members and more than 200 corporate sponsors for your continued support of PLUS.

Stephanie Resnick *is a partner with Fox Rothschild LLP and chair of the firm's Directors' & Officers' Liability & Corporate Governance practice. She can be reached at sresnick@foxrothschild.com.*

John C. Fuller *is an attorney at Fox Rothschild LLP and can be reached at jfuller@foxrothschild.com.*

As Department of Justice Takes Aim at Board Members, How Can Companies and Their Insurers Mitigate Risks?

By Stephanie Resnick & John C. Fuller

In recent years, companies in a variety of industries have reported an increase in the number of potential directors who are declining invitations to join their corporate boards. Although many of the reports are anecdotal, they are numerous and widespread, and raise issues of why potential board members are now turning down once prestigious positions. Will this trend continue, and what can companies do to attract top candidates and invigorate or re-invigorate their boards?

The answers are that personal liability is the strongest disincentive, new government enforcement initiatives are bound to dissuade even more candidates, and adaptive insurance policies offer one of few realistic solutions for companies seeking to attract board members. Companies must set in motion plans to attract new board members and ensure indemnification even if such indemnification may not be covered under traditional directors' and officers' insurance policies.

After years of general concern over the decline of board membership, the specter of catastrophic personal liability has reached unprecedented levels following the recent release of the U.S. Department of Justice, Office of the Deputy Attorney General's Memorandum from Sally Quillian Yates dated September 9, 2015 (the "Yates Memo"), which announces new directives for holding individual directors and officers liable for corporate acts. With personal liability for board members poised to reach an all-time high, companies, their insurers and underwriters need to have a dialogue about their existing policies in an effort to offer appropriate protections to board members. Most likely, the ramifications of the Yates Memo will result in increased premiums to cover the increased incidents of potential board member liability and will be a challenge to insurers and underwriters in view of the Department of Justice's aggressive new stance.

The Yates Memo

On September 9, 2015, Deputy Attorney General Sally Quillian Yates released the Yates Memo—a memorandum to all federal investigators and prosecutors—outlining new procedures for investigating and prosecuting board members and other individuals involved with acts of alleged corporate wrongdoing.[1] Set forth as six directives, the core goals of the Yates Memo are to harmonize civil and criminal investigations, to ensure that directors and officers are the focus of the government's efforts, and to heighten the difficulty for directors and officers to evade personal liability when their specific role in corporate misconduct is identified.

First, a company must mitigate the charges against the entity by identifying all relevant facts about the potentially responsible directors and officers in order to receive "cooperation credit." If a company refuses to divulge information, or only provides minimal information about the individual directors and officers, the company will not receive any consideration for its cooperation in an investigation. The Yates Memo specifically instructs prosecutors to proactively scrutinize board members' roles and review all disclosures from companies in great detail to ensure that no officer's or director's role has been minimized or obscured. This directive clearly has ramifications for the insurer, which will need to retain separate counsel for the company and individuals in light of the potential inherent conflicts of interest.

Second, investigators and prosecutors are directed to focus on the officers and board members from the outset of their investigations. This directive is designed to increase prosecutorial pressure on officers and board members, but is also a strategic method of uncovering the full extent of alleged corporate misconduct by focusing on the acts (i.e., individual communications and decisions) of the officers and directors rather than the narrative told by the board minutes and corporate financial disclosures.

Third, criminal and civil prosecutors are instructed to stay in close contact with each other. This directive similarly has a multi-faceted goal of guaranteeing that the full breadth of remedies are available in each case of corporate wrongdoing and ensuring that directors and officers are pursued by the proper prosecutorial authorities if and when their involvement is uncovered by investigators.

Fourth, prosecutors are now expressly required to seek written approval from the Attorney General's Office or United States Attorney's Office to release officers and directors as part of the resolution of corporate matters. Moreover, absent "extraordinary" circumstances, individual liability is not to be released as part of settlement with the subject entity and prosecutors are instructed to ensure that all individual claims are preserved.

Fifth, cases are also not to be resolved without an articulated plan to pursue potential claims and charges against the directors and officers. Such plans are to set forth the status of the action, what investigative work remains, and a plan to complete the investigation before the applicable statute of limitations runs. In addition, if a decision is made not to pursue charges or claims against related directors and officers, the investigative office must memorialize, in writing, why further charges were not pursued.

Sixth, a director's or officer's ability to pay potential fines or penalties is no

continued on page 12

Ethical Implications of Posting Video Depositions Online

By Seth L. Laver & Jessica L. Wuebker

Seth L. Laver *is a partner and* **Jessica L. Wuebker** *is an associate in the Professional Liability Practice Group at Goldberg Segalla, where they counsel and defend lawyers, accountants, and other professionals in a wide range of professional negligence and risk management matters. Their publication credits include co-authoring an exploration of the ethical implications of the virtual law office for the American Bar Association. Seth is the editor of and Jessica is a frequent contributor to Professional Liability Matters, Goldberg Segalla's blog focusing on legal developments and risk management tips impacting the professional liability community.*

Many of today's media sensations often arise from a "private" moment finding its way to the internet. Granted, some of these well-publicized moments are venued in a celebrity's bedroom, but there are plenty involving the courtroom as well. Justin Bieber's infamous deposition footage is perhaps the most recent example of a celebrity's videotaped deposition that drew national attention. Other well-known deponents include Tupac Shakur, Bill Cosby, Lil Wayne, and Larry Flynt. Regardless of your level of interest in celebrity testimony, the fact that these depositions have reached the public eye is worthy of further investigation. In particular, the Rules of Professional Conduct governing attorneys are instructive on the limitations placed upon attorneys who intend to use deposition footage outside of the courtroom.

The 1993 amendments to the Federal Rules of Civil Procedure "dramatically liberalized" the rules governing an attorney's use of video depositions. *Michael J. Henke & Craig D. Margolis, The Taking & Use of Video Depositions: An Update, 17 Rev. Litig. 1, 2 (Winter 1998).* Initially, audio and video equipment was not trusted; it was considered an inferior method of preserving testimony. So, while video testimony was once permitted only by order of the court or stipulation of the parties, the new F.R.C.P. 30(b)(2) granted the noticing party the right to unilaterally select the use of video without prior approval. This amendment, combined with technological advances to audio and video equipment, put "video and stenographic recording on an equal footing" and resulted in a surge of video at the deposition table.

