ACTIVE SHOOTER: Training, preparation help organizations limit damage - PAGE 4

BUSINESS INSURANCE®

www.businessinsurance.com

NOVEMBER 2017

SPECIAL REPORT

CYBER LIABILITY

PAGE 25

SMARTER WORKWEAR

Wearables improve safety but raise privacy concerns

PAGE 31

property	casualty	energy
surety	healthcare professional liability	homeowners
programs	life sciences	construction
travel protection	executive and professional lines	transportation
marine	environmental	builder's risk
medical stop loss	multinational	transactional liability

partner.

IN LOCKSTEP WITH YOU LONG TERM

Berkshire Hathaway Specialty Insurance®

Asheville | Atlanta | Boston | Chicago | Houston | Indianapolis | Irvine | Los Angeles
New York | San Francisco | San Ramon | Seattle | Stevens Point
Auckland | Brisbane | Dublin | Düsseldorf | Hong Kong | Kuala Lumpur | London
Macau | Melbourne | Singapore | Sydney | Toronto

www.bhspecialty.com

BUSINESS INSURANCE®

CEO
Adam Potter

PUBLISHER
Peter Oxner
(Chicago)
poxner@businessinsurance.com

EDITOR
Gavin Souter
(Chicago)
gsouter@businessinsurance.com

DEPUTY EDITOR
Gloria Gonzalez
(Washington)
ggonzalez@businessinsurance.com

SENIOR REPORTER
Judy Greenwald
(San Jose)
jgreenwald@businessinsurance.com

REPORTER
Louise Esola
(New Orleans)
lesola@businessinsurance.com

REPORTER
Joyce Famakinwa
(Chicago)
jfamakinwa@businessinsurance.com

REPORTER
Rob Lenihan
(New York)
rlenihan@businessinsurance.com

REPORTER
Matthew Lerner
(New York)
mlerner@businessinsurance.com

COPY CHIEF
Katherine Downing
(Chicago)
kdowning@businessinsurance.com

COPY EDITOR
Kristen Beckman
(Denver)
kbeckman@businessinsurance.com

ART DIRECTOR
Jeremy Werling
(Cincinnati)
jwerling@businessinsurance.com

DIRECTOR OF RESEARCH, PLANNING AND INSIGHTS
Andy Toh
(Chicago)
atoh@businessinsurance.com

MAJOR ACCOUNTS DIRECTOR - MIDWEST & WESTERN U.S.
Keith Kenner
(Chicago)
kkenner@businessinsurance.com

MAJOR ACCOUNTS DIRECTOR - NORTHEASTERN U.S. & INTERNATIONAL
Ron Kolgraf
(Boston)
rkolgraf@businessinsurance.com

HEAD OF SALES - EVENTS & WORKERS COMPENSATION MAGAZINE
Jeremy Campbell
(Cincinnati)
jcampbell@businessinsurance.com

HEAD OF EVENT PROGRAMMING
Joanne Wojcik
(Denver)
jwojcik@businessinsurance.com

DIGITAL OPERATIONS MANAGER
Kate Lichnerska
(Chicago)
klichnerska@businessinsurance.com

MARKETING MANAGER
Katie Kett
(Portland)
kkett@businessinsurance.com

REPRINT SALES MANAGER
Lauren Melesio
(New York)
lmelesio@businessinsurance.com

SUBSCRIPTIONS & SINGLE COPY SALES
membership@businessinsurance.com
954-449-0736

Business Insurance is published by Business Insurance Holdings.

COVER STORY

Augmented reality is coming to a workplace near you in the form of helmets, glasses, belts, watches and more. These wearable devices promise to help employees work smarter and safer and keep them healthier, but what about the related privacy issues? Experts advise employers to obtain the consent of workers, only collect the data they need and guard it carefully. **PAGE 31**

INSIDE

SPECIAL REPORT: CYBER LIABILITY

The cyber insurance market comes of age as buyers weigh the costs and benefits of coverage; ransomware gives risk managers headaches; the pitfalls of complying with New York's cyber regulations; preparing and practicing for hacks. **PAGE 25**

NEWS ANALYSIS

FOR BREAKING NEWS COVERAGE, VISIT
businessinsurance.com

RISK MANAGEMENT
In the wake of the Las Vegas shooting, organizations refocus on training, security and mitigation. **PAGE 4**

WORKERS COMP
Workers compensation fraud abounds, even though getting caught is more likely than ever. **PAGE 12**

INTERNATIONAL
Ecuador has a long history of earthquakes, but a 2016 temblor shook up its insurance market. **PAGE 17**

PERSPECTIVES
Insurance coverage attorney James Buldas discusses the ins and outs of indemnity agreements. **PAGE 35**

OFF BEAT
Demonstrating the power of the press, one TV station comes to a man's insurance rescue. **PAGE 42**

VIEW FROM THE TOP

JOHN HAHN

John Hahn is CEO of EPIC Insurance Brokers & Consultants, a retail brokerage owned by private-equity investor Oak Hill Capital Partners, which bought EPIC in July. He started on the wholesaler side and eventually co-founded EPIC, which has grown substantially over the past 10 years. In this issue, he discusses this year's acquisitions and EPIC's growth strategy. **PAGE 20**

BUSINESS INSURANCE (ISSN 0007-6864) Vol. 51, No. 12, is published monthly by Business Insurance Holdings, 4100 S. Hospital Drive, Suite 209, Plantation, FL 33317. Periodicals postage paid at Fort Lauderdale, FL, and additional mailing offices.
POSTMASTER Send address changes to Business Insurance, 4100 S. Hospital Drive, Suite 209, Plantation, FL 33317. Printed in USA.

Training key in shooting response

BY MATTHEW LERNER
mlerner@businessinsurance.com

Training paired with security and mitigation efforts can help companies, organizations, schools and others avoid being the target of an active assailant, and cope proactively and effectively if such a situation arises, according to those engaged in training and some who have been through an event.

In the aftermath of the Oct. 1 shooting incident in Las Vegas, which left 58 dead and more than 500 injured, such training and tactics have become even more important for organizations looking to minimize exposures and maximize chances for survival.

After the 2012 shooting at Sandy Hook Elementary School in Newtown, Connecticut, "the FBI partnered with other federal agencies such as the Department of Homeland Security, FEMA, the U.S. Department of Education, the U.S. Department of Justice and the U.S. Department of Health and Human Services to adopt 'Run. Hide. Fight.' as the coordinated federal strategy for civilian active shooter response," said Washington-based Unit Chief James Green of the violence reduction unit of the office of partner engagement at the FBI.

"Training is critical, and our clients and many in the security industry are recognizing that," said Nicholas Smith, practice leader for the security risk consulting business unit of Willis Towers Watson P.L.C. in New York

A study by the FBI of 160 incidents from 2000 through 2013 shows businesses are the most frequent venue or target for such occurrences (see chart).

There are preventive measures that can be taken to make a target less compelling or accessible to an attack, sources said.

"The most robust actors in this space are very conscious to develop site-specific active shooter response plans following the Department of Homeland Security's 'Run. Hide. Fight.' methodology," Mr. Smith said. "Training with a site-specific emergency response around violence tends to raise and harden the security profile of the site or facility, and therefore terrorists and criminals may look elsewhere. Training is absolutely a key component of attack avoidance."

REUTERS

Las Vegas Metro Police and medical workers converge at the site of the mass shooting Oct. 1 at the Route 91 Harvest music festival near Mandalay Bay.

"An intruder, based on experience from our security consultant, will take the 'path of least resistance' and move on to an unblocked or unfortified room or area," said Michael Pokora, executive vice president and managing director with Willis Towers Watson in Chicago. In late September, the brokerage launched its Shooter/Armed Intruder Readiness Program for senior living communities, which includes training videos, sample plans and procedures, a readiness assessment and webinars.

Training should also include a mechanism for identifying behaviors that can precede or foreshadow an event, according to experts.

"The first step is to be able to recognize behavior of concern," because subjects sometimes experience a change in behavior prior to acting out violently. This can include social media posts as well as observable actions, said Harry Rhulen, Denver-based president of Novume Solutions Inc. and founder of Firestorm Solutions, a crisis management firm now owned by Novume.

Efforts should include a mechanism for reporting what has been observed, experts say.

"Addressing employee conduct early regarding threats and threatening behavior, in my opinion, is a good mitigation measure," said Regan J. Rychetsky, loss control manager with York Pooling, a unit of York Risk Services Group Inc. in Austin, Texas, and a past president of the Public Risk Insurance Management Association. "Having a formal program where you have an established reporting process and you track all security incidents, together with an employee training program to bring awareness to the issue," is a good way to help accomplish this, he said.

"The thing we all need to get better at is reporting things. I think that makes a huge difference," said Cindy Stevenson, current superintendent of the Boulder Valley School System and a previous Jefferson County superintendent of 12 years, retiring in 2014.

Ms. Stevenson was in Jefferson County when the shooting event occurred at Columbine High School in Colorado on April 20, 1999. Colorado subsequently mandated that every school in the state have a safety plan.

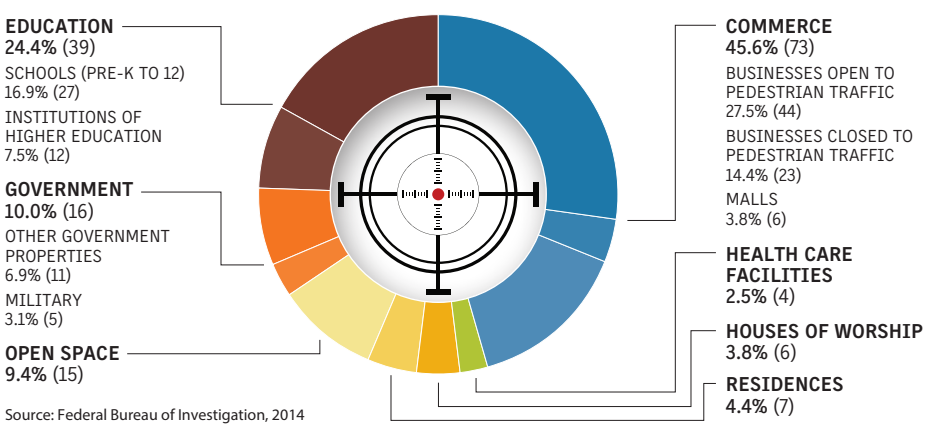
"We've learned a lot from the incidents that have occurred in schools, and I think that schools and agencies and districts have taken that all to heart and used it in the training process," she said.

Another aspect of successful training is repetition, sources said. "Training has to occur again and again and again," said Scott Murphy, retired superintendent of the Littleton Public School District in Colorado who was in his position during a shooting incident at Arapahoe High School in December 2013.

"In a crisis situation, you revert to your level of training," Mr. Rychetsky said, citing school fire drills as an example.

LOCATION CATEGORIES

A study of 160 active shooter incidents in the United States between 2000 and 2013



Source: Federal Bureau of Investigation, 2014

TECHNOLOGY A RELIABLE PARTNER IN PREDICTION

Technology is increasingly being used in efforts to mitigate and respond to active-assailant exposures.

Looking to the internet for signs of behaviors that could be a prelude to someone acting out has been made easier and more effective through the use of tools and technology, according to sources.

"There are tools out there that allow you to crawl through the data," looking for relevant words, names and other information, said Harry Rhulen, Denver-based president of Novume Solutions Inc., and founder of Firestorm Solutions, a crisis management firm owned by Novume.

An organization, company, or other group should be aware of its online presence.

"It's important to understand company executives' posture on social media," said Nicholas Smith, practice leader for the security risk consulting business of Willis Towers Watson P.L.C. in New York.

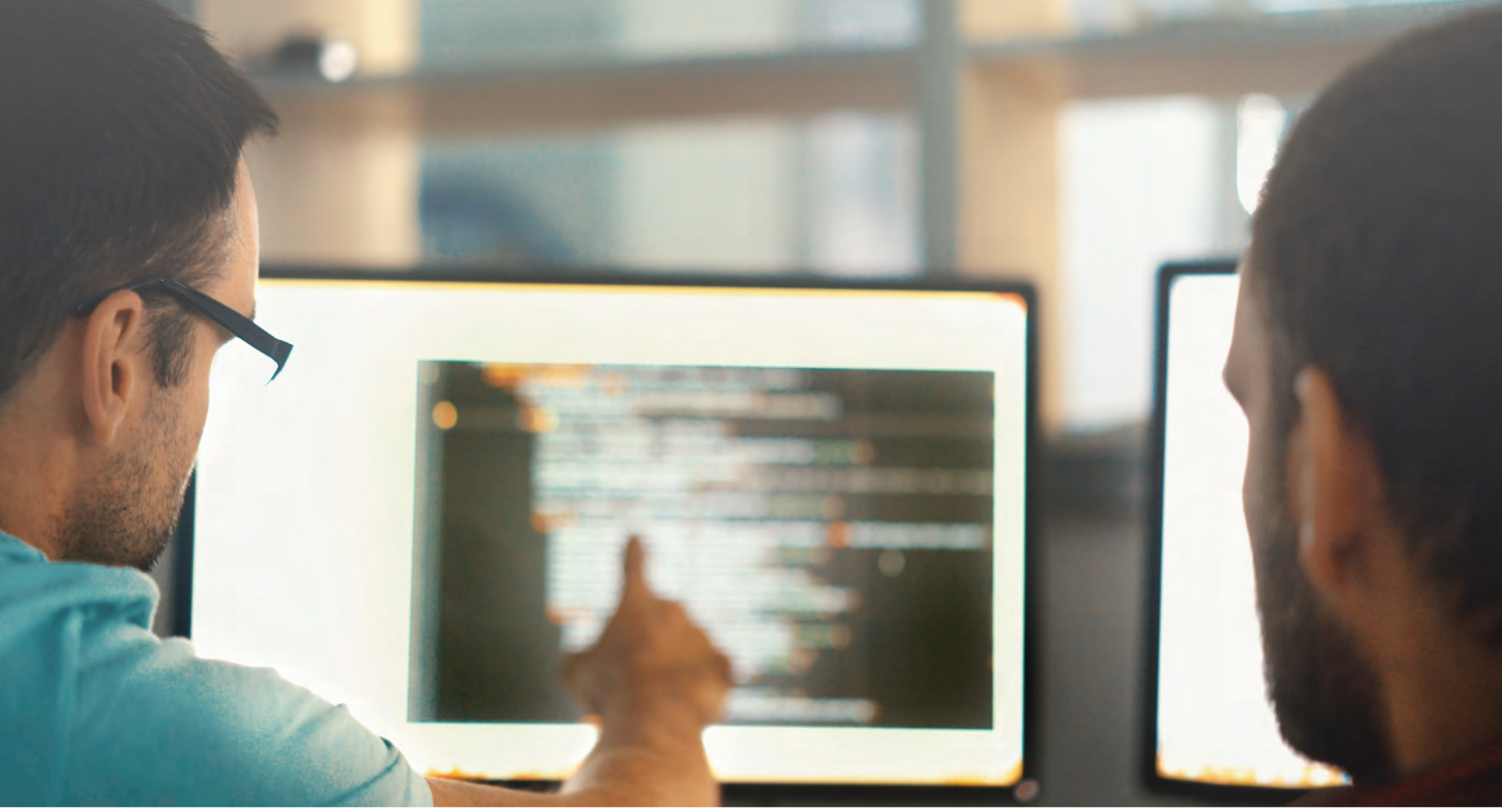
"Social media intelligence — what I like to call social media protective intelligence — is one of the few innovative and creative industry tools of the last five to 10 years that jumped out at me and I thought was a huge step forward," he said.