Notably, videotaped depositions provide the viewer with a wealth of valuable information lacking in a transcribed record. According to one court: "facial expressions, voice inflection and intonation, gestures, 'body language', and notes between counsel and deponent may all express a message to persons present at a deposition as to which a typed transcript is completely silent." *Riley v. Murdock*, 156 F.R.D. 130, 131 (E.D.N.C. 1994). Another advantage to a video deposition is that jurors now prefer to receive information communicated by television which is "the primary medium by which most Americans receive information today." *Henke, 17 Rev. Litig. At 19.* Moreover, video depositions may alleviate scheduling conflicts and permit particularly vulnerable witnesses, such as minors, the opportunity to testify without the intimidation of a courtroom. *See, The Testimony of Child Victims in Sex Abuse Prosecutions: Two Legislative Innovations, 98 Harv. L. Rev. 806, 814 (1985).*

Today's videographers are in demand and, as such, the market for would-be videographers is growing. Certification for "certified legal video specialists" is available nationwide through the National Court Reporters Association, which has enjoyed certification growth from approximately 550 in 1998 to nearly 15,000 today.

Indeed,[1] videotaping depositions has become standard practice, particularly since technology has advanced and improved since the days of grainy videos and inconsistent, poor sound quality. Recorded depositions are increasingly used in lieu of trial testimony altogether, particularly in mass torts and other large, complex cases. Even in cases with less financial risk, excerpts of a video deposition can be used for impeachment purposes.

Most jurisdictions permit depositions to be videotaped as long as certain processes are followed. The Federal Rules Advisory Committee has noted that video depositions provide a superior means of securing the testimony of a witness who would otherwise not be able to be present at trial. The Federal Rules of Civil Procedure mandate that a transcript of the video is required by Rules 26(a)(3)(B) and 32(c) if the party intends to offer the video as evidence at trial or on a dispositive motion. F.R.Civ.P. 30, Advisory Committee Notes.

District courts have also enacted local rules regarding the practice. Pursuant to the Middle District of Pennsylvania's[2] Local Rules 30.2 - 30.12, the attorney wishing to take a video deposition must so advise in the deposition notice. At the start of the recording, the camera operator must recite certain information about the deposition and the parties, and must state on the record that the deposition has concluded. The deposition must be timed. Importantly, the attorney who noticed the deposition takes possession of the video and must provide a copy to any party who requests and pays for it. Pennsylvania only permits a video deposition to be used in court if accompanied by a transcript of the deposition. Once the video is introduced into evidence, it is marked as an exhibit and remains in the court's custody.

The Eastern District of Washington[3] has a similar rule. The Northern District of Mississippi's[4] rule includes instruction for filming regarding the "scene" of the deposition and zoom-in procedures. Many other district courts, such as the Northern District of Florida,[5] the District of Maine,[6] the Western District of Pennsylvania,[7] the Southern District of Texas',[8] and the Western District of Texas[9] have less stringent versions of these rules.

Various states have also enacted procedural rules governing the logistics of video depositions. Pennsylvania state rules of civil procedure mirror those enacted in the Middle District of Pennsylvania, discussed above (Pa.R.Civ.P. 4017.1), while Michigan, Minnesota, Illinois, New Jersey, and Washington are just a few of the states who have enacted statutes with provisions similar or identical to Pennsylvania's. MCR 2.315; Minn. R. 30.02(c); 75 ILCS 206(g); NJ R. 4:14-9; RCW 30.

A more complicated question revolves around who controls the video and how it may be used. Again, many states require that a party in possession of a videotaped deposition must provide a copy to other parties who request and

pay for it. The rules also mandate that the court receive and retain a copy if the video is to be used at trial. This issue is not as simple when it comes to parties outside of the litigation. The practice of uploading deposition excerpts to YouTube is apparently widespread. An unsophisticated survey (i.e., a search for the term "deposition") reveals 110,000 deposition videos. Generally, these videos fall into three categories: depositions of well-known public figures; foibles, bloopers, and outbursts; and instructional videos about conducting depositions.

Whether you are considering such an upload, either to advertise your services or assist other lawyers, or you are fighting to have your deponent's video deposition removed from the internet, here are some ethical points to consider when confronted with this relatively new use of technology.

Advertising Angles

A deposition video upload could be construed as an attorney advertisement. According to Florida's Standing Committee on Advertising, videos "used to promote the lawyer or law firm's practice are subject to the lawyer advertising rules" and thus an attorney's unsolicited invitation to view or link her video constitutes an ethics violation. Kentucky[10] requires any attorney advertisement, including a video, to be submitted and approved by a special commission. Texas Disciplinary Rule of Professional Conduct 7.07[11] includes a similar requirement. The Florida Bar has even promulgated guidelines for video sharing.[12] These guidelines state that videos appearing on video-sharing sites that are used to promote the lawyer or law firm's practice are subject to the lawyer advertising rules. That means such a shared video may not include misleading information, which includes references to past results that are not objectively verifiable, predictions or guarantees of results, or statements characterizing skills, experience, reputation, or record unless they are objectively verifiable.

Further, according to these guidelines, sending an unsolicited invite to view or link to a lawyer's video, for the purpose of obtaining or attempting to obtain business, is a violation of Florida Rule of Professional Conduct 1.18(a) (governing duties to prospective clients), unless the recipient is the lawyer's current client, former client, relative, has a prior professional relationship with the lawyer, or is another lawyer.

If you are posting a video to advertise your services, rules regulating the advertisement of legal services apply. Because a YouTube-based advertisement can be accessed in different jurisdictions, make sure that the advertisement complies with the professional responsibility rules in all jurisdictions. An important rule to remember is Model Rule 7.3(c).[13] In applying this rule to YouTube deposition videos, an attorney may not send an unsolicited invitation to view or link to such a video, and any such video must include the words "Advertising Material" at its beginning and end. A video posted on YouTube must also include this disclaimer.

Playing Nice

Most jurisdictions prohibit discovery that causes unwarranted annoyance, embarrassment, or oppression, or undue burden and expense. A deposition clip posted on YouTube that unnecessarily includes personal or embarrassing information, or is edited in a misleading fashion may very well violate these rules.