Technology can also be a part of a company's or organization's efforts to report and track incidents of troubling behavior. Firestorm has developed a tool using texting as the mechanism for the anonymous reporting with a company or organization, according to Mr. Rhulen.

Communication has also become more robust.

"We have electronic resources," said Scott Murphy, retired superintendent of the Littleton Public School District in Colorado, who was in his position during a shooting incident at Arapahoe High School in December 2013. "We can engage people very quickly, both to get information to them and from them. The ability of organizers to communicate quickly and outside the normal media chain has been extremely helpful."

Matthew Lerner



Training masters.

Claims gurus. Lawyers. Worldwide.

Meet your cyber-age insurance team.

For nearly 20 years, AIG has built a network of experts and a spectrum of award-winning solutions to help protect clients from cyber risk. With global claims expertise, end-to-end cyber risk management services, and proactive planning and response, we're here to help businesses become more cyber resilient. See how we can tackle the challenges of an ever-evolving cyber world together.

To learn more, visit www.AIG.com/cyberedge

AIG®

Disability suits over website access surge

BY JUDY GREENWALD
jgreenwald@businessinsurance.com

More courts are ruling against companies over the issue of website accessibility, while the number of lawsuits filed against them continues to grow dramatically.

Plaintiff attorneys have been encouraged in particular by a U.S. District Court ruling in Miami in *Juan Carlos Gil v. Winn-Dixie Stores Inc.* that, following a trial, held the supermarket chain was obligated to provide an accessible website to a legally blind plaintiff under the Americans with Disabilities Act (see related story).

In addition to the basic issue of accessibility, courts disagree whether, under the ADA, only companies that have "brick and mortar" facilities are obligated to provide accessible websites or if the law applies to web-only businesses as well.

Complicating the situation, experts say, is the federal government's failure to date to develop promised clear guidelines on this issue, which has left the law's interpretation up to courts that have released divergent rulings on the issue.

Experts say although the Obama administration promised regulation in this area in 2010, it never followed through, nor is any rule expected from the U.S. Department of Justice under the Trump administration, which has put the issue on its "nonactive" list.

For now, many firms concerned about the issue are complying with the World Wide Web Consortium's voluntary, privately developed Level AA Success Criteria of the Web Content Accessibility Guidelines 2.0, although alternatives, such as 24/7 phone access, may be considered acceptable as well, experts say.

The basic issue is disabled users' ability to easily access company websites. Experts say the cost of achieving this can vary widely. It is relatively inexpensive for firms that are starting from scratch, but it can become considerably more complicated — and expensive — for complex existing sites.

The screen readers that enable the blind to read websites operate as an interface between the computer's operating system, its applications and the user, according to the New York-based American Foundation for the Blind.

The user sends commands by pressing different combinations of keys on the computer keyboard or braille display to instruct the speech synthesizer what to say and to speak automatically when changes occur on the computer screen.

Although the ADA covers a wide range of disabilities, the clear majority of the litigation over website accessibility has focused on those who are visually impaired, experts say.

Many firms still do not have accessible websites, said William D. Goren, a Decatur, Georgia-based attorney and ADA consultant. These are cases where website designers are "trying to design something that looks really cool" but "don't think about how people with disabilities must have to use it," he said.

The general legal trend is pro-plaintiff, say observers.

"The pendulum is certainly shifting" toward rulings that say a company's website needs to be accessible under the Title III of the ADA, said Steve A. Miller, regional managing partner with Fisher Phillips L.L.P. in Chicago.

Title III prohibits discrimination on the basis of disability in places of public accommodation.

A court ruling on the issue "really depends on what court you're in and which judge you get," said Kristina M. Launey, a partner with Seyfarth Shaw L.L.P. in Sacramento, California. But each pro-plaintiff ruling "emboldens plaintiff attorneys to push harder."

Meanwhile, encouraged by the *Winn-Dixie* ruling, more plaintiff firms are filing suit, although there is no requirement that courts in other jurisdictions follow the decision, experts say.

The number of suits filed in federal court over accessibility surged this year (see box). This doesn't include cases filed in state court nor demand letters sent by plaintiffs to firms that are resolved without litigation.

"It's not just the volume. You're seeing a huge increase in the number of players in the space," said Joshua A. Stein, a member of law firm Epstein Becker & Green P.C. in New York.

Increasingly, he said, plaintiff attorneys who had not operated in this space before are now filing copycat cases, he said. This can make it more difficult for defendants because, unlike the firms that had specialized in this area, these attorneys do not understand the litigation's substance, he said.

Another issue facing defendants, he said, is that in cases where there have been settlements, the company is given, for instance, 18 months to modify its website, but then additional lawsuits are filed against it even before it can introduce the agreed-upon changes.

There has also been a piling-on of cases, "where the same businesses are being sued multiple times across the country by different plaintiffs and firms," said Joseph J. Lynett, a principal with Jackson Lewis P.C. in White Plains, New York.

Observers say the problem is the lack of federal guidance. "There are multiple benefits to having regulation in this area," said Mr. Lynett. Not only would it add clarity to the accessibility standard, but once it is introduced there is usually a 12- to 18-month compliance period that "essentially closes the courthouse door" to plaintiffs filing suit, he said.

And while the ADA's Title III prohibits discrimination on the basis of disability in the activities of places of "public accommodation," the issue of whether the 1990 law applies to website-only companies remains unsettled, observers say.

"A small majority of the courts of appeal have looked at this and have said in order for a website to be considered a place of public accommodation, it must have some nexus or connection to a physical location," which derives from the ADA's 1990 passage, when banks and retail stores "were expressly included in what constituted a place of public accommodation," said Mark T. Phillis, a shareholder with Littler Mendelson P.C. in Pittsburgh.

Meanwhile, litigation is expected to continue, said Mr. Lynett. "I don't see any reason why the plaintiffs bar is going to stop feeding from the trough here," he said.

WINN-DIXIE DECISION SPURS ADDITIONAL SUITS

A U.S. District Court ruling that holds a supermarket chain must make its website more accessible to the visually impaired is encouraging litigation against other firms, experts say.

While there have been other pro-plaintiff rulings since, the June 13 ruling by the U.S. District Court in Miami in *Juan Carlos Gil v. Winn-Dixie Stores Inc.* has garnered significant attention because it followed a bench trial rather than being based on a motion to dismiss, experts say.

Mr. Gil, who is legally blind, filed suit against the Jacksonville, Florida-based supermarket chain because of problems he had with his screen reader software in using the chain's website, according to the ruling.

"The factual findings demonstrate that Winn-Dixie's website is inaccessible to visually impaired individuals who must use screen reader software," says the ruling by Judge Robert N. Scola Jr.

"Therefore, Winn-Dixie has violated the (Americans with Disabilities Act) because the inaccessibility of its website has denied Gil the full and equal enjoyment of the goods, services, facilities, privileges, advantages or accommodations that Winn-Dixie offers to its sighted customers," says the ruling.

"Winn-Dixie has presented no evidence to establish that it would be unduly burdensome to make its website accessible to visually impaired individuals," said the ruling.

"To the contrary, its corporate representative unequivocally testified that modifying the website to make it accessible to the visually impaired was feasible," said the ruling, in also holding Mr. Gil proved he is entitled to injunctive relief in the case.

The decision is being appealed to the 11th U.S. Circuit Court of Appeals in Atlanta.

Judy Greenwald

PARADIGM RULE #12 | **Don't ask your mechanic to give you a root canal.**

PARADIGM RULE #1 | **Catastrophic injuries require catastrophic experts.**

Expert CAT teams

- ✓ 50 best in class physicians
- ✓ 200 specialist nurses
- ✓ 3x more CAT cases than anyone else

Better outcomes

- ✓ 5x better clinical outcomes
- ✓ 40% lower costs, per Milliman
- ✓ Fixed price contract, guaranteed

Amputation • Brain • Burn • Multiple Trauma • Spinal Cord

800.676.6777 | paradigmcorp.com/rules

PARADIGM® OUTCOMES

Harassment claims set to increase

By Judy Greenwald
jgreenwald@businessinsurance.com

Other companies are likely to continue to feel the fallout from the problems of film producer Harvey Weinstein, who resigned from his position as co-chairman of the Weinstein Co. last month after numerous allegations of sexual harassment and assault were revealed.

The Weinstein incident has led to a deluge of sexual harassment complaints from women in many industries.

Fidelity Investments, Fox News, Uber Technologies Inc. and various Silicon Valley-based firms are among those that have been accused of tolerating a culture of sexual harassment.

In addition, New York Attorney General Eric G. Schneiderman announced a civil rights investigation into Mr. Weinstein's former firm

"As more of these high-profile cases come to light," it will "embolden women to come forward, too, in other companies," said Paul E. Starkman, a member of law firm Clark Hill P.L.C. in Chicago.

The allegations came after years of decline in the number of sexual harassment charges filed with the U.S. Equal Employment Opportunity Commission (see chart).

Some question, however, whether the Weinstein incident will ultimately lead to any significant change.

Experts say the way to avoid problems is to encourage a "top down" culture in which even top executives and performers are expected to act appropriately (see related story).

"I think the lesson really is, no matter who in an organization is involved … you can't bury your head in the sand like an ostrich and just ignore it," said Jonathan T. Hyman, a partner with Meyers, Roman, Friedberg & Lewis in Cleveland.

Referring to reports that Mr. Weinstein had settled at least eight sexual harassment charges in the past, Mr. Hyman said if board members see large checks going out, "maybe you should ask somebody why we're cutting so-and-so a $100,000 check — and if you don't have the answer, maybe you have an obligation to get to the bottom of what's going on."

REUTERS

Actress Rose McGowan, one of the many women with sexual harassment complaints against Harvey Weinstein, speaks at the opening session of the three-day Women's Convention in Detroit in October.

There was "so much smoke, it's hard to believe anyone besides Harvey didn't know what was going on," said Mr. Hyman.

In addition to potential violations of Title VII of the Civil Rights Act of 1964 stemming from charges made by employees against Mr. Weinstein, there are also charges being made by nonemployees, Mr. Hyman said.

"If I were a board member, I'd be really nervous" about investors suing the company for breach of their fiduciary obligations, Mr. Hyman said.

He pointed to litigation filed by shareholders of Los Angeles-based American Apparel Inc., which faced shareholder lawsuits after its former chairman, Dov Charney, was fired for allegedly misusing funds and allowing the posting on the internet of nude photos of a former female employee who had accused him of sexual harassment.

Private companies can also be sued by their shareholders and others.

The Weinstein publicity will lead to lawsuits filed against other employers, say experts.

"I think we'll see a trickle down, where people will start to see these claims more," in part because the case is "very high-profile," said Mr. Hyman.

The case "probably demonstrates that there's still a significant problem with harassment and gender discrimination in the upper management of many large companies," said Mr. Starkman. It shows there are company leaders who "believe that the rules regarding harassment or discrimination don't apply to them," he said.

"There needs to be additional training," he said. Boards of directors and major shareholders "need to recognize that this is an issue, and the fact that the person has increased the bottom line and met financial goals does not mean that they're filling all their responsibilities as leaders, because you cannot have subordinates" in the human resources or legal departments "trying to tell CEOs and owners of companies what they can and cannot do."

"They can try, but it's often a recipe for a quick exit out of the organization, so it has to come from the people who have influence on the top-level decision-makers, and then it needs to be carried through in terms of training and oversight down the organization," Mr. Starkman said.

Sara E. Flotte, a partner with Michael Best & Friedrich L.L.P. in Chicago, said executives should be aware they may be held personally liable for sexual harassment.

"One hook that I often use with clients who say, 'the CEO or someone in a position of power isn't going to listen to me' is to remind those individuals in power that there's personal liability associated with sexual harassment claims in many states," she said.

Martha J. Zackin, a partner with Bello/Welsh L.L.P. in Boston, said she is concerned this situation will lead more firms to follow the "so-called Pence rule."

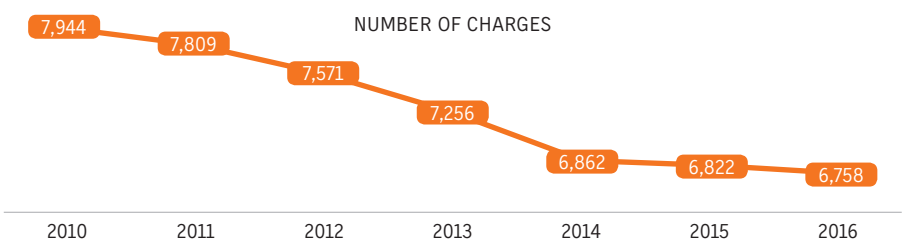
She noted that Vice President Mike Pence has made it publicly known he will not attend a dinner alone with a woman or any event where alcohol is served without his wife's presence.

The reaction to the Weinstein case "could be that men are going to be less willing to be mentors and to work with women on a one-on-one basis, which is how men get a lot of help — by being mentored and having good, substantive discussions. But those (mentoring meetings) don't tend to happen in the workplace," she said.

"It could end up really limiting networking and mentoring opportunities for women, more than they're already limited," she said.

SEXUAL HARASSMENT CHARGES

Charges alleging sexual harassment filed with the U.S. Equal Employment Opportunity Commission



Source: U.S. Equal Employment Opportunity Commission

BEHAVIOR IN C-SUITE MUST BE ADDRESSED

Employers need to tackle the issue of sexual harassment, particularly when it comes from the executive suite, say experts.