Assessing Access

Judicial proceedings and court filings are generally available to the public. However, a deposition is not a public event. Once a deposition transcript is filed with the court, it is available to the public for viewing and copying, unless it is subject to a protective or confidentiality order. By analogy, this rule would also apply to a deposition video filed with the court. Indeed, at least one court has held that a deposition must be removed from the internet unless and until it was filed with the court and made public record.[14]

If a video is not filed with the court, courts have created different tests to assess whether the public has a right to access.[15] The Third Circuit, for example, mandates that the public may only access "judicial records," or those physically on file with the court, while the First and Second Circuits have held that public access is not permitted to materials, such as videos, which do not play a role in the court's adjudicative process.

Deft Defense

Situation: Your opponent wants to upload the deposition video, and you're opposed. What to do? Prior to the deposition, you can seek a stipulation with the other parties proscribing the distribution and use of the video outside of the proceeding. You can also seek a protective order from the court permitting the deponent's counsel to mark deposition testimony and exhibits "confidential"; such material cannot be shared with third parties and may be lodged, but not publicly filed with, the court. Attempting to bar the use of the video after the fact is more complicated; a protective order may work, though your opponent may not respect it. You can also request that the website remove the video.

If your adversary won't cooperate, consider reaching out to the video-sharing site itself. You can request removal of content[16] on YouTube based on the site's Privacy Guidelines.[17] For content to be considered for removal, an individual must be uniquely identifiable, and in making this assessment, YouTube will consider factors such as a person's image or voice, full name, contact information, and financial information. Under these criteria, a deposition video is a likely candidate.

Endnotes/Links

1 http://apps.americanbar.org/litigation/litigationnews/trial_skills/second-chair-civil-trial-depositions.html
2 http://www.pamd.uscourts.gov/sites/default/files/local_rules/LR120114.pdf
3 http://www.waed.uscourts.gov/sites/default/files/Local_Rules-20150505.pdf
4 http://www.mssd.uscourts.gov/sites/mssd/files/2014MASTERCOPYCivil.pdf
5 http://www.flnd.uscourts.gov/forms/Court Rules/local_rules.pdf
6 http://www.med.uscourts.gov/pdf/Local_Rules.pdf
7 http://www.pawd.uscourts.gov/Documents/Forms/lrmanual.pdf
8 http://www.txs.uscourts.gov/sites/txs/files/dclclrl2014.pdf
9 http://www.txwd.uscourts.gov/Rules/Online/Civil/cv-30.pdf
10 http://www.kybar.org/general/custom.asp?page=attorneyadvertising
11 https://www.texasbar.com/AM/Template.cfm?Section=Error&Template=/CM/ContentDisplay.cfm&ContentID=27271
12 http://www.floridabar.org/TFB/TFBResources.nsf/Attachments/4AEC3CC3C76510A885257B5900643E6E/$FILE/Guidelines - Video Sharing Sites.pdf?OpenElement
13 http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_7_3_direct_contact_with_prospective_clients.html3
14 http://firstamendmentcoalition.org/2009/06/judge_orders_removal_of_deposition_excerpt_from_youtube/
15 http://www.lexology.com/library/detail.aspx?g=cdb1805d-9aca-4ac2-9808-98897995854a
16 http://support.google.com/youtube/bin/answer.py?answer=142443
17 http://www.youtube.com/t/privacy_guidelines

Jesse Lyon *grew to maturity in northern California, was educated at Saint Mary's College of California, Moraga where he took a double major in history and English. Presently he lives in Reno, Nevada where he has worked in financial fields which involved retail banking, residential property valuation, and professional insurance. He can be reached at jelyon@gmail.com.*

Wanted: Responsible 21st Century Insurance Activity

By Jesse Lyon

There is a crisis right now that is affecting nearly everyone on the planet; one that is growing more costly and more destructive with each passing year. At the core of the crisis are binary code, software technology companies, and the professional insurance sector. How the professional insurance sector addresses this problem will either define it as one that cares little for others, or as a socially responsible sector that honors its heritage.

As technology evolves, humans are increasingly dependent on it to function, both in the personal and professional spheres. Computers, operating systems, and productivity software like Microsoft Office have been developed and survive with very little oversight from either the U.S government or the technology sector itself. The 1990s saw the creation of Windows 95, 98, and 98SE, all of which caused all users to experience (sometimes with frequency) the "blue screen of death." To this day security, stability, and speed issues continue as evidenced by the awkwardness of Windows Vista, Android, and the numerous hacking incidents from 2010 forward. Most attentive people know that upgrading from one version of Android to the next causes a person's mobile device to suffer speed and stability issues, and upgrading to the next version of Android does not seem to provide much in the way of improved security. Moreover, for the past thirty-five years, there have been very few judicial rulings and laws that have been able to hold the technology sector accountable for any of its actions. Companies that offer Tech E&O policies have blithely ignored or taken for granted that it has been very difficult, prior to August 2015, to sue a software company for the poor coding and performance of its software. Now we are on the cusp of that change taking place, and these changes must be met with a strong sense of purpose and corporate social responsibility (CSR) on the part of Tech E&O insurers.

The only agency that has had any real measure of success in policing the technology world, at least in the United States, is the Federal Trade Commission (FTC). After all, the Uniform Commercial Code (UCC) has a plethora of limitations that make it difficult to sue for a faulty product. Meeting the requirements of negligence, which include duty, breach of duty, and foreseeable harm, severely limit suing a software company due to negligence. What duty does Google have to a given Android user? When that duty is established, if it is established at all, then what exactly would Google have to do to breach that duty? And how is the consumer's suffering foreseeable to Google? With over one billion users it is difficult to claim that harm to any of those users could be reasonably predicted on Google's part. However, Section 5a of the FTC Act allows the agency to take legal action against an organization that is involved "in a deceptive or unfair commerce practice". In the 2015 Wydnham Worldwide ruling it was Section 5 that the federal court upheld in order to validate the action that the FTC took against Wydnham Worldwide. The FTC has used, albeit infrequently, Section 5 to encourage better behavior out of software companies. In 2003, after Microsoft admitted to a flaw in its Passport Service, the FTC encouraged Microsoft to be more responsible by threatening it with a $2.2 trillion fee. However, the frequency of the FTC using Section 5 to force more secure software from any technology company is now going to sky rocket. This is almost entirely due to the increasing number of breaches that are putting undue stress on the ordinary consumer. It is also supported by history. Starting in 2008, the Secretary of Health and Human Services unleashed Recovery Audit Contractors (RACs) on the United States, and those contractors have been quite eagerly finding medical billing errors in hundreds of cases involving medical organizations throughout the United States. After the Great Recession of 2008 social anger at financial institutions was forged into the Dodd-Frank Act, which continues to have repercussions in the financial sector.