"This is an important issue that maybe hasn't been addressed as much as it should have been," said Eric B. Meyer, a partner with law firm Dilworth Paxson L.L.P. in Philadelphia. "Maybe we don't do enough training in the C-suite."

"I'm certainly talking to my clients about 'when was the last time you did harassment training,'" said Jonathan T. Hyman, a partner with Meyers, Roman, Friedberg & Lewis in Cleveland.

Companies need to have a clear, well-defined policy and complaint and investigation procedures, said Amy Epstein Gluck, a partner with FisherBroyles L.L.P. in Washington.

"When all of these are enforced, you're going to have much less of a possibility" of sexual harassment lawsuits, Ms. Gluck said.

It is important to "take rumors, allegations and observations seriously, and not tolerate behavior like this in the workplace," said Martha J. Zackin, a partner with Bello/Welsh L.L.P. in Boston, referring to sexual harassment.

Treat everyone equally when it comes to addressing sexual harassment complaints, say experts.

Complaints should be addressed even if it is against someone in the C-suite, "someone with whom the buck is supposed to stop," Mr. Meyer said.

It is important for organizations to have a "top-down culture of zero tolerance to keep the workplace free of any harassment," said Ms. Gluck.

"There's no substitute for having that culture of equality and no tolerance for any kind" of harassment, she said. "And it's important not just women report it." The onus should not be just on them to report these issues, she said.

Meanwhile, a report issued in December 2016 by Sterling, Massachusetts-based Betterley Risk Consultants Inc., which described an intensely competitive market for employment products liability insurance, said EPLI value-added services provided by insurers, "when done right," offer employers access to tools "that can truly make a difference in the frequency and severity of claims — as well as the bad feelings that accompany employee/employer disputes."

Judy Greenwald

IF IT CAN BE BUILT, IT CAN BE HACKED.

SO IT'S A GOOD THING WE'VE EXPANDED THE CYBER COVERAGE IN OUR ADVANTAGE POLICY.

The new reality is that cyber exposure is no longer limited to credit card breaches, identity thefts, or even network interruptions. Now everything that is connected, from production to power, can be hacked. But you can be prepared for it with the cyber protection of our FM Global Advantage® policy. Expanded cyber coverage backed by increased assessment and mitigation is just what you need to take on new threats.

WHEN YOU'RE RESILIENT, YOU'RE IN BUSINESS.®
SEARCH **FM GLOBAL CYBER** FOR MORE.

FM Global®

MOUNT A STRONG DEFENSE AGAINST RANSOMWARE *BEFORE* YOUR FILES ARE TAKEN HOSTAGE.

HOW VULNERABLE ARE YOU TO RANSOMWARE ATTACKS?

- An average of almost 730,000 attacks per month[1]
- Ransoms as high as $50,000 are not unheard of
- Employees click on phishing emails 20 percent of the time[2]
- If 10 employees receive the same phishing email, one will likely click on it

Extortion through ransom notes, although new to the digital arena, is a crime that's been committed in the U.S. since the late 19th century.

The first ransom note in American history was written in 1874, when kidnappers demanded $20,000 to return 4-year-old Charley Ross to his parents. "You wil [sic] have to pay us before you git [sic] him from us, and pay us a big cent to [sic]," the note read.

Ransom notes have come a long way since that hand-scribbled message. In our digital world, the form has morphed into malicious software that holds a computer and its data hostage. Victims' computers are to be set free only after the ransom money demanded is paid—usually in cryptocurrency like bitcoins in lieu of paper money. Personal computers are most commonly attacked, but businesses of all sizes are a growing target.

The first case of ransomware dates back to 2005. And the number of attacks has grown exponentially since then. Ransomware attacks in 2014 were up 113 percent over 2013, according to Symantec's 2015 Internet Security Threat Report, **with an average of almost 730,000 attacks per month.**[1]

When the files held hostage are held dear by their owners, victims often pay the ransom that criminals demand. It usually ranges anywhere from $300-$600, though ransoms as high as $50,000 are not unheard of.

HOW DOES RANSOMWARE BREAK INTO YOUR COMPUTER?

Ransomware may be triggered in different ways: a phishing email that looks like a legitimate invoice or image; a visit to an infected website; or an ad containing malware that's been injected into a legitimate webpage.

When an unsuspecting victim opens the email or inadvertently falls into a ransomware-laden trap, the virus is silently installed on the victim's computer.

HOW DOES RANSOMWARE HOLD YOUR FILES HOSTAGE?

There are two types of ransomware attacks:

1. Locking. Lock-screen ransomware displays a window that prevents access to any part of the computer until a sum is paid.
2. Scrambling. File-encrypting ransomware is a more sophisticated adaptation that keeps the computer available but scrambles certain types of files; for instance, databases that hold sensitive or proprietary customer and business information. Then it displays a pop-up screen with detailed instructions on how to buy the private decryption key that will decrypt the scrambled files.

HOW SHOULD YOU RESPOND?

Lock-screen ransomware can often be cleared by shutting down one's computer and starting it back up again. There's no such simple fix for file-encrypting ransomware. Lack of access to essential data can be crippling for a business, compelling business owners to act quickly to resolve the intrusion.

The right response: *Neither negotiate with nor pay the perpetrator.*

Those who cooperate with the criminals only encourage continued crime. They may also pay a heavy ransom and never get their data back.

But the element of time and other practical considerations can sometimes force a business owner's hand.

If your business falls victim to ransomware, take these steps:

1. **Report** the incident to your local FBI office and file a complaint with the Internet Crime Complaint Center.
2. **Restore** file backups if you have them. Backups can immunize your business from the effects of an attack.
3. **Check your insurance coverage.** Cyber insurance policies may cover the cost of the ransom money paid and provide response assistance. Before you act, review policy terms regarding:
   - What is and isn't covered
   - Requirements for prior consent
   - Guidelines on how to respond. Does the insurance company want to interact with the bad guys or do you make the decisions?
   - Services and resources to guide you through the response process, including third parties to coordinate with law enforcement and handle negotiations
   - Ransom reimbursement
4. **Pay the ransom *only* if all else fails** within a timeframe that's reasonable for your business. According to an October 2015 article in *SC Magazine,* a security news and information resource, the FBI recommends this option for file-encrypting ransomware, simply because it's so difficult to crack.[3]

Payment is generally required in bitcoin, a mysterious and unfamiliar form of currency for most people that has a learning curve associated with it. You'll need to set up an account at an online exchange and purchase bitcoin in order to release funds to the extortionist.

The Hartford offers a unique and comprehensive risk management solution that rewards businesses for boosting their defense against cyber crime. Find out how at thehartford.com/cyber.

HOW CAN YOU PROTECT YOUR BUSINESS FROM CYBER EXTORTION?

Businesses should anticipate the real possibility of cyber extortion and take these preventive measures now so they don't fall victim later:

- **Back up sensitive business files regularly** and maintain copies off your main network. Backed up files can be quickly restored, averting the effects of an attack.
- **Plan your business's response.** Establish safeguards, including multifactor authentication to protect sensitive data from unauthorized access and use.
- **Educate employees on ransomware and how it works.** Conduct training sessions on detecting suspicious emails and attachments, and set up a protocol for reporting them to a designated manager.
- **Install updates to your company software** as soon as they're released. They often contain patches that address security vulnerabilities that help keep your business protected against online threats.
- **Purchase cyber liability insurance** with the option to include coverage for cyber extortion loss, which entitles you to assistance in responding to a threat and also reimburses the ransom amount if payment is made.

Visit **thehartford.com/cyber** today for additional cyber insights and resources.

THE HARTFORD

Business Insurance

Employee Benefits

Auto

Home

[1] www.symantec.com/security_response/publications/threatreport.jsp
[2] phishme.com/enterprise-phishing-susceptibility-report/
[3] www.scmagazine.com/cheaper-easier-for-hacked-businesses-to-pay-ransom/article/449489/

CyberChoice First Response is offered on a SURPLUS LINES basis.* For Producers Only – Not for Distribution to the General Public.

*Eligibility for surplus insurance coverage is subject to state regulation and requires the use of a licensed surplus lines broker. Surplus lines insurance policies are generally not guaranteed by state guaranty funds. Policies should be examined carefully for suitability and to identify all exclusions, limitations, and other terms and conditions. Surplus lines coverage is underwritten by Pacific Ins. Co. Ltd (except in CT and HI) and Hartford Ins. Co. of Illinois in CT and HI. The Hartford has arranged for data risk management services for our policyholders at a discount from some third-party service providers. Such service providers are independent contractors and not agents of The Hartford. The Hartford does not warrant the performance of third-party service providers even if paid for as part of the policy coverage, and disclaims all liability with respect to use of or reliance on such third-party service providers.

The Hartford® is The Hartford Financial Services Group, Inc. and its subsidiaries. Its headquarters is in Hartford, CT.

Social media posts flag comp fraud

BY LOUISE ESOLA
lesola@businessinsurance.com

Double-dipping, Monday-morning injuries, faking, malingering and illegal banking activity are mainstays in workers compensation claimant fraud with no end in sight despite the fact that it's now easier to get caught, according to experts.

"We are seeing the same things over and over again," said Dan Fodor, assistant director with the special investigations department for the Ohio Bureau of Workers' Compensation, which distributes public information on fraudulent claimants in an effort to raise awareness of the crime that often comes with prison time and fines in the tens of thousands of dollars.

"Insurance fraud, across the board, has gone up," said Sam King, Glendale, California-based vice president of Fraud Investigations for Employers Holdings Inc., a holding company that specializes in workers comp insurance and services. "There's an acceptance factor in the public that wasn't there 20 years ago."

"For whatever reason (offenders) think 'It's not going to happen to me, I'm not going to get caught,'" Mr. Fodor said of those who commit claimant fraud. "I think the bottom line is people want money; they want more money than they are entitled to. So they circumvent the system … and get caught."

"It might be easier to tell you what I haven't seen," said Thomas Martin, president and lead investigator with Newport Beach, California-based Martin Investigative Services, which helps insurers and employers investigate fraud — a steadily increasing stream of business. Mr. Martin estimates that upwards of 25% of workers comp claims have some element of fraud involved. "It's like a feeding frenzy."

Mr. Fodor has a word for what is increasingly helping insurers and employers tackle the workers comp fraud problem: technology.

"While what they do hasn't changed, how we find them has evolved with technology," Mr. Fodor said.

For example, prescription fraud — especially when it comes to opioids — is a continuing problem, one easily mitigated by a doctor's ability to check a prescription-monitoring database, he said. Forty-nine states now have such databases in place; Missouri is creating its own.

Meanwhile, exaggerated or fake injuries are now easier to uncover, experts say.

Sometimes it's traditional video surveillance while other times it's a claimant's social media activity that tips off investigators, said Steve Cassell, Lake Mary, Florida-based president and CEO of Command Investigations L.L.C.

"(Social media) is an addiction; people can't put their phones down," said Mr. Cassell, adding that roughly 80% of adults use one or several social media platforms. "Lawyers always tell injured workers to get off social media, but social media doesn't skip a beat. People drink a wonderful cup of coffee and they post about it."

Or, they play football, lift weights, get another job, and post photos and "brag"— examples of some of the cases Command has worked on in the past, according to Mr. Cassell, who cautions that firms such as his can only use information that is publicly available. And there's no shortage, he added.

"Head and shoulders above anything else from falsifying an accident or exaggerating an injury, the biggest trend is how social-media monitoring is being used as an investigative tool to understand and predict future activities of these presumably injured people," Mr. Cassell said. "People brag; it never stops."

Mr. King said one software program allows investigators to search upwards of 200 social media sites. "All you need is an email address," he said. "It's all public information."

In many instances, social media gives investigators the tip they need to know that video surveillance — which is more likely to be admissible in court because of the time stamp — might be necessary, said Mr. Cassell, adding that photos posted of an injured worker engaged in an activity could have been taken pre-injury.

Meanwhile, companies are also catching on to surveilling employees before an incident; real, exaggerated or fabricated altogether, experts say.

"Employers have wised up and put surveillance all over the place," said Jim Marasco, a partner with Rochester, New York-based StoneBridge Business Partners, which provides litigation support for insurers on evaluating loss claims. "Offices, parking lots, everywhere."

Take, for example, the widely publicized sprinkler-head incident, a video that has gone from employer to news outlet and now, YouTube.

In the video, a woman is sitting at her desk in Fort Lauderdale, Florida, when a sprinkler head falls from the ceiling, hitting a space just in front of her. She picks up the sprinkler head, pauses, and — after a quick glance around — hits herself on the head with it. Voila!: workplace injury.

As reported in media outlets, her employer's insurer got suspicious of the claim and referred the incident to Florida's Division of Investigative and Forensic Services, which then requested security camera footage, now available on YouTube.

"Get good surveillance," is a piece of advice Mr. Marasco tells clients grappling with questionable claims.

Aside from faking the severity of an injury, experts say real injuries that were incurred outside of the workplace are finding their way into the comp world. Injuries from extreme sports, gardening or merely tripping on an uneven sidewalk can wind up as workers comp claims, according to experts.

Here, surveillance also helps, said Mr. Marasco. "There's surveillance in parking lots, too," he said. "It's interesting to see (a worker) hobble in on a Monday morning and, all of a sudden, has a workplace accident."

WORRYING ABOUT FRAUD

13%
of small businesses are concerned about workers comp fraud

24%
of small businesses have installed surveillance cameras on their properties

21%
of small businesses say they are unprepared to identify workers comp fraud

Source: Employers Holdings Inc. survey of small businesses grappling with fraud

EXPENSIVE HEALTH CARE, UNCERTAINTY DRIVE WORKERS TO CHEAT COMP SYSTEM

Contributing to the problem of workers compensation fraud are the uncertainty of health care coverage with the new presidential administration, high-deductible insurance plans that call for an employee to spend at least $1,000 before benefits kick in and the ever-increasing cost of doctor-visit copays, experts say.

"There's a greater incentive to go through workers comp," said Jim Marasco, a partner with Rochester, New York-based StoneBridge Business Partners, which provides litigation support for insurers on evaluating loss claims. "It's always advantageous to say, 'I got hurt at work.' That's the richer policy: workers comp."

Under workers comp — a liability coverage — employees see all medical costs covered in most cases, along with indemnity payments and more.

"This problem is high on the radar for insurers," a spokesman for the Washington-based Coalition Against Insurance Fraud said. "It will likely accelerate as the uncertainty in health care continues because workers are not counting on their health coverage any longer; increasingly we will likely see more nonwork claims being dumped onto workers comp insurers so that the people can have that certainty of coverage at far more affordable terms than they are getting with their traditional health coverage."

"This is more than just chatter; this is an increasing reality in the street," the spokesman said.

Louise Esola

Transatlantic Law Firm of the Year 2017
The American Lawyer/Legal Week

CLYDE&CO

When it comes to risk, the world is more interconnected than ever. A risk in one location or line of business can quickly spiral into others. Managing risk requires connection of experience across a range of business areas and economies. That's why we're creating a law firm that can partner with you to manage risk across business lines, in the US and around the world

Find out how we can partner with you at clydeco.com/US

Atlanta, Chicago, Miami, New Jersey, New York, Long Beach, Los Angeles, San Francisco, Washington, DC and over 40 offices globally.

J401739 - October 2017

Nurse triage services expand into telehealth

BY JANET LAVELLE

As companies weigh whether to expand their workers compensation strategies to include telemedicine, many are maintaining or expanding the use of more traditional 24/7 nurse triage phone centers and on-site clinics to quickly evaluate injured workers.

Nurse phone triage and on-site clinics have been around for two decades or longer, but have grown substantially in the past decade — growth that continues, according to service providers.

Nurse triage calls are the first step in evaluating an injured worker and determining whether self-care, treatment by a doctor or a trip to the emergency room is in order. That immediate attention can prevent unnecessary medical tests and trips to the ER, while saving time and keeping some workers on the job, experts say.

Third-party administrator Gallagher Bassett Services Inc. "has seen no slowing of interest in our nurse triage program. Customers often call it the most important part of their workers comp program," said Niel Simon, senior vice president of vendor solutions and medical operations for the Itasca, Illinois-based firm.

More than 80% of its larger clients use nurse triage, he said.

At McHenry, Illinois-based Medcor Inc., a provider of on-site clinics and nurse triage phone services, there's still "strong interest" in nurse triage, with a "better than 98% retention rate," said Executive Vice President Curtis H. Smith.

Medcor opened its first on-site clinics in 1984 and now operates 200 of them for 80 public- and private-sector entities. Clients choose whether to include occupational health and workers comp services along with primary care.

Medcor began its nurse triage phone line for worker injuries in 1997. It employs 104 nurses trained on Medcor triage software that uses algorithms to determine best treatments. The company contracts mostly with large, self-insured companies, although some insurers include it in benefits packages to midsize companies, he said.

Medcor provides injury triage at about 250,000 work sites and fields about 1,000 calls a day, with 40% of injured workers recommended for self-care, 60% told to see a doctor, and 1% directed to call 911.

While nurse triage lines have been popular among large employers, many companies are now considering whether to move into telemedicine that provides video conferencing with a doctor who can treat or advise on visual injuries such as lacerations, contusions and mild burns.

Nurse triage is "the gateway" to telemedicine, as about a third of clients with nurse triage services inquire about expanding into telehealth, Mr. Simon said.

Over the summer, Gallagher Bassett piloted a telemedicine program and has just made it available broadly to its clients, he said.

"A lot of clients are asking about it but are waiting to see the data" on cost-effectiveness, Mr. Simon said. Still, he expects interest to grow over the next six months.

Third-party administrator Sedgwick Claims Management Services Inc., based in Memphis, Tennessee, has offered a 24/7 nurse triage service since 2008 that is used by more than 100 Fortune 500 companies, said Jim Harney, vice president of client services.

In June, Sedgwick began a pilot program in telemedicine for workers comp injuries and made it available in July to all clients that use the nurse triage service, which Sedgwick calls a clinical consultation service. A "handful" of clients have opted not to have telemedicine as an option, Mr. Harney said.

For an employee whose injury can be treated through a video call, "the benefit really comes from that continued productivity — the ability to eliminate travel and save time," Mr. Harney said.

While employers decide whether to move ahead with telemedicine, others are seeing that the existing nurse triage service can have value beyond saving medical costs.

That was the case for Ray Hansen, safety director for South Weber, Utah-based Sure Steel Inc., which employs about 200 people.

Sure Steel has had a Medcor nurse triage phone service for worker injuries for nearly three years — part of the benefit package offered by his insurance company, he said. The steel erector company has had few worker injuries in the past three years, but the company and employees have been happy with the results from its phone calls to the nurse, Mr. Hansen said.

But one call may have saved an employee's life, he said. It happened when a worker at a mine site in Nevada complained to his supervisor that he'd had pain in his neck radiating down his arm for three days but had refused to go to a doctor.

The supervisor put the worker, who spoke Spanish, on the triage phone line with a bilingual nurse. She convinced the man to go to a clinic near the mine, where he was helicoptered to a hospital.

"He underwent an emergency procedure for his heart," Mr. Hansen said. "He made a full recovery and returned to work. It all worked out beautifully."

ON-SITE HEALTH CLINICS PROLIFERATE AS EMPLOYERS SEEK COST SAVINGS

The number of on-site health centers is substantial and growing among large companies, national surveys show. All on-site clinics provide primary care to employees and initial treatment and referrals for injured workers, clinic operators say. They also offer employers the option of occupational health services.

Several surveys document the trend:

- Willis Towers Watson P.L.C. surveyed 678 U.S. employers with a total of 11.9 million employees for its "Best Practices in Health Care Employer Survey 2017" and found 20% have an on-site health clinic and another 4% may by 2019.
- The Washington-based National Business Group on Health surveyed 148 employers with a total of 10 million workers and found 54% had an on-site clinic in 2017 and another 12% expect to open one by 2020, according to its "2018 Large Employers' Health Care Strategy and Plan Design Survey." More than half of those clinics offer occupational health services.
- Results of a 2017 survey by the Alexandria, Virginia-based Society for Human Resource Management indicate that smaller employers are less likely to have on on-site clinic. Its 3,227 survey respondents included small businesses, nonprofits and government agencies. It found that 8% have on-site clinics, a figure that has held steady since 2013.

The uptick in interest in on-site clinics, at least for large companies, has been a boon for the businesses that operate on-site clinics for employers, experts say.

Among them are QuadMed L.L.C., based in Sussex, Wisconsin. QuadMed opened its first on-site clinic in 1991. Today, QuadMed operates on-site health centers at more than 100 companies in 23 states, said Liana Wayda, QuadMed's manager of strategic marketing.

"We've seen interest in on-site and near-site health centers steadily increasing," Ms. Wayda said. "But we've also seen a bit of a pause recently because of uncertainty over federal health care."

Charlotte, North Carolina-based Healthstat Inc., launched in 2001, operates about 300 on-site clinics for more than 100 public- and private-sector clients, typically with 500-plus employees, in 34 states, market development manager Melissa Parks said.

Marathon Health, based in Winooski, Vermont, began in 2005 and now runs 140 on-site health centers for 90 public- and private-sector employers nationwide, said a company spokeswoman. The majority have 500 to 5,000 employees. "At Marathon Health centers we always do triage and first treatment of injured workers," she said. "There are typically two motivations for having an on-site center. One is to drive down health care costs. The other is a genuine concern about the health of their employees and as a tool for attracting and maintaining talent."

Janet Lavelle

Generation gaps challenge safety

JOYCE FAMAKINWA
jfamakinwa@businessinsurance.com

Changing demographics and aging workforces may complicate employer efforts to create effective safety cultures.

Employers may have to use different methods to communicate about workplace safety to protect their multigenerational workforces, but they shouldn't get too caught up in stereotypes about the different generations, according to experts.

"It's something that affects every employer, but probably some employers to a greater degree than others depending on the industry," said John Dony, Itasca, Illinois-based director of the Campbell Institute and environmental, health, safety and sustainability at the National Safety Council. "For example, we see this in industries like manufacturing where the workforce tends to have aged in place with the work and you have a median age in some facilities that is creeping up into the mid to late 50s. The aging in place has begun to hit organizations hard."

Along with an aging workforce, there are multiple generations of workers that currently make up the U.S. workplace, including baby boomers, Generation X and millennials.

The 2008 economic downturn in the United States is one of the biggest contributing factors to why baby boomers who have passed retirement age continue to work, experts say.

"That downturn ended up impacting a lot of retirement plans, and as a result, a number of baby boomers that were set to retire decided to stay in the workforce and continue earning money so that when the markets rebounded they would be able to retire in comfort and maintain a quality of life," said Peter Sullivan, Houston-based manager in the plant practice of Accenture Asset and Operations Services at Accenture Consulting.

This generation of workers often has knowledge on how to run things safely due to their years of experience in the workplace, according to Mr. Sullivan. When this knowledge leaves with these workers upon retirement, experts say it becomes difficult for employers to reacquire it, creating a knowledge gap.

By 2025, it is projected that millennials will make up approximately 75% of the global workforce, which represents a significant population within the workforce, Mr. Sullivan said. Complicating the demographic shift is the retirement of the baby boomer generation, many of whom have been at their current employers for years, if not decades, he said.

"They have this profound sense of loyalty in how to run their business ... in how to do it safely that has often gone undocumented within policies, procedures, and training," Mr. Sullivan said. "As they are getting ready to retire and as they are walking out the door they are taking this knowledge with them."

These generations that occupy the workplace have different expectations when it comes to communication and employers must address this to establish an effective workplace safety culture. "There is some concern that what worked in engaging one generation to be attentive to safety might not work for another generation," said Mr. Dony.

"Full classes on safety will become a rarer occurrence because younger generations don't necessarily learn best that way," said Christina Lincicome, Salem, Oregon-based director, diversity, and inclusion, at SAIF Corp., Oregon's state-chartered workers comp insurer.

One of the ways that employers can address this is by using eLearning and micro-learning methods for safety training, said Ms. Lincicome. Employers need to understand that "from a generational perspective there are differences in how to deliver information. For example, millennials are highly intuitive. Safety concerns should be relayed showing the best methods quickly and decisively. For boomers, you want to include the entire method and build in time for questions. Both groups need a clear understanding of 'the why' in the safety approach," she said.

"They are focused on the effect of things and how that is going to impact things. If you want to make a change in the workplace, if we can illustrate to them how that is going to have an impact ... they are more willing to adapt to that workplace safety issue," said Tracey Cekada, Indiana, Pennsylvania-based associate professor, safety sciences department, at Indiana University of Pennsylvania.

Pairing generations together has been successful in addressing workplace safety.

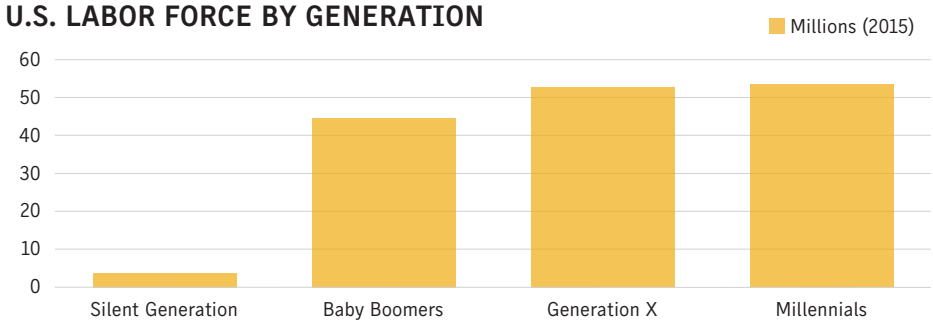
"Millennials bring intuitive problem-solving approaches while boomers carry the social and institutional knowledge. These two can create new approaches by leveraging the best in each other. Generation X is generally excellent at project management. They have been referred to as the latch-key generation and understand what it is like to work alone. They excel in productivity and creativity when you give them a charge, a deadline, and leave them alone," said Ms. Lincicome.

Considering what works best for different workers is important when employers decide how to address safety issues but experts say employers should move beyond stereotypes.

"The concerns can't be divorced from that when a new employee walks into the workforce, whether they are 25, 45, or 65, they are still going to need to learn a lot about the risks and what's in front of them," said Mr. Dony.

"I don't think there is that much of a difference as many people would assume," he said. "I think that ultimately engaging people about safety is about getting to their heart, as well as their brain, and making them understand the value of why you are trying to keep them safe and what you are trying to do. There are a lot of organizations that have done a lot with gamifying safety and making people feel like they are making incremental improvement toward something. I think that this works for any generation."

U.S. LABOR FORCE BY GENERATION



Source: Pew Research Center, 2015

TRAINING BY GENERATION

SILENT GENERATION

BORN: 1928 – 1945

This generation of workers prefers training in a structured classroom environment. They learn based on studying and memorization, according to a report called "Training a Multigenerational Workforce, Understanding Key Needs & Learning Styles" by Tracey Cekada, Indiana, Pennsylvania-based associate professor, safety sciences department at Indiana University of Pennsylvania.

"They were very self-sacrificing, loyal, and committed to their company," Ms. Cekada said.

BABY BOOMERS

BORN: 1946 – 1964

This generation of workers prefers the lecture and workshop environment while using case studies to learn.

"They struggle with change, but they realize that it has to happen. I think it's just harder for them to adapt to changes and make those changes," said Ms. Cekada.

GENERATION X

BORN: 1965 – 1980

This generation prefers fun learning environments where they can explore. They learn with hands-on activities including games and role playing.

"They learned to be independent and adapt to changes," said Ms. Cekada.

MILLENNIALS

BORN: 1981 – 1997

This generation prefers a digital learning environment where they can utilize their technological literacy.

"They are different in that they have that access to technology. They love change and like to multitask. They are very focused on the effect of things and how that will impact things," said Ms. Cekada.

BUSINESS INSURANCE®

WORLD CAPTIVE FORUM

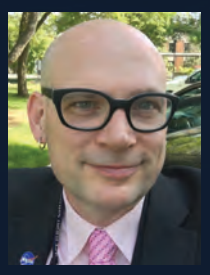
JANUARY 31 - FEBRUARY 2, 2018

FORT LAUDERDALE MARRIOTT HARBOR BEACH RESORT & SPA, FLORIDA

Celebrating its 27TH year, the **2018 World Captive Forum** will address new and emerging risks facing companies and organizations worldwide, demonstrating how captives can offer solutions that may not be available in the traditional insurance marketplace. A domicile-neutral conference, the **World Captive Forum** provides in-depth, high-caliber educational content to risk managers, benefit managers and financial executives whose organizations have risks insured by a captive or who are exploring the formation of one. Educational content will be presented on three separate tracks: General, Property/Casualty and Benefits.