For the past thirty-five years software companies have been telling consumers to trust them, and, yet, that trust has resulted in years of poorly written software, whether it is an operating system, software that controls vehicle functions, or an online platform. In the near future, when software controls nearly every function of an automobile, when software comes to dominate mass transportation, when software becomes integrated into all aspects of the ordinary consumer's home, then even our everyday safety becomes an issue. If the poor coding of software can expose our dark desires, like those exposed through the Ashley Madison hack, or if software can make our homes prey to outside forces, then how will any part of our lives be protected? Perhaps the worst part is the fact that, for over fifteen years, insurance companies have been indemnifying and sustaining the reckless disregard software companies have for humanity. This must not continue!

Insurance companies need to start forming coalitions, both within the insurance sector as well as within other sectors of business, because, ultimately, the ordinary consumer is not going to be protected by the government. In time Congress will pass a law that will give software companies the ability to continue their reckless activities, or the FTC will find itself fighting against a software company, or perhaps the software industry at large, before the U.S Supreme Court. At the conclusion of that putative trial the FTC could theoretically be stripped of most of its power to regulate software companies. Regardless we have arrived at a pivotal moment in U.S history, at

continued on page 9

Meet Jen Lee: Future PLUS Chair

By Plus Team

New Future PLUS chir Jennifer Lee recently chatted with the editors of PLUS Journal about her career. We appreciate Jen taking the time to complete this profile, and hope you enjoy it.

PLUS: What is your current position, and what do you do?

Jen: I am currently a Senior Underwriter at Markel for professional liability lines of business. I underwrite various professional liability classes and I am located in the Scottsdale, Arizona office.

PLUS: What led you to the professional liability field?

Jen: I started working in the professional liability field in 2003 after spending nearly 1 year underwriting personal lines. After gaining knowledge and experience in the position that I was in, I found a passion for professional liability that has kept me focused in this field for 12 years.

PLUS: What do you like about working in professional liability?

Jen: I enjoy the variety of risks that I review and work with every day. It is exciting to analyze risks ranging from Medical Professionals to Engineers to Real Estate Agents all in the same day. I also value the people that I have met working with in this industry and the great relationships that I have been able to be a part of because of the professional liability field.

PLUS: Where do you hope to be in five years?

Jen: My five year plan is to continue to expand my knowledge of the professional liability field. Completing the RPLU program was extremely beneficial in helping me understand the nuances of many different coverage forms and the challenges associated with these lines of business. As opportunities become available, I would like to move into a leadership role to assist others in achieving their goals and objectivities.

PLUS: How did you become involved with PLUS?

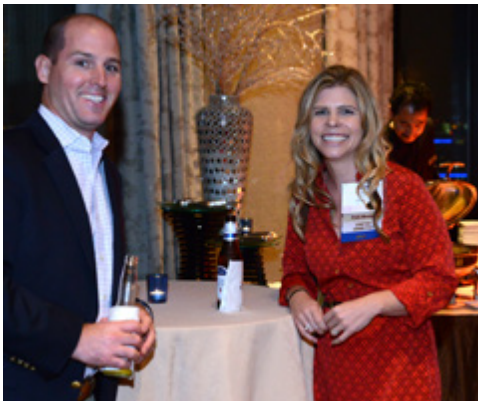
Jen: A co-worker of mine introduced me to PLUS and suggested that I attend the local events. After attending a few events and enjoying the experience as well as the benefits of PLUS, I joined our local Southwest Chapter Committee.

PLUS: What about working in professional liability insurance has surprised you?

Jen: It is surprising that there is something new to be learned every day in this field. The professional liability field encompasses an extremely wide range of professionals, services, and exposures which creates an endless learning opportunity.

PLUS: What is a typical day like for you?

Jen: My day starts out at 4:45am and includes taking my children to their schools before I start my work day. After my day in the office underwriting, I enjoy dinner and family time with my husband and 2 children.



PLUS: What advice would you give to new entrants to the professional liability industry?

Jen: Be aggressive with expanding your knowledge of the industry. I would encourage all new entrants to take advantage of as many mentors and learning opportunities that they come across with, as well as join Future PLUS!

PLUS: What do you do for fun or when you aren't working?

Jen: When not working, I enjoy jogging, hot yoga, learning to play golf, and spending time with my family.

Thanks to Jen Lee for sharing her story with PLUS Journal readers.

Be Published in the PLUS Journal

As a PLUS member you have tremendous insight on the hot topics in professional liability insurance. **Why not share your knowledge by writing an article for the PLUS Journal?**

If you have a topic you're considering, or a full article you'd like to submit for consideration, please email Lance Helgerson at lhelgerson@plusweb.org.

PLUS Foundation—Financial Aid College Scholarships for 2016

The PLUS Foundation is pleased to announce Financial Aid Scholarships, made possible by the personal donations of leaders in our industry:

- ***Constantine "Dinos" Iordanou Scholarship***
- ***H. Seymour Weinstein Scholarship***

Up to four scholarships will be awarded and scholarships will be for up to $12,000 each, payable in increments over four years.

ELIGIBILITY:

Children of any PLUS member or ***employee of a PLUS corporate sponsor company*** are eligible to apply.

Note that children of any company employee are eligible even if their parent is not a direct member of PLUS. Please share this information with your support staff that have children heading off to college that could use some support.

- Post the information in your company newsletter.
- Have your human resources department distribute to employees with children entering college next year.
- Distribute the information via company email lists or bulletin boards—though it is a PLUS Foundation program, ***you do not need to be a PLUS member to qualify***!