SESSION HIGHLIGHTS:

- Captives 201: The Fundamentals and Recent Developments (Pre-conference Workshop)
- Brexit, BEPS and Other International Regulations
- Global Employee Benefit Programs: Are They Still Worth It?
- Medical Stop-Loss: Structuring the Risks
- Pooling in Microcaptives
- Reinsurance in the Aftermath: Impact of 2017 Storms and Quakes
- Growing Your Captive with Voluntary Benefits
- Multiple Captives — Why and How?
- Cell Company Overview and Innovative Applications
- The World of RRGs (Risk Retention Groups)



OPENING KEYNOTE

SPACE WEATHER: ITS IMPACT ON OUR TECHNOLOGICAL WORLD

Dr. C. Alex Young
NASA Heliophysicist

SPONSORSHIP INFORMATION

Jeremy Campbell | Head of Sales | Events & Workers Compensation Magazine
jcampbell@businessinsurance.com | 513-737-4063

SPONSORS

DIAMOND

R&Q

Willis Towers Watson

GOLD

BDA Bermuda Business Development Agency

GENERALI Employee Benefits Network

SILVER

MARSH

Maxis Global Benefits Network

75 years SAFETY NATIONAL Since 1942

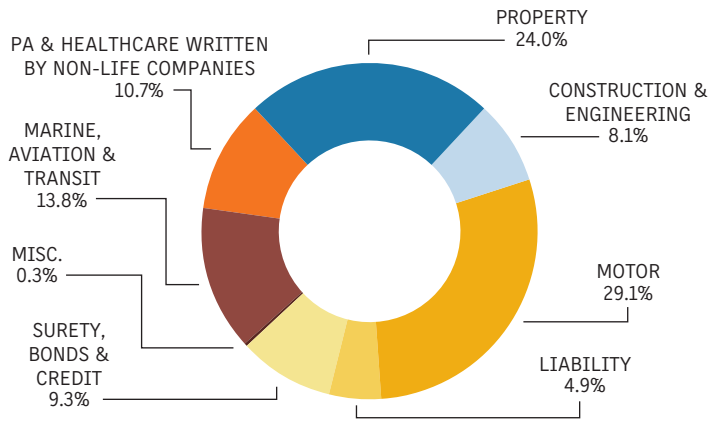
REGISTER, VIEW FULL AGENDA & MORE:
businessinsurance.com/conference/wcf

PROFILE: ECUADOR

52
GLOBAL P/C MARKET RANKING

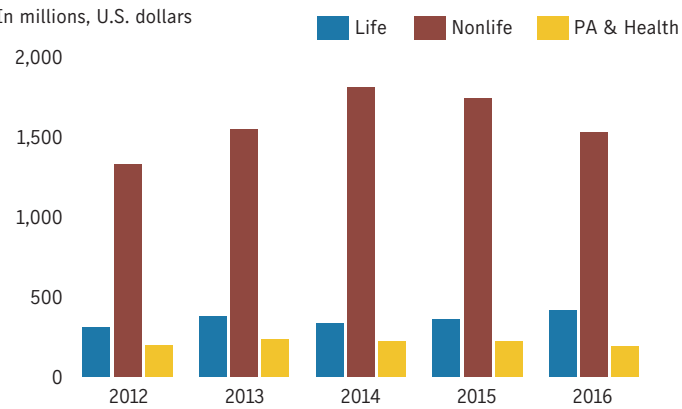
Ecuador is a low-income developing country and one of the poorest in Latin America. It has considerable oil reserves and other natural resources, however, which helped it fund generous social programs during the past decade. Although Ecuador has a long history of earthquakes and volcanic eruptions, damage from these events had not caused major losses for insurers until the earthquake of April 2016, which resulted in around half a billion dollars in claims payouts and led to temporary tax measures to raise funds. There were 34 national insurers and one national reinsurer listed by the regulator as active in the market in August 2017.

MARKET SHARE



MARKET GROWTH

In millions, U.S. dollars



Source: Axco Global Statistics/Industry Associations and Regulatory Bodies

AREA
105,037
square miles

POPULATION
16.5
million

MARKET CONCENTRATION
51.6%
market share of top five insurers

2017 GDP CHANGE (PROJECTED)
1.02%

MARKET DEVELOPMENTS

Updated September 2017

- A magnitude-7.8 earthquake on April 16, 2016, was felt throughout the country, with more than 1,500 aftershocks running into May. At least 675 people were killed, and economic losses were estimated at $3.3 billion. The national insurance association FEDESEG estimates about $422 million has been paid out in claim settlements, with a final total of $575 million expected.
- Former President Rafael Correa, who served three terms until Lenin Moreno won the post in April 2017, announced temporary tax changes in response to the disaster, including an increase for a year of the value-added tax rate by 2% (it returned to 12% in June 2017) and a one-off contribution by companies of 3% of profits for the 2015 fiscal year.
- Despite losses from the 2016 quake, any slowing of rate reductions in property lines was only momentary. Overall property/casualty premiums contracted by 11.9% in 2016, and the market continued to be very soft in most lines supported by abundant reinsurance capacity at competitive rates.
- Under Financial Junta Resolution No. 223-2016-S of March 11, 2016, companies were given a further period of 18 months from March 2016 to comply with changes to the insurance law, including those increasing capital requirements. By mid-2017 two small insurers had ceased operating rather than attempt to meet the minimum requirements, while one of two local reinsurers had merged with an insurer with which it had common shareholders.
- In mid-2017, the Ecuadorean operations of American International Group Inc. and Assicurazioni Generali S.p.A. were widely rumored to be up for sale, or open to possible merger with local companies.

COMPULSORY INSURANCE

- State-run workers compensation
- Marine cargo for imports
- Aviation passenger liability
- Fire insurance for condominiums
- Auto personal accident coverage

NONADMITTED

Nonadmitted insurance is not permitted in Ecuador because the law provides that insurance must be purchased from local authorized insurers with a few exceptions, which include property owned abroad and liabilities that may be incurred overseas.

INTERMEDIARIES

Intermediaries must be authorized to transact insurance business and are not allowed to place business with nonadmitted insurers, except where express permission has been granted by the regulator. Brokers involved in nonadmitted placements do not have to warn buyers that their insurer is not subject to local supervision.

MARKET PRACTICE

Despite the clear provisions of the insurance law, there is said to be some abuse of the nonadmitted regulations, and business is placed abroad, more in the life and health classes than in the property/casualty classes. Fronting may be used as a way around the nonadmitted issue for large risks.

Information provided by Axco Insurance Information Services.
www.axcoinfo.com

Celebrate 45 outstanding women in insurance!

Women to Watch Awards & Leadership Conference EMEA 2017 NEW!
November 16-17, 2017
Sheraton Grand London Park Lane, UK

12th Annual Women to Watch Awards & Leadership Conference 2017
December 14-15, 2017
Grand Hyatt New York

SPONSORS | NEW YORK EVENT

PLATINUM

CLYDE&CO

GOLD

AIG

sedgwick
caring counts

ZURICH

SILVER

Alliant CNA MARSH

RSG RYAN SPECIALTY GROUP

75 years SAFETY NATIONAL Since 1942

XL CATLIN

SPONSORS | LONDON EVENT

GOLD

AIG

SILVER

MARSH

REGISTER NOW
TO ATTEND THESE INSPIRING LIVE EVENTS

Join ***Business Insurance*** **& CLM** for the **Women to Watch Awards & Leadership Conferences**. This year, the program has been expanded to two events: **London** and **New York**. Winners based in Europe, Middle East and Africa will be honored at the inaugural London event. Winners based in North America and other countries outside EMEA will be honored at the flagship event in New York.

Come to network, learn and be inspired at these events that celebrate women in the commercial insurance industry and other related fields who are successfully driving the industry forward.

NEW YORK
AWARDS
KEYNOTE

Ashley Judd
Feminist +
Social Justice
Humanitarian

LONDON
OPENING
KEYNOTE

Carolina Klint
CEO North West Region,
Continental Europe
Marsh

REGISTRATION, AGENDA, HONOREES & MORE:

LONDON EVENT:
businessinsurance.com/conference/WomentoWatchEMEA

NEW YORK EVENT:
businessinsurance.com/conference/WomentoWatch

#BICLM_Women

BUSINESS INSURANCE + CLM

WOMEN TO WATCH

SPONSORSHIP OPPORTUNITIES: Jeremy Campbell | jcampbell@businessinsurance.com

LEGAL BRIEFS

Aon Consulting sues Marsh units over data access

■ Aon Consulting Inc. filed a federal lawsuit against Marsh Inc. and Marsh & McLennan Agency L.L.C. charging the companies improperly gained access to a secure Aon website to obtain survey reports and data and used the information to provide compensation consulting services to their customers.

The complaint, filed in U.S. District Court for Northern Illinois based in Chicago, seeks a jury trial and charges Marsh and Marsh & McLennan Agency with "misappropriation of trade secrets, deceptive trade practices, unfair competition and tortious interference with a prospective economic advantage."

Aon, through its San Jose, California-based Radford business unit, offers compensation data surveys to its customers, the complaint said. The survey data is obtained from about 3,000 participating organizations, which provide compensation data to Aon in exchange for having access to Aon's survey reports and data through a secure website that requires a username and password issued by Aon, the complaint said.

Marsh and Marsh & McLennan Agency are competitors of Aon that offer, in part, compensation consulting services through their business unit, San Diego-based Barney & Barney Insurance Services. Aon alleges that the rival companies improperly gained access to Aon's secure website by using a participating organization's username and password and then downloaded Aon's survey reports and used the information to provide compensation consulting services to their customers, the complaint said.

"As a result of defendants' actions, Aon has suffered irreparable injury and seeks damages, a permanent injunction, costs and attorneys' fees as authorized by the applicable federal and state laws," the complaint said.

AIG sues Disney to avoid claim over 'pink slime'

■ American International Group Inc. last month sued Walt Disney Co. to avoid having to reimburse the parent of ABC News for part of a settlement of a meat producer's defamation lawsuit over a product that critics call "pink slime."

In a complaint filed in a New York state court in Manhattan, AIG Specialty Insurance Co. urged a judge to reject Disney's $25 million reimbursement demand, related to its larger June 28 settlement with Beef Products Inc., under an insurance policy that excluded coverage for claims alleging malice.

The lawsuit stemmed from BPI's lawsuit against ABC and reporter Jim Avila over reports in March and April 2012. According to the privately held South Dakota company, the reports falsely implied that BPI's "lean, finely textured beef" was not safe, nutritious or even meat.

AIG said in its lawsuit that Disney's policy covered some defamation claims, but only if the company had first found an outside lawyer to say the statements it planned to broadcast were acceptable.

The New York-based insurer accused Disney of trying to "create coverage where none exists."

AIG filed its lawsuit nine days after Burbank, California-based Disney sued the insurer in Los Angeles federal court, seeking to send the dispute into arbitration.

In an Aug. 8 regulatory filing, Disney said it had incurred $177 million of costs, in addition to what insurance covered, to settle litigation during the second quarter.

BPI had said ABC's reports forced it to close plants and lay off several hundred workers. It had sought $1.9 billion of damages, which could have been tripled to $5.7 billion under a South Dakota "food products disparagement" law.

The New York case is *AIG Specialty Insurance Co. v American Broadcasting Companies Inc. et al.* The Los Angeles case is *Walt Disney Co. v. AIG Specialty Insurance Co.*

Reuters

Dismissal upheld in Marsh employee's claim against AIG

■ A federal appeals court upheld dismissal of breach of contract and bad faith claims against an American International Group Inc. unit in a case involving a Marsh USA Inc. employee who was involved in an automobile accident.

The long-running case involves a former salesperson in Marsh USA's Los Angeles office, Judy Bamberger, who was required to use her personal vehicle for business travel and was reimbursed by Marsh USA for her mileage. In 2010, Ms. Bamberger, who planned to stop on her way home for personal errands, hit a motorcyclist, who sued Ms. Bamberger and Marsh USA.

In addition to two insurance policies Ms. Bamberger had personally purchased, she had coverage as an additional insured under a business auto policy issued by AIG unit National Union Fire Insurance Co. to Marsh USA, according to court papers in *Judy Bamberger v. Marsh USA Inc. et al. and National Union Fire Insurance Co.*

In 2012, she settled all claims against her for $1.25 million, which was primarily covered by her personal insurance, except for a $150,000 gap that existed between her personal and excess policies that she agreed to personally pay, according to court papers. Ms. Bamberger filed suit against Marsh USA and National Union in May 2014 charging the insurer with breach of contract and breach of duty of good faith and fair dealing.

Marsh USA reimbursed Ms. Bamberger for her out-of-pocket expenses in the litigation, and the two parties resolved their dispute. In 2014, AIG reimbursed Ms. Bamberger $156,000, reflecting the $150,000 plus interest.

The District Court dismissed her claims against the insurer, which a three-judge appeals court panel unanimously upheld.

Appeals court rules New York comp law constitutional

■ The New York Court of Appeals found constitutional a 2013 amendment to the state's workers compensation law closing the statewide fund for cases that are reopened, ruling against 20 insurers that long held that the amendment created a collective of unfunded liabilities between $1.1 billion and $1.6 billion.

The insurers filed their original lawsuit in July 2013, claiming that the amendment — known as The Business Relief Act — served no legitimate purpose and would result in an enormous financial burden on private insurers, self-insureds and a nonprofit carrier for state employees.

The state created its Fund for Reopened Cases in 1933 to help employers and insurers pay for workers compensation claims that are reopened after a minimum of seven years following the injury and a minimum of three years since the last payment. The fund, which was paid for with special fees collected from business owners by their insurer, was closed per the amendment because costs increased dramatically.

DOCKET

WILLIS TOWERS WATSON, AON SETTLE CFO HIRING DISPUTE

Willis Towers Watson P.L.C. resolved a dispute with rival brokerage Aon P.L.C. regarding the hiring of Michael J. Burwell as its new chief financial officer. Terms of the settlement agreement are confidential. Lawsuits pending in the federal courts in Michigan and Illinois were dismissed, the brokerage said. Aon had alleged Mr. Burwell had knowledge of Aon's trade secrets from when he worked with Aon as a consultant at PricewaterhouseCoopers L.L.P. and breached his fiduciary duty to Aon by taking on his new post.

CHUBB UNIT PREVAILS IN COVERAGE DISPUTE WITH BANK

A federal appeals court upheld a lower court ruling that found a unit of Chubb Ltd. did not have to cover BancorpSouth Inc. for a $24.6 million settlement of class claims where the bank was charged with collecting excessive overdraft fees.

In *BancorpSouth v. Federal Insurance Co.*, the 7th U.S. Circuit Court of Appeals in Chicago agreed with a ruling by the U.S. District Court in Indianapolis that found Chubb subsidiary Federal Insurance Co. had no duty to defend or indemnify Tupelo, Mississippi-based BancorpSouth because overdraft fees were excluded.