APPLICATION SCHOLARSHIP REQUIREMENTS:

Awarded based on family financial need and proof of average to above average high school performance.

Consistent with our mission of philanthropy and the advancement of education, the PLUS Foundation Board of Directors aims to support families and students who have greater financial needs. This step expands on our record of service to and on behalf of the professional liability community.

- The success of the PL industry relies on many employees who may be of limited financial means—the assistants, clerks and other entry level and support staff who move our business forward.
- With the cost of education rising dramatically, many deserving students struggle to attend the college of their choice…or any college at all.
- Most of the Foundation's giving goes to highly worthy charitable organizations. This new scholarship is an opportunity to direct resources to the colleagues and families of our members, creating more personal and closer connections within our PLUS community.

APPLICATIONS & DEADLINES:

Applications will be available online at on the Foundation website January 4 to March 15, 2016.

2016 GILMARTIN SCHOLARSHIPS

Eligibility: Children of any PLUS member or any employee of a PLUS corporate sponsor company

Applications & Deadlines: Applications will be available online starting January 4, 2016. Applications are due March 15. Complete information is available at **www.plusfoundation.org**.

Leo Gilmartin Scholarship: Scholarships are awarded for scholastic merit and extracurricular activity. Application requirements include, but are not limited to:

- College entrance exam scores
- G.P.A. and class rank
- Essay and letters of recommendation
- Extracurricular and community service activities
- Recipients must be full time students and meet GPA requirements to be eligible for subsequent years

General Details & Requirements:

- Up to four scholarships will be awarded
- Scholarships will be for up to $12,000 each, payable in increments over four years
- Applicants must be a child of a current PLUS member or employee of a PLUS corporate member
- An applicant is required to be in his/her senior year of high school
- A recipient must successfully complete high school and enroll in an accredited school in the fall

For more information on all scholarships, please go to: www.plusfoundation.org

least as far as insurance companies and consumers are concerned. The path forward for the professional insurance industry is exceedingly clear: when the government fails to protect consumers, the professional insurance sector needs to be ready to stand between the public and technology companies. If insurance companies that offer Tech E&O fail to adhere to the principle of CSR, then insurance companies will be equally responsible for every cyber breach, for every stolen social security number, and for all of the pain that people will experience in a software dominated world. To do the right thing, however, insurance companies will need to pursue multiple courses of action.

Software engineering is perhaps one of only a handful of professions that requires extreme technical knowledge while lacking real licensing standards. Attorneys must pass the bar exam, residential property appraisers must meet USPAP certification requirements, but there is no professional certification body for software engineers, though these engineers have a tremendous impact on our daily lives. There are some IEEE (Institute of Electrical and Electronics Engineers) concepts that can be followed in order to foster a more grounded approach to software engineering, and universities which want to secure a more thoughtful software engineering program will meet the standards set forth by the Accreditation Board for Engineering and Technology. However, IEEE concepts are not comprehensive, nor are they required to be followed in software creation, and ABET accreditation is voluntary and its accreditation standard is less exacting than that demanded of architects and civil engineers. In a real sense there is little difference between the sixteen year old that has learned how to write in HTML, PHP, and Java and the twenty-two year old software engineer who just graduated from an accredited university. Both of those individuals, from a standards standpoint, are equal in that they have not had to prove themselves. The software for the avionics control systems on an airplane is written by software engineers who have not had to demonstrate a level of experience beyond what is needed to obtain a four year degree. Insurance companies need to work with universities, software engineering companies, and organizations like IEEE and ABET to develop structured software engineering practices and standards that graduating software engineers must meet in order to be accepted into the society of professional software engineering. Furthermore, insurance companies need to work with those same organizations to develop continuing education requirements.

To encourage software companies to help with the framework of higher and continuing education, insurance companies could create two tiers of Tech E&O. The tiers would be distinguished by the percentage of software engineers employed that meet the previously mentioned professional standards. Tier one policies would be for companies whose software engineer workforce is comprised of at least sixty percent of engineers meeting the professional software engineering standards. And tier two policies would be for companies whose software engineer workforce is below the sixty percent threshold. The tier one Tech E&O policies will enjoy benefits such as lower premiums, lower deductibles, and higher limits, both on an individual policy or when layering policies in order to achieve, for example, a higher policy limit. The tier two policies, on the other hand, will have premiums that are treble those of tier one premiums for the same class of business with similar revenues. Additionally, tier two policies will have higher retentions, and the policies will only be offered by non-admitted carriers. Consequently, if a company with a tier two Tech E&O policy is paying thirty-thousand dollars and has a fifteen thousand dollar retention while having a lower policy limit, then it has three strong incentives for becoming socially responsible, incentives that will endure even if a law is passed that limits the force a government may have on the actions of software companies.

In the past fires were a very real civic danger, and it was the insurance sector in the late 17th century which rose to the occasion and paved a better path forward for Europe and the United States. Because of insurance companies, fire patrols were established which allowed for a much better response time when a fire broke out. Because of insurance companies, ordinary consumers had a much better chance of having their home or office saved from being completely destroyed by a fire, due to a decreased response time. When insurance companies' fire brigades worked together to put out fires the whole city stood a better chance of not being consumed by fire. A similar approach by insurers to this new threat is now warranted.

The likelihood that a law will be passed or a legal decision made that will limit the regulating of software companies is extremely high. That possibility, plus the lessons of history, demands that the insurance sector must build coalitions and frameworks that will foster a high level of excellence from software companies. Even if a law were passed that forced better behavior out of software companies, insurance companies still will have the same responsibility from a CSR standpoint to pave the path forward. The professional insurance sector must be mindful of the past and act in the present to help assure a more secure future for humanity. It is time to help shape and build the best possible future, instead of propping up a sector of the business world that cares very little for how easily it can devastate lives, countries, and humanity's future.

Cyber Emergency Response Team (ICS-CERT), which works with private industry to reduce risks to critical infrastructure, reported that for the second year in a row it received and responded to more incidents in the energy sector (79) than in any other sector of critical infrastructure. And, according to a recent report prepared by Lloyd's and the University of Cambridge Centre for Risk Studies, a sophisticated cyberattack on the U.S. power grid could cause nearly $250 billion in economic losses and, under the most severe circumstances, cost more than $1 trillion to the U.S. economy.

So, what should energy companies in the private sector be doing to attempt to mitigate risks – risks that clearly cannot be totally eliminated – with well-funded and resourceful virtual armies of nation states, hackers and hacktivists at the ready and constantly upping the ante? The key, of course, is preparedness, which begins with the dedication and investment of resources. Cybersecurity of physical assets cannot be an afterthought and must be a priority.

Fortunately, there are many resources available to assist the energy industry with developing and maintaining a robust cybersecurity program designed to address the risks of SCADA system failure, in addition to data security. Following is a description of one such resource – the guidance issued by the U.S. Department of Energy earlier this year as a follow up to the NIST Cybersecurity Framework.

DOE Guidance

In January of 2015, the Office of Electricity Delivery and Energy Reliability of the U.S. Department of Energy released guidance to help the energy sector establish or align existing cybersecurity risk management programs to meet the objectives of the voluntary Cybersecurity Framework released by NIST in February 2014, through collaboration with, among others, the Electricity Subsector Coordinating Council and the Oil & Natural Gas Subsector Coordinating Council (the "DOE Guidance"). The DOE Guidance incorporates the seven step process outlined in the Cybersecurity Framework, specifically: (1) Prioritize and Scope; (2) Orient; (3) Create a Current Profile; (4) Conduct a Risk Assessment; (5) Create a Target Profile; (6) Determine, Analyze, and Prioritize Gaps; and (7) Implement Action Plan. Importantly, the DOE Guidance notes throughout the steps that the organization should identify and consider legal and regulatory requirements.

The DOE Guidance also includes a Cybersecurity Framework implementation approach using the Cybersecurity Capability Maturity Model[1] ("C2M2") and a mapping of the C2M2 to the Cybersecurity Framework. The C2M2 has three variants: the Electricity Subsector Cybersecurity Capability Maturity Model, the Oil and Natural Gas Subsector Cybersecurity Capability Maturity Model, and the more general Cybersecurity Capability Maturity Model. It was developed by DOE and contributors from industry and other government agencies and includes a self-evaluation toolkit to guide an organization to identify its cybersecurity and risk management practices, map them to specific levels of maturity, set target maturity levels, and identify gaps and potential practices for maturing over time. The C2M2 has 10 domains:

1. Asset, Change, and Configuration Management (ACM);
2. Cybersecurity Program Management (CPM);
3. Supply Chain and External Dependencies Management (EDM);
4. Identity and Access Management (IAM);
5. Event and Incident Response, Continuity of Operations (IR);
6. Information Sharing and Communications (ISC);
7. Risk Management (RM);
8. Situational Awareness (SA);
9. Threat and Vulnerability Management (TVM); and
10. Workforce Management (WM).

In turn, each domain has four maturity indicatory levels (MILs): MIL0 (Not Performed); MIL1 (Initiated); MIL2 (Performed); and MIL3 (Managed).

Attorney-Client Privilege Considerations

It is easy to imagine subpoenas, civil investigative demands and discovery requests seeking the work product of such gap assessments and maturity models in the event of class action litigation, regulatory inquiries or even criminal investigations following a cyberincident causing significant economic or physical damage. A gap analysis showing organizational awareness of low levels of maturity around certain cybersecurity domains could serve as powerful evidence of wrongdoing (ranging from negligence to willful misconduct) in litigation or regulatory inquiries. Given these potential consequences, it is not surprising that many organizations shy away from conducting such risk assessments altogether. This is not the answer. It is critical that organizations in the energy sector take action to help mitigate the risks associated with a potential cyberincident and engage in the process. However, in creating such detailed gap analyses and maps, organizations should work within a defined team of pre-identified stakeholders and should engage in-house or outside counsel to direct the work and provide advice in order to obtain the protections of the attorney-client privilege and work product doctrine, particularly with respect to early drafts or reports.

What About Privacy?

Critical infrastructure is one of those areas where the interests of privacy and security do not always align. Particularly when it comes to enhanced information sharing between the private sector and government agencies, in the post-Snowden era, privacy advocates have balked at the idea of giving the government even more access than it already has to the details of individual American lives. EO 13636 acknowledged this (pre-Snowden), stating that "[a]gencies shall . . . ensure that privacy and civil liberties protections [based on the Fair Information Practice Principles and other privacy and civil liberties policies, principles, and frameworks] are incorporated into such activities." EO 13636, § 5(a). It is worth noting, in this regard, that existing law, 6 U.S.C. § 133, protects critical infrastructure information (including the identity of the submitting person or entity) that is voluntarily submitted to a federal agency for use by that agency regarding the security of critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, reconstitution, or other informational purpose, from disclosure under the Freedom of Information Act. And the DOE Guidance includes references to consideration of privacy

and civil liberties obligations in identifying legal and regulatory requirements.

Federal legislators have introduced numerous bills over the last several years seeking to encourage and expand information-sharing between the private sector and the government for purposes of assessing the mitigating risks to critical infrastructure. Thus far, no bills have gained traction, due in large part to the understandable concerns of the privacy advocacy community.

Protection of our country's power lines, oil pipelines and, most importantly, people, will require a balancing act. Privacy cannot and should not be sacrificed altogether, but industry must look for creative ways to engage in more meaningful information-sharing without endangering the privacy rights of U.S. citizens. Here again, legal and privacy professionals should be incorporated into the development of cybersecurity programs, any maturity assessment/gap analyses, and data sharing arrangements with other industry participants and the government.

Conclusion

Cybersecurity means much more than information security, and the consequences of cyberattacks extend far beyond identity theft and credit card fraud. Americans have reacted with horror to data security breaches resulting in disclosure of Social Security Numbers and celebrity photos. One can only imagine the true horror in the aftermath of an attack on our nation's critical infrastructure. With the law providing little to no guidance on what reasonable security means for this purpose, and Executive Orders and voluntary frameworks providing only vague guidance, the task falls to companies across the private energy sector to work collaboratively with each other, and the government, to bolster cybersecurity defenses. The process should be an ongoing and continual one, as the threat is ever-evolving and growing in sophistication. And every stakeholder must be a meaningful participant in the process - engineers, information security professionals, legal, insurance/risk privacy professionals, and policymakers, just to name a few.