LAWSUIT OVER FLUSHABLE WIPES REVIVED

A federal appeals court reinstated a putative class action lawsuit filed by a consumer who alleges Kimberly-Clark Corp.'s flushable wipes are not, in fact, flushable. Jennifer Davidson filed suit against Irving, Texas-based Kimberly-Clark alleging that its wipes, which promise to be flushable, were not "truly flushable" because they failed to "disperse and disintegrate within seconds or minutes." The U.S. District Court in Oakland, California, dismissed the case, but a unanimous three-judge appeals court panel reinstated the case with a majority opinion plus an affirming opinion.

John Hahn is CEO of EPIC Insurance Brokers & Consultants, a San Francisco-based retail brokerage owned by private-equity investor Oak Hill Capital Partners, which bought EPIC in July. One of the founders of Tri-City Brokerage Inc., Mr. Hahn started on the wholesale side of the brokerage business. In 2007, a few years after Tri-City was sold, he founded EPIC with Dan Francis, a former executive at ABD Insurance & Financial Services Inc. The firm has grown substantially over the past 10 years and was ranked the 17th-largest brokerage of U.S. business in *Business Insurance*'s most recent ranking with about $250 million in 2016 brokerage revenue. EPIC earlier this year bought the retail operations of The Capacity Group of Cos. and recently announced plans to buy Frenkel & Co. Mr. Hahn spoke with *Business Insurance* Editor Gavin Souter about EPIC's growth strategy. Edited excerpts follow.

John Hahn

EPIC

Q You added about 25% in revenue in 2016, and you've been growing in 2017 through acquisitions. What's been driving that?

A It's a combination of acquisitions, producer recruiting and team recruiting. The Capacity deal gave us a specific platform in the Northeast, which was high on our to-do list. It also brought us some focus in and around the transportation space, which is of great interest for us. Historical loss ratios over the last few years have not been good, so we're seeing a fair amount of rate increase in that space. We think that's going to last for a while, so we want to be able participate on a bigger scale and be able to bring to our clients both loss mitigation and risk control capabilities.

Q What will the Frenkel acquisition bring to EPIC?

A Strategically it's a terrific fit. It brings us a central, large New York City presence and a presence in some surrounding locations, such as Boston, that we've had our eye on for a while, and it brings us an upper-midmarket capability that fits right in with the core value of EPIC. It's a terrific platform to begin to recruit people in the New York/New Jersey area, and it brings us a really terrific employee benefits platform that, from an employee benefits perspective, takes us to over $100 million in revenue. And their marine team and private client practice are just great fits and complementary add-ons for us. Then in some areas where they don't have expertise and we do, we think there's an opportunity to strategically expand their playing field by bringing in some construction talent and developing a construction practice in the Northeast, which currently they don't have and is probably our biggest industry segment nationally.

Q How do you differ from other private equity-owned brokerages?

A We're not in the velocity game of acquisitions. We're not looking to do five-to-10 acquisitions a quarter. We're not looking to just roll up revenue. Every deal we do, we want to be consistent with either business segments, specialty niches we already have established or it's going to establish a new niche for us or a new industry specialty that we want to be able to mobilize behind. Or we're going to get some geographic expansion that we think is important. We think they need to fit culturally as well as operationally and strategically, and it's hard to find a lot of firms checking off all of those boxes.

We're willing to spend a lot of time in advance of the deal socializing with whoever the operators and owners are to make sure it would be a good fit for us and for them. When we get it right, we know that we've got a winning edge, and we know that there will be very little risk around integration.

Q&A

Our investors' belief is that our above-market and above-industry organic growth is the driver of value for us, so everything we do is looking to make sure that we can maintain organic growth at 7% to 8%, which is two to three times the industry average, and also to be strategically connected with our clients in a way that our client retention levels and revenue retention levels are best in class.

Q How do you achieve that organic growth rate?

A We infuse capital and intellectual capital into each of our acquisitions to help them bring on talent, and that talent adds to what they've already been doing. We'll invest as well in client resources and deliverables, so we bring a real risk management-like approach into the middle and upper-middle market in both property/casualty and employee benefits, which most of our competitors don't really do.

We're bringing long-term value to clients, whether it's loss control or the claims side or the claims advocacy side. That will drive the stickiness, but it also leads us to new client engagements, and we have a very aggressive producer model that also really facilitates our producers being owners in the business. We have around 200 employee-owners out of 1,000 people, so they wake up differently every day, we believe, and they're going to build value with us, and they're able to earn equity and purchase equity. We see our producers are out trying to earn as much as they possibly can to be equity participants in our business.

Q Where are you looking to grow in the future?

A Our main growth over the next two to three years will be in and around the established regions we have, which are Northern and Southern California, the Southwest out of Texas, Southeast out of Atlanta, our Northeast platform, and up and down the East Coast and mid-Atlantic. Secondarily, we've invested a lot of money in our employee benefits business. We built a centralized consulting service model, and it's really where clients' pain is most acute, so we'll continue to put firepower behind our employee benefits business.

And then the goal for us in our specialty business is that we'd like that to be 40% or so of our business in the next couple of years (currently it's about 30%), so we have designs on building out our current industry national practices, adding to the national practices we have and growing our program and products portfolio as well.

Q What will EPIC look like in three to five years?

A Our hope is that we'll have each of our regional platforms in and around $100 million in revenue or more, so by definition the company would be about twice the size — so somewhere around $600 million in revenue by then. If the business could look 40% specialty, 30% employee benefits and 30% commercial property/casualty, I think that would be a solid mix for us.

The goal from there would be to continue to stay private — we like the private equity model, we understand it — find a new sponsor in five years and look to take the company from $600 million at that stage, or whatever we are, to $1 billion. And at that stage, I think we'd have the scale to be relevant in more ways.

Every deal we do, we want to be consistent with either business segments, specialty niches we already have established or it's going to establish a new niche for us or a new industry specialty that we want to be able to mobilize behind.

CYBER SECURITY 2017

BUSINESS INSURANCE®

Cyber breaches like the ones Equifax Inc. and Yahoo Inc. have experienced are not unique to big and high-profile companies. Smaller and lesser known companies may not garner as much media attention, but they are also subject to cyber attacks that results in quantifiable losses.

XL CATLIN

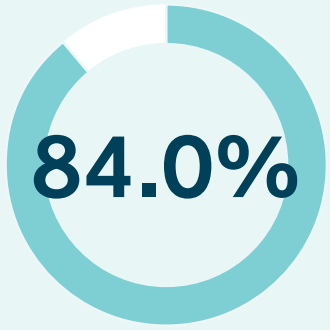
BUSINESS INSURANCE®

CYBER SECURITY 2017

In August 2017, *Business Insurance* conducted an online survey of its subscribers with the objective of understanding how companies are preparing for the increased threats to cyber security and how they are protecting themselves and controlling the costs of such attacks.

This report is based on the responses of 322 risk managers and commercial insurance buyers who are familiar with and actively participated in cyber risk management/insurance decisions/programs in their companies. An additional section of the report is based on 852 insurers and insurance brokers — nonbuyers — who are familiar with any type of cyber protection their company may offer. The base used is total answering each question.

GREATEST CONCERNS



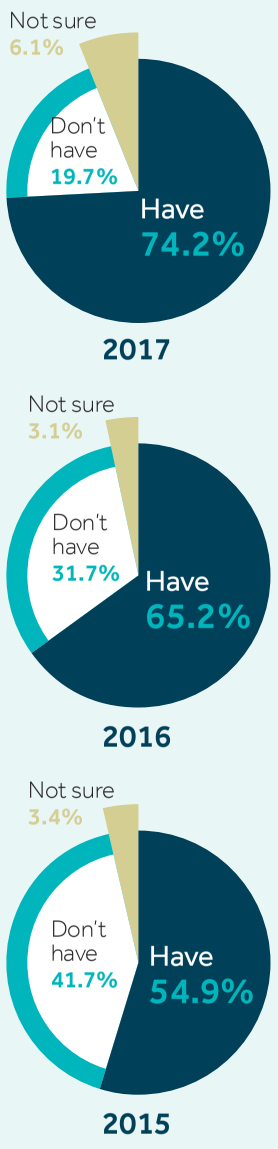
Hackers that penetrate systems

51.0%
Operational risks or natural disasters

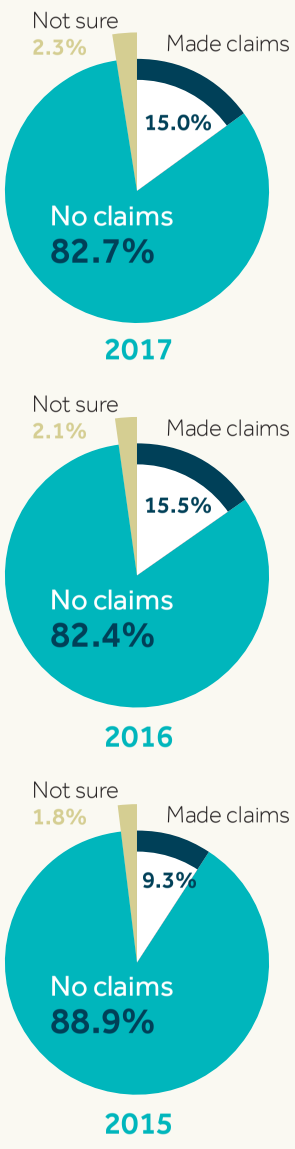
50.2%
Employees manipulating data or systems undetected

CYBER INSURANCE — UPTAKE + CLAIMS

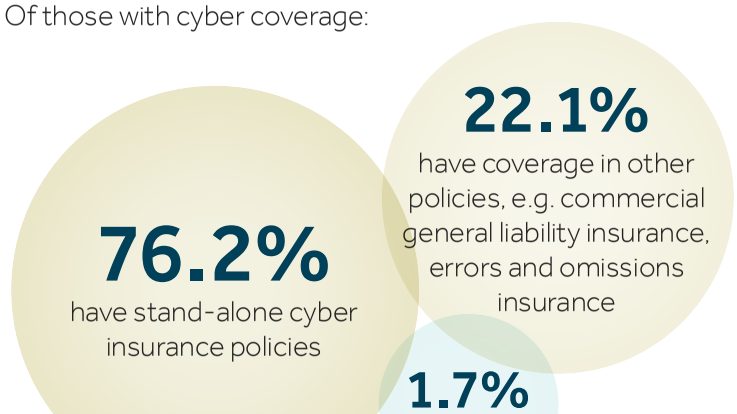
CYBER COVERAGE



CYBER CLAIMS



Of those with cyber coverage:



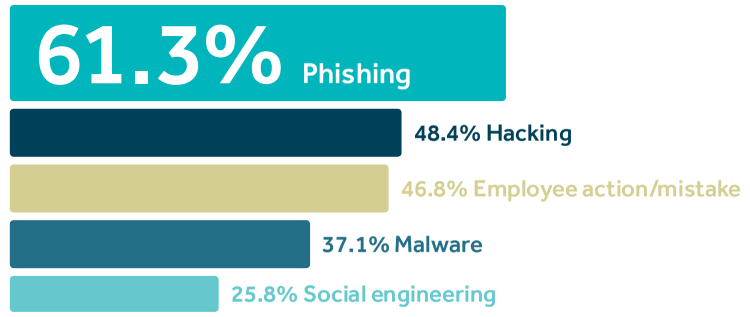
CYBER POLICY PREMIUMS

The average premium on the stand-alone cyber insurance policies is **$188,250** with an average limit of **$12.7 MILLION**.

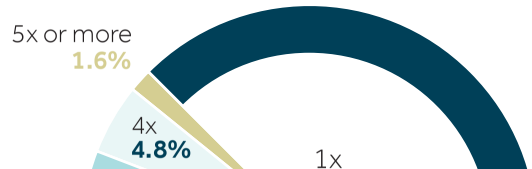
Less than $10,000	7.6%
$10,000-$19,999	8.4%
$20,000-$29,999	9.2%
$30,000-$39,999	7.6%
$40,000-$49,999	5.3%
$50,000-$74,999	11.5%
$75,000-$99,999	7.6%
$100,000-$199,999	6.9%
$200,000-$299,999	6.1%
$300,000-$399,999	2.3%
$400,000-$499,999	3.8%
$500,000-$749,999	1.5%
$750,000-$999,999	0.8%
$1 million and more	3.1%
Don't know	6.1%
Prefer not to answer	12.2%

CYBER BREACHES

The **TOP FIVE** most common type of breaches are:



The average number of times of those who experienced a breach the past year is **1.8 TIMES**.



22.6%
Terrorists penetrating system to destroy information

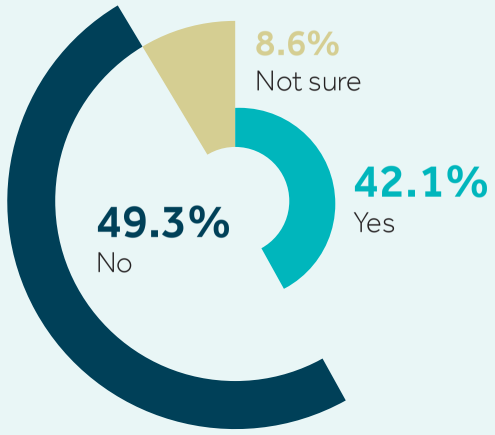
18.5%
Employees or other authorized users stealing trade secrets

11.5%
Competitors penetrating systems to commit corporate espionage

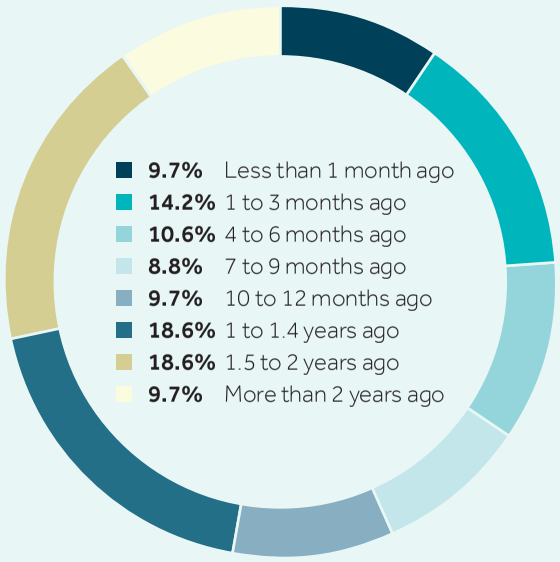
4.9%
Other

2.5%
None of the above

Percentage of those who experienced cyber breach in the past five years



Of those who experienced breach, **53.1%** said they experienced it less than a year ago. The average time frame of those breaches was **14.1 MONTHS AGO**.