Data may be the "new oil," but the omnipresent and growing risks to physical assets in the energy industry call for attention, public discussion and focused work to build cyber defenses (technical, policy-based, and legal) worthy of the 21st century.

Endnote

1 http://energy.gov/oe/cybersecurity-capability-maturity-model-c2m2

The Yates Memo continued from page 3

longer to be considered when deciding whether to pursue claims or charges against them. Prosecutors have long balanced the "twin aims" of returning funds to public coffers and punishing wrongdoers. As part of their determination of whether the level of financial penalty assessed to a director or officer would be sufficient to benefit the public and deter future conduct, prosecutors have, historically, also considered whether such a penalty would be disproportionate or even recoverable in light of the director's or officer's personal means. Under this directive, prosecutors are to be guided by the seriousness of the crime and the ability to secure a criminal conviction or civil judgment, rather than the concerns as to whether the director or officer has funds worth pursuing.

"This will result in new levels of personal risk for board members and increased costs for companies and their insurers."

Only over the course of the coming months and years will the effect of these directives on officers and directors in connection with criminal and civil investigations and prosecutions be fully known. Perhaps most concerning for potential board members, however, are the definitive requirements with regard to cooperation credit and approval for release of liability. These directives go beyond aspirational increases in cooperation and changes in decision making rubrics and require prosecutors and agencies to take affirmative actions to comply with their obligations under the directives. Therefore, the Department of Justice's enforcement of the Yates Memo directives will likely first be visible in denials of cooperation credit and refusals by the government to release individual directors and officers from liability. This will result in new levels of personal risk for board members and increased costs for companies and their insurers.

What Will the Yates Memo Mean for D&O Insurance?

If the Yates Memo indeed brings about a new wave of enforcement, there is little doubt that insurance premiums for directors' and officers' insurance policies will rise. However, in order to provide effective coverage for board members without dramatically raising premiums, companies and their insurers need to anticipate how the specific Yates Memo directives may affect litigation. Among the issues that companies and insurers must consider when discussing coverage for board members and officer are the appropriate scope of conduct exclusions; heightened conflicts of interest; new demands for independent counsel; increases in early, in-depth discovery; higher defense costs; and, increases in judgments against individual directors and officers.

Conduct Exclusions

Perhaps the single largest concern for potential board members in light of the Department of Justice's new focus on individual accountability is whether directors' and officers' insurance will even cover the defense of the charges and claims against them. Although directors' and officers' insurance policies may still cover some or all of the defense, some policies may leave individual directors and officers vulnerable as a result of the new prosecutorial focus on board member accountability for acts that have long been attributed to the corporate entity only. Moreover, the barriers to negotiation and resolution, including the directive that directors and officers will not be released from liability absent extraordinary circumstances, may lead to additional individual charges which, in the past, may have been resolved as part of a company's settlement.

Conflicts of Interest

Directors will also need to re-examine their relationship with General Counsel on whom they have long relied. General Counsel and board members are no doubt aware of the potential conflicts of interests which arise when the interests of the company are at odds with those of the individual directors. Significantly, the new Department of Justice directives may put companies and their directors in conflict far sooner.

As a result, even in the earliest stages of investigation or litigation, the company must provide information about the individuals who made the corporate decisions at issue in order to "cooperate" with the authorities. The decision to seek cooperation will, almost necessarily, require identifying the directors or officers who were part of the decision-making process. In addition, targeted directors and officers may find themselves in a position where identifying other board members or disclosing additional information regarding the company may aid their own defense.

With these significant potential conflicts of interest now arising at almost the very moment when a company comes to anticipate litigation, directors and officers will almost certainly require independent counsel much sooner and more frequently than they have in the past. Not only will the extent of coverage for independent counsel be a concern for potential directors, it is one of the many additional costs insurers and companies must consider going forward in the underwriting process and premium assessment.

Litigation Costs

In addition to possible conduct exclusions and the potential for highly adverse boardroom situations, the Yates Memo directives undoubtedly create additional litigation costs which will require higher policy limits and higher premiums. Both companies and potential board members should be clear about their respective financial burdens if policy limits are exceeded.

The Department of Justice's pursuit of individual directors and officers from the outset of a given action may also add increased pressure to expedite discovery in the early stages of litigation. Rather than making massive disclosures on behalf of the company, targeted investigations could mean targeted discovery. While a streamlined process could theoretically decrease costs, the burden of distilling corporate documents to respond to specific requests regarding the involvement of individual directors and officers will fall heavily on defense counsel and significantly increase the cost of defense. Moreover, as prosecutors have been instructed to fully investigate any productions made, counsel may be required to engage additional discovery requests and more aggressive motion practice.

Additional costs will also arise if the government elects to pursue different civil and criminal cases against individual officers and directors. In addition to the potential need for independent counsel for individual board members, the scope of legal work that can be performed jointly on behalf of numerous directors and officers may be substantially diminished. Moreover, not only may the claims and respective courses of litigation diverge and require separate motion

practice and trials, but tasks such as document productions may become segregated by individual defendant and a single corporate production may no longer suffice.

As is the trend with electronically stored information, using technology to increase efficiency with document production will be key to offset these additional costs and to minimize duplicative efforts on behalf of multiple defendants. One potential strategy may be to have counsel work with investigators to develop agreeable defendant-specific search terms. A robust production of documents responsive to these search terms will put the defense in an advantageous position should the government press for additional, duplicative disclosures.

Judgments

Beyond increased defense costs, larger judgments and added obstacles to negotiated resolutions may also push defense costs beyond current policy limits. The Yates Memo directive that an individual's ability to pay should not affect prosecution decisions may lead to unprecedented judgments against individual officers and directors.

The ability for board members, companies and their insurers to determine the ultimate range of potential judgments is further obscured by the directive that prosecutors are not to settle matters without an articulated plan for pursuing claims and charges against individual directors and officers. This directive creates the distinct possibility of multiple rounds of defenses and judgments all emanating from a single claim which can quickly exhaust defense funds. Moreover, the uncertainty of the future prosecution of directors and officers makes negotiation of a final resolution within policy limits significantly more difficult.