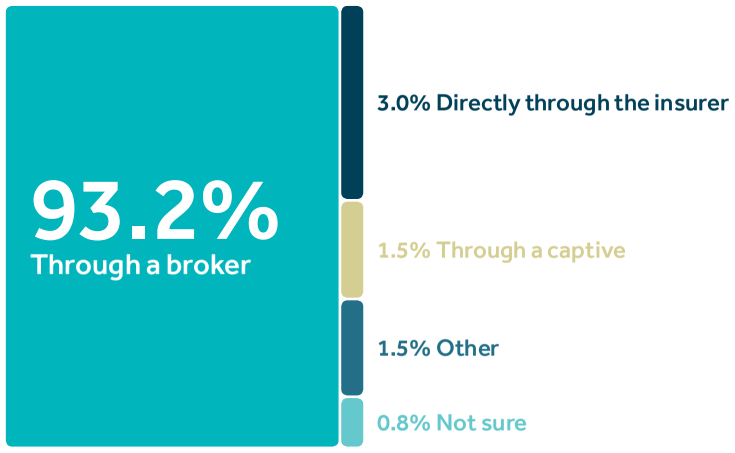


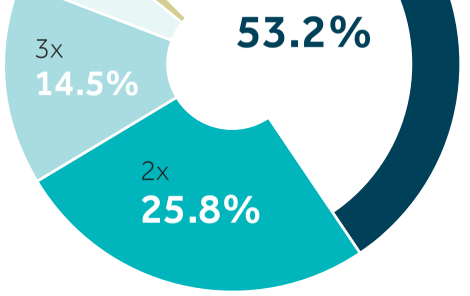
AGE OF CYBER POLICIES

TWO-THIRDS of companies first purchased cyber coverage less than five years ago, with an average age of their cyber insurance policies of **4.2 YEARS**. More than half of insurers, brokers and related service providers began offering cyber products to clients in the past five years.

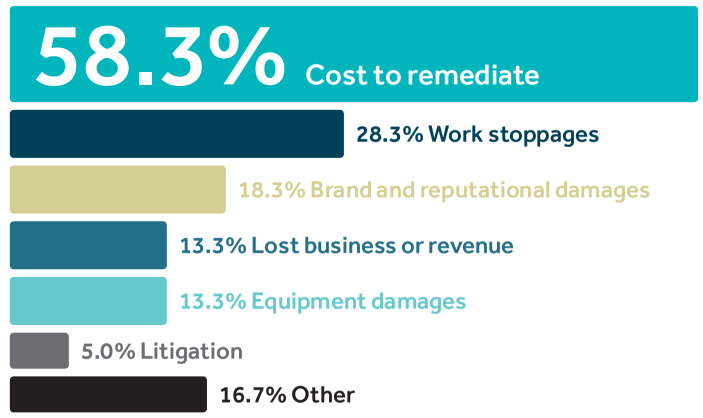
	BUYERS	NONBUYERS
2017	**11.7%**	**8.7%**
2016	**17.8%**	**14.9%**
2015	**20.6%**	**15.9%**
2014	8.9%	8.1%
2013	6.7%	5.7%
2012	5.0%	2.2%
2011	0.6%	2.6%
Before 2011	20.0%	15.7%
Not Sure	8.9%	26.1%

Most companies purchase their stand-alone cyber insurance policies through a broker.

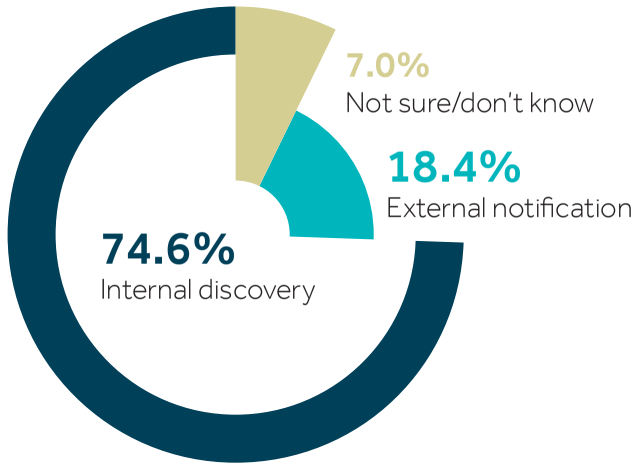




40.9 PERCENT of breaches in the past year resulted in quantifiable losses. Other damages include:



Almost **THREE-QUARTERS** of the breaches were discovered internally.



XL CATLIN

XL CATLIN

ANYONE CONCERNED ABOUT THE THREAT OF CYBER RISK, LET'S TALK.

And there's good reason to be concerned. Cyber attacks cost companies, on average, $4 million. XL Catlin can put some firepower behind your firewall. Talk with us about our unique coverage plus preventive and response services.

But maybe use an encrypted email.

MAKE YOUR WORLD GO

xlcatlin.com

"Highest Customer Satisfaction among Large Commercial Insurers"

XL Catlin received the highest numerical score among 11 insurers in the J.D. Power 2016 Large Commercial Insurance Study, based on 1,484 total responses, measuring the opinions of risk professionals in the U.S. and Canada with commercial insurers, surveyed April-July 2016. Your experiences may vary. Visit jdpower.com.

Cyber insurance comes of age

BY JUDY GREENWALD
jgreenwald@businessinsurance.com

Cyber insurance is expanding and shifting its focus.

Where once the primary emphasis was on privacy protection, there is now increasing attention being paid to business interruption, contingent business interruption — for disruptions caused by vendors — internet-caused property damage and cyber crime policies, experts say.

Observers describe the market as competitive, with some 70 insurers offering the coverage. Policyholders are generally satisfied with the limits they are getting, albeit some say there is a risk-reward equation to be considered as higher limits become costlier (see story page 26). Meanwhile, the Equifax Inc. data breach could have some long-time implications for the industry (see story page 27).

"It's a good time to be a buyer of cyber insurance, between the broadening coverage in the policy form and the competitive pricing," said Robert Horn, associate director at Crystal & Company in New York.

The cyber insurance market is "robust and growing, and it's growing in a way that probably no one foresaw five, six years ago," when "everyone was very much fixated on privacy breaches," said Bob Parisi, New York-based cyber product leader at

See **CYBER MARKET** next page

INSIDE

Cyber buyers weigh costs and benefits

Policyholders are generally getting the cyber insurance limits they want as they conduct analyses to decide whether more expensive, higher limits are worth their additional cost.

Experts say that, in general, there is about $600 million in capacity available for individual cyber risks. "I haven't seen anyone walk away saying, 'If only I could buy another $100 million,'" said Bob Parisi, New York-based cyber product leader for Marsh L.L.C.

"I think clients are able to buy as much as they want or are willing to spend, given their budget, with few exceptions," he said.

"The highest cyber tower that I have credible information on is $700 million," said Michael Born, Kansas City, Missouri-based vice president of the global technology and privacy practice at Lockton Cos. L.L.C., although he added he has heard rumors of even larger limits.

Cost can be a barrier, however, Mr. Born said. "There are more carriers out there willing to write more limits," but their cost is prohibitive, he said.

"You see the buying community deciding whether the trade-off makes sense, given the attachment to which the potential loss might hit, and you have to weigh that against your balance sheet," said Adam Cottini, managing director of insurance and risk management in North America at Arthur J. Gallagher & Co. in New York.

No one is coming into the market with a blank check saying, "Get me every available limit you can and I'll buy," Mr. Parisi said. They usually have an "X" amount of dollars they are willing to spend, he said.

The available capacity will grow, said Joe DePaul, New York-based cyber/errors and omissions practice leader for Willis Towers Watson P.L.C. "As the market continues to expand and new entrants come in, I think that will increase significantly, frankly, over the next year."

Judy Greenwald

CYBER MARKET

Continued from previous page

Marsh L.L.C.

"No one was paying attention" then to issues including operational risks, the disruptions cyber problems can cause in business, or the property issues cyber can create, he said.

While the market was responsive to the issue of privacy breaches, "there was a misconception among other sectors, such as manufacturing, that they did not have cyber risks. And even if they did, the cyber insurance market was not responsive to their needs," Mr. Parisi said.

Observers say the now-broadened offerings include coverage for systems failures, which can be triggered not only by a breach but by any factor, including human error or a technical glitch.

The cyber insurance markets are starting to provide business interruption and contingent business interruption with limits in the "hundreds of millions of dollars," Mr. Parisi said.

Insurers are "continuing to build out how cyber is interacting" with other policies, including kidnap and ransomware, general liability and product liability policies, said Joe DePaul, New York-based cyber/errors and omissions practice leader for Willis Towers Watson P.L.C.

They are starting to offer difference-in-conditions and difference-in-limits polices for cyber coverage that could fit as umbrella coverage over policies including property, kidnap and ransom and potentially even directors and officers liability, said Florence Levy, Denver-based senior vice president for cyber/E&O with JLT Specialty USA, a division of Jardine Lloyd Thompson Group P.L.C.

"What we're seeing is coverage pushing out in every direction," said Nicholas Economidis, Philadelphia-based underwriter of professional liability and specialty lines at Beazley P.L.C.

American International Group Inc., for instance, is moving toward explicit coverage for both physical and nonphysical cyber-related risks in its policies. The premium charged will be based on the risk, the threat environment and the potential business impact, according to a market source.

"Essentially, this is still a young but maturing market," said Tim Marlin, Alexandria, Virginia-based senior managing director and head of cyber and professional liability underwriting at Hartford Financial Services Group Inc. "Given the fluid nature of cyber risk and the fluid nature of the threats, the industry is staying close" to emerging trends, including the move toward property-related and business interruption coverages, as well as the addition of explicit cyber extortion wordings in policies, he said.

Adam Cottini, managing director of insurance and risk management in North America at Arthur J. Gallagher & Co. in New York, said policyholders must coordinate their policy portfolios to see what is covered, how coverage is triggered and what mechanisms are in place to respond to first-party property damage and loss of data.

Competition is strong, though. "At this very moment I would describe the market as still relatively soft," said Michael Born, Kansas City, Missouri-based vice president of the global technology and privacy practice at Lockton Cos. L.L.C.

Insurers that have traditionally put sublimits on certain coverage are now offering full limits, he said, and many are offering full retroactive coverage instead of limiting the coverage date to when the policy was first purchased.

In the meantime, "organizations that can really demonstrate" they have cyber security controls and hygiene are experiencing slight decreases in rates, while most primary and excess polices are experiencing flat to single-digit increases, said Mr. DePaul.

Mr. Cottini said the market can be divided into segments based upon size. The market is fairly competitive for businesses with less than $250 million in annual revenue. For those with more revenue, while the competition is still robust, it is "definitely not as competitive as that lower tranche of business" because larger companies, with their greater amount of data, have larger potential losses, he said.

However, Ms. Levy said that while the market is "relatively robust from a capacity standpoint," the pool of markets "greatly shrinks" when it comes to insurers that write primary coverage for large, complex customers. She also said underwriters are "beginning to be a little more critical and scrutinizing the underwriting process." They are "going to be very focused on managing their aggregation limits," including cases where there may be aggregation from additional lines of business from a cyber event, she said, pointing to "silent cyber," which are noncyber policies indirectly impacted by a cyber event.

Also, while rates have been "probably still flat" the past year or so, "if we have a couple more major breaches the pressure's going to be on premiums going up a little bit," said Steve Bridges, senior vice president of the cyber/E&O practice with JLT Specialty USA in Chicago.

Penetration into the market is growing, experts say.

"We're seeing much more interest from organizations that fall outside" of what can be called the "information holder" industries, including health care, financial institutions, retailers and hospitals, said Stephanie Snyder, Chicago-based senior vice president and national sales leader for cyber insurance with Aon P.L.C. These include the manufacturing, food/agriculture, life sciences and energy sectors.

The penetration rate among large, complex organizations is around the 80% mark, said Mr. DePaul, who estimated the overall penetration among all firms to be 25%. But among small and middle-market firms, "there's still quite an opportunity there," he said.

With recent incidents, though, "more organizations are exploring stand-alone cyber polices," said Jennifer Rothstein, senior director at Kroll Associates Inc. in New York.

"One of the nuances and benefits of cyber liability coverage is not just as a financial reimbursement tool," but in its ability to offer access to experts and risk management programs, she said.

EQUIFAX DATA BREACH COULD LEAD TO STRICTER UNDERWRITING

The Equifax Inc. data breach revealed in September may have long-term consequences for policyholders and the insurance industry.

Equifax said hackers had accessed personal information on up to 145.5 million of the firm's customers. Equifax carried cyber liability coverage, which market sources say was led by London-based Beazley P.L.C., and the breach will likely result in a limit loss for insurers and reinsurers, observers say.

As a result of the Equifax breach, "we will see heightened underwriting scrutiny on accounts, especially accounts that have large amounts of personal data," said Michael Born, Kansas City, Missouri-based vice president of the global technology and privacy practice at Lockton Cos. L.L.C. "Specifically, they will focus on patching protocols, because that seems to have been an issue in this case," he said.

In addition, he said, "We may see some slight lessening of capacity for some carriers." Some of the insurers that provided $10 million of capacity on the risk may have to pay that entire amount and could decide to pull back from the marketplace, he said.

The incident may ultimately prove to be a directors and officers liability issue, some observers say.

For instance, *Hampden Kuhns v. Equifax Inc. et al.*, a putative class action complaint, was filed against the company and its directors and officers in U.S. District Court in Atlanta on Sept. 8. The lawsuit charges the company failed to maintain adequate security measures, that its share price dropped after the breach's disclosure, and that company officers had sold stock before the firm revealed the breach.

Prior D&O lawsuits filed in response to data breaches "haven't been particularly successful," according to Kevin LaCroix, executive vice president of RT ProExec, a division of R-T Specialty L.L.C., in Beachwood, Ohio. The prospect of Equifax D&O litigation "does seem more favorable than some of the other lawsuits that have been filed," because it involves an element of alleged insider trading, a stock drop and a delay between the breach's discovery and its disclosure, he said.

"If a publicly traded company came into my office tomorrow and said, 'We just had a cyber event, can you help us evaluate managing this risk and what we should do?' I'm going to ask for both the D&O and cyber policy immediately. I'm going to want to tear into both of them," said policyholder attorney Duke F. Whalquist, a partner with Rutan & Tucker L.L.P. in Costa Mesa, California.

Judy Greenwald

Ransomware risks go mainstream

BY JUDY GREENWALD
jgreenwald@businessinsurance.com

Organizations are facing an unrelenting stream of ransomware attacks.