While the thought of increased defense costs are unpleasant, the potential financial liability for directors and officers if policy limits are reached is likely to dissuade even more potential board members. Insurance policy limits and corporate indemnification policies should be clearly communicated to board members so that they have a complete understanding of the risks they are assuming when they join the board—not when an issue arises. Companies will need to address difficult subjects such as liability policy limits, as well as the other heavy burdens created by the Yates Memo, if companies are attempting to recruit the best and brightest board members.

The Yates Memo represents a significant increase in the potential liability for individual board members. Companies that want to attract board members will need to offer means of mitigating individual risk and will need to work with their insurers to do so. While companies will need to prepare for increased premiums, insurers should also consider the structure of the policies they offer in light of the government's transition from corporate to individual targets.

Endnote

1 The Yates Memorandum is addressed to the Assistant Attorneys General of the Antitrust, Civil, Criminal, Environmental and Natural Resources, and Tax Divisions, the Director of the Federal Bureau of Investigation, the Director of the Executive Office for United States Trustees, and all United States Attorneys.

PLUS
D&O Symposium

2016 D&O Symposium

February 3 & 4, 2016 | New York, NY
Marriott Marquis

PLUS is pleased to announce the topics for the 2016 D&O Symposium!

The 2016 D&O Symposium will cover issues that are currently hot in the D&O insurance marketplace:

- **Consolidation in the Insurance Industry: Is Bigger Better?**
- **Not a D&O Claim Yet? Where's My Coverage?**
- **Shareholder Activism & Litigation in Canada**
- **D&O Exposure Minefield: A Case Study**
- **Private/Non Profit D&O: New Exposures/New Concerns?**
- **The DOJ, SEC and the New Era of Individual Accountability**
- **How Innovative Has D&O Innovation Been? What's Next?**
- **U.S. Securities Class Action Update**

WITH KEYNOTES BY:

Patrick G. Ryan
Chairman and CEO
Ryan Specialty Group LLC

Sallie Krawcheck
One of the most respected voices on Wall Street
CEO & Co-Founder
Ellevest

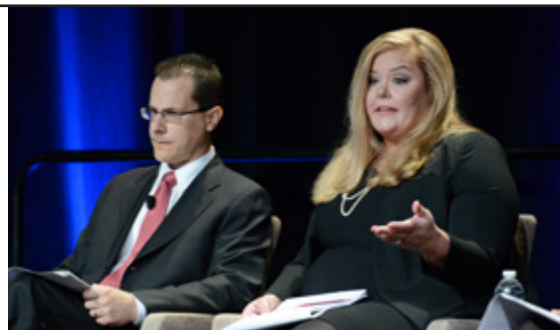
2016 Conference Request for Proposals

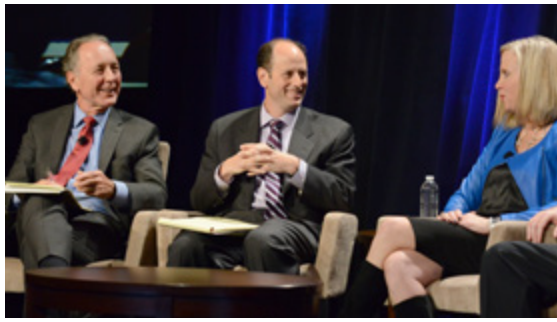
The annual PLUS Conference is the premier educational event serving the professional liability insurance industry. To keep the educational sessions on the leading edge of the industry, PLUS is now accepting proposals for topics and panelists for the 2016 PLUS Conference, November 9-11 in Chicago, Illinois.

To submit a topic to PLUS, please download and complete the Call for Proposals form at:

http://plusweb.org/Events/SubmitTopic.aspx

PLUS must receive proposals before Midnight CST, **February 15, 2016**. Thank you in advance for your submission.





Professional Liability Underwriting Society
5353 Wayzata Blvd., Suite 600
Minneapolis, MN 55416-4758

phone 952.746.2580 or 800.845.0778
email info@plusweb.org
www.plusweb.org

PLUS
5353 Wayzata Blvd., Suite 600, Minneapolis, MN 55416

Calendar of Events

January 2016 • Vol. XXIX • Number 1

**Many Chapter event dates will be finalized and reported in future issues. You can also visit the PLUS website to view the most up-to-date information.*

Chapter Events*

Canada Chapter
- November 19, 2015 • Networking Reception • Toronto, ON
- November 26, 2015 • Education and Networking Reception • Montreal, QC

Eastern Chapter
- February 2016 • Educational Seminar • New York, NY

Hartford Chapter
- March 2016 • Networking Reception • Hartford, CT

Mid-Atlantic Chapter
- February 2016 • Networking Reception • Baltimore, MD
- March 2016 • Networking Reception • Wayne, PA

Midwest Chapter
- February 2016 • Networking Reception • Arlington Heights, IL
- March 2016 • Future PLUS • Chicago, IL
- Spring 2016 • Networking Reception • St. Louis, MO

Northern California Chapter
- March 17, 2016 • Future PLUS w/EIP • San Francisco, CA

Southeast Chapter
- March 3, 2016 • Educational Seminar • Tampa, FL

Southern California Chapter
- March 17, 2016 • Educational Seminar • Los Angeles, CA

Southwest Chapter
- February 2016 • Educational Seminar • Las Vegas, NV

Texas Chapter
- February 18, 2016 • Networking Reception • Houston, TX

International Events

2016 PLUS Foundation: Strikes for Charity
- February 2, 2016 • Bowlmor Lanes, Time Square • New York, NY

2016 D&O Symposium
- February 3-4, 2016 • Marriott Marquis • New York, NY

2016 MedPL/PRS Symposia
- April 20-21 2016 • Chicago, IL

2016 Cyber Symposium
- September 26, 2016 • New York, NY

2016 PLUS Conference
- November 9-11, 2016 • Hyatt Regency • Chicago, IL

The mission of the Professional Liability Underwriting Society is to be the global community for the professional liability insurance industry by providing essential knowledge, thought leadership and career development opportunities.

reuse reduce recycle
The PLUS Journal is printed on recycled paper.

PLUS
Professional Liability Underwriting Society
5353 Wayzata Blvd., Suite 600
Minneapolis, MN 55416-4758
phone 800.845.0778 or 952.746.2580
www.plusweb.org