While not as widespread as the WannaCry, Petya and NotPetya ransomware attacks that struck earlier this year, the less-publicized attacks also are creating significant problems for companies, experts say.

And the availability of ransomware on the so-called dark web gives criminals easy access to programs that can be used to target organizations.

With the relatively small amounts generally demanded — usually in the form of bitcoin — it is often cheaper for companies that don't have backup files to pay the ransom than to spend potentially many thousands more restoring their systems, even though paying the ransom raises the troubling issue of abetting criminals or even terrorists.

When they pay, in most cases the victims receive the encryption key that restores their data.

Ransomware attacks have caused problems for organizations for several years, but the WannaCry attack in May and an attack using a new variant of Petya in June hit numerous companies, particularly in Europe, causing widespread concerns.

But smaller, less far-reaching attacks are also causing big problems for companies, and there is little sign of criminals relenting, said Richard May, Seattle-based managing principal for Integro Ltd. "I think it's unfortunately going to be more of the same," he said.

Ransomware is an effective business model for criminals because it involves little expense, experts say. It is "essentially a pure profit gain," said Alan Brill, senior managing director at Kroll Associates Inc. in Secaucus, New Jersey.

The only effective measures firms can generally take, observers say, is preventive, with frequent backups.

Insurance coverage for ransomware attacks is generally available in both cyber and kidnap and ransom

See **RANSOMWARE** next page

RANSOMWARE

Continued from previous page

policies (see related story).

"Ransomware does continue to grow as a problem, both in terms of the sheer volume and sophistication," said Tim Marlin, Alexandria, Virginia-based senior managing director and head of cyber and professional liability underwriting at Hartford Financial Services Group Inc.

He noted that criminals can now buy ransomware software on the dark web without even having to bother to develop it themselves.

While hard data on the issue is hard to find, "certainly the impact has increased," while its incidence is higher as well, increasing dramatically last year and perhaps accelerating even faster this year, said Thomas Fuhrman, Washington-based global leader of cyber security consulting and advisory services at Marsh Risk Consulting.

"We've seen a significant increase" in ransomware in the past 12 months, particularly in the small and medium-size enterprise and middle-market space, said Kimberly Horn, New York-based global focus group leader for Beazley P.L.C.'s breach response and information security claims. These small to midsize companies "don't necessarily have the same resources as Fortune 500 companies to invest" in data security and are also limited in their ability to have robust procedures to back up their data, she said.

"The effects of ransomware have evolved," said Dan Twersky, New York-based claims advocate and cyber claims leader for FINEX North America with Willis Towers Watson P.L.C. The "big issues" initially concerned whether the ransomware should be paid, he said. Now, its impact on firms' business operations has "really become the primary concern," he said.

Paying ransomware "is not particularly effective," Mr. Fuhrman said. Organizations should focus on prevention, he said. "The only real way to restore data is to go to backups." Those who do not have backups "are in trouble," he said.

Willis Towers Watson has no hard and fast rule as to whether ransomware should be paid, Mr. Twersky said. "We've taken the position that each incident and each attack warrants its own unique analysis," he said, with relevant factors including whether the data has been compromised or encrypted, whether there is a decryption key available and whether there is a backup.

"Many of our clients who have suffered ransomware attacks had excellent backup systems in place, and good IT personnel were able to isolate and disable the affected machines," said Michael Born, Kansas City, Missouri-based vice president of the global technology and privacy practice at Lockton Cos. L.L.C.

But for firms without backups and property protections, ransomware "can cripple your company, and often the ransomware demands are not that big, so for the cost of paying the demand," it may be worth it if companies can get their systems back, Mr. Born said.

"If it's the difference between insolvency and continuing your business for an additional $300, it's probably an easy choice for most," said Joshua Gold, a shareholder with Anderson Kill P.C. in New York.

Robert Horn, associate director at Crystal & Company in New York, said in one case a 911 dispatching firm that fell victim to ransomware "didn't think they had the opportunity to negotiate with hackers" and paid the roughly $44,000 demanded in ransomware.

Meanwhile, observers warn that the malware that carries the ransomware may include other insidious software, including the installation of "back doors" that give crooks easy future access into computer systems.

There is also the danger of computers becoming botnets, or part of a remote-controlled network of compromised computers that become "zombies" used to spread malware to other computers. Data retrieved by criminals through ransomware may also be sold to others on the web, say experts.

> "Many of our clients who have suffered ransomware attacks had excellent backup systems in place, and good IT personnel were able to isolate and disable the affected machines." But for firms without backups and property protections, ransomware "can cripple your company."
>
> Michael Born,
> Lockton Cos. L.L.C.

K&R, cyber policies can cover ransomware hits

Ransomware coverage is available in both cyber liability and kidnap and ransom policies, although it may take some analysis to determine the best combination of coverage, say experts.

Dan Twersky, New York-based claims advocate and cyber claims leader for FINEX North America with Willis Towers Watson P.L.C., said the brokerage tries to structure the coverage so that a K&R policy, which almost always has no deductible, is the primary insurance, with a cyber policy providing excess coverage.

Adam Cottini, managing director of insurance and risk management in North America at Arthur J. Gallagher & Co. in New York, said he asks his clients to look at and coordinate cyber and K&R coverages in making their purchasing decisions.

"We're seeing some carriers taking K&R policies" and sublimiting the cyber pieces of the coverage, he added. "Be careful of that," because "you might want to purchase" cyber extortion coverage as part of the cyber coverage to take advantage of these policies' higher available limits compared with those in K&R policies, he said.

"Most K&R policies have historically provided extortion coverage" even before cyber "was on most risk managers' radar," said Joshua Gold, a shareholder with Anderson Kill P.C. in New York.

But "lots of people don't actually buy K&R coverage," although "it never hurts to have that coverage updated and perhaps expanded in policies," he said.

And policyholders with K&R coverage should be sure their policies are "written broadly enough to cover some of the most likely extortion claims out there from a cyber context," he said.

Experts note that ransomware demands generally falls within cyber policy retentions because of the relatively small amount usually demanded. The real value of these policies is the consulting help they provide, these experts say.

Judy Greenwald

Implementation deadline nears for major cyber security rule

BY MATTHEW LERNER
mlerner@businessinsurance.com

The New York State Department of Financial Services' new cyber security regulations are putting a strain on insurers and brokers as they move toward compliance with the rules designed to improve cyber security among "covered entities" and their vendors.

The department's cyber security regulation requires banks, insurers and other financial services institutions that it regulates to have a cyber security program designed to protect consumers' private data; a written policy or policies that are approved by the board or a senior officer; a chief information security officer to help protect data and systems; and controls and plans in place to help ensure the safety and soundness of New York's financial services industry.

Part 500 of Title 23 of the Official Compilation of Codes, Rules and Regulations of the State of New York, otherwise known as 23 NYCRR Part 500, became effective March 1, 2017, and the 180-day transitional period ended Aug. 28, when covered entities were required to be in compliance with requirements of Part 500 unless otherwise specified. Covered entities are required to submit the first certification by Feb. 15, 2018, according to the department.

Part 500 is "designed to promote the protection of customer information as well as the information technology systems of regulated entities. This regulation requires each company to assess its specific risk profile and design a program that addresses its risks in a robust fashion," according to the regulation.

Insurers and brokers have faced challenges along the road to compliance, according to several of those involved in the process.

"Insurers and brokers, compared with their banking counterparts, which have been practicing sophisticated cyber security for years, are playing catch-up because they've never had to be as secure as banking regulators have forced banks to be," said Scott Corzine, senior managing director with Ankura Consulting Group L.L.C. in New York.

Part of the burden is managing insurers' and brokers' vendors, which must also comply with the new standards, experts say.

"Compliance with the vendor management provisions has led to challenges," said James Gkonos, special counsel with Saul Ewing Arnstein & Lehr L.L.P. in Philadelphia. "As part of the requirement that covered entities ensure compliance by third-party vendors, they must track compliance. Many companies have neither done this in the past nor dedicated the resources to this task, so this new requirement is proving to be a challenge."

"The biggest unknown and difficulty factor for insurers and brokers to get over is how they identify third-party information parties, which are addressed in Part 500," Mr. Corzine said. "They must risk-assess vendors and set minimum standards. They must go into the field and validate vendor cyber security, and must do it regularly. That's a bear."

Mr. Gkonos adds that there may also be a time crunch involved. "For companies with many contracts with affected third-party vendors, the logistics of renegotiating these contracts within the prescribed time frame could be daunting," he said.

There will likely also be more work for some companies' board members.

"Undoubtedly, there are new responsibilities that will apply to the boards of the regulated companies," said Matt McCabe, senior vice president in Marsh USA Inc.'s cyber practice in New York. "It's yet another burden on the board and something else operational that they have to carry."

"Firms have been assessing their cyber security organizational structure and determining the appropriate placement and reporting lines of the CISO. This includes special attention being paid to the independence of the CISO," said Jaime Kahan, advisory services principal with Ernst & Young L.L.P. in New York.

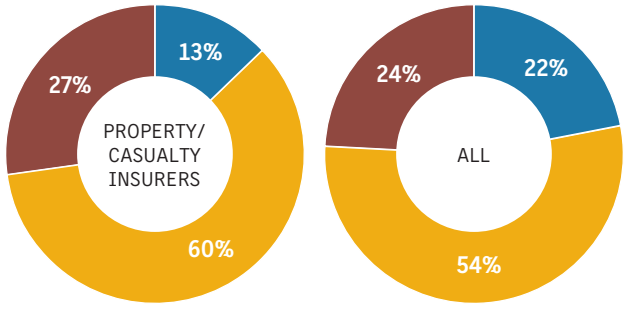
"As noted in EY's 2017 Chief Risk Officer Survey, boards have been aware of cyber threats for several years, but in 2016 and 2017 the survey identified a significant increase in organizational awareness and concern from all of those involved in the survey."

Although insurers and brokers will have to dedicate time and resources to compliance, an ounce of prevention could be worth a pound of cure given the potential extent of cyber breach damage, sources said.

"The potential damage and existential threat from a cyber event is a very powerful reason for focus in this area," said Ms. Kahan.

"With the average cost of a data breach and regulatory defense and fines rising dramatically, NY Reg 500 is a much-needed and fundamentally sound regulation that aligns well with good information security standards like ISO 27001 and NIST 800," said Karen Painter Randall, partner and chair of cyber security and data privacy, and co-chair of professional liability with Connell Foley L.L.P. in Roseland, New Jersey.

MANAGEMENT & REPORTING STRUCTURES FOR CYBER SECURITY



Source: EYGM Ltd., 2017

The ISO/IEC 27000 family of standards helps organizations keep information assets secure, according to the International Organization for Standardization.

NIST Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, from the National Institute of Standards and Technology was "developed by NIST to further its statutory responsibilities under the Federal Information Security Management Act ... NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems."

Ms. Randall added that "once implemented and executed, it will notably reduce a covered entity's risk of data breaches and other common cyber security incidents resulting in the protection of consumers' personally identifiable information and reduced legal and regulatory exposure."

The New York regulation could even spark the creation of similar state regimes, some sources said.

"You'd expect other states to issue new regulations, and what this will lead to is a mosaic of cyber regulations across the country," said Mr. McCabe. "Large organizations which are subject to multiple jurisdictions have to meet every one of those regulatory guidelines."

"At a state level, other states such as Kentucky and Colorado have proposed cyber security requirements for financial institutions in their state," said Ms. Kahan.

EQUIFAX HACK EXTENDS OVERSIGHT

New York Gov. Andrew Cuomo extended the regulations in Part 500 of Title 23 of the Official Compilation of Codes, Rules and Regulations of the State of New York to credit reporting agencies in the wake of the Equifax Inc. breach on Sept. 18.

"Oversight of credit reporting agencies will help ensure that personal information is less vulnerable to cyber attacks and other nefarious acts in this rapidly changing digital world. The Equifax breach was a wake-up call, and with this action New York is raising the bar for consumer protections that we hope will be replicated across the nation," Gov. Cuomo said in a statement at the time.

Consumer credit reporting agencies that operate in New York must register annually with the state's Department of Financial Services beginning on or before Feb. 1, 2018, and by Feb. 1 of each successive year for the calendar year thereafter.

Further, every credit reporting agency must also comply with the department's cyber security regulation on a phased-in schedule of compliance beginning April 4, 2018.

"The data breach at Equifax demonstrates the necessity of strong state regulation like New York's first-in-the-nation cyber security actions," said Financial Services Superintendent Maria T. Vullo in New York. "This is one necessary action of several that DFS will take to protect New York's markets, consumers and sensitive information from criminals."

The move was a positive and even necessary step, according to one New York technology consultant.

"I think for the optics and the substance, credit reporting companies have to be included," said Scott Corzine, senior managing director with Ankura Consulting Group L.L.C. in New York. "These are companies that provide stewardship over vast amounts of highly personal data in a way that is aggregated and concentrated."

Matthew Lerner

Reduce hack fallout with foresight

BY ROB LENIHAN
rlenihan@businessinsurance.com

Cyber attacks have been dominating the news, with stories about breaches at Equifax Inc., Yahoo Inc. and Sabre Systems Inc. and the damage done by ransomware such as WannaCry and NotPetya — but the best time to respond to a cyber breach is long before it happens, experts say.

Insurance executives and risk management analysts warn that organizations cannot afford to plan their response to a breach after it has occurred, as regulators, shareholders and clients will be demanding immediate answers.

"You really can't talk about breach response without first talking about how an organization should be prepared, what they should be doing, what they should be thinking about as an organization and then putting a plan in place," said Joe DePaul, New York-based cyber/errors and omissions practice leader for FINEX North America at Willis Towers Watson P.L.C. "It really has to come from the top down, from the board, from the C-suite executive team down through the organization. Having that culture in place that's very focused in this area is very important."

The key elements for any incident response plan involve preparation and practice, Mr. DePaul said.

"If you don't prepare, if you don't practice, ultimately your response plan will fail," he said. "You really need to understand what that response says, who's involved, and make sure that plan is really up to speed."

"Ironically, the key to an effective response is what you actually do before the breach ever occurs," said Jeffrey Dennis, managing partner and cyber security practice lead with Newmeyer & Dillion L.L.P. in Newport Beach, California. "Having an effective rapid response plan — what we call a cyber incident response plan — is really the key."

Mr. Dennis recommended a four-step approach to dealing with a breach: do an initial assessment, take steps to minimize further damage, record and collect the data related to the type of breach, and then notify law enforcement, regulators, employees and affected consumers (see related story).

"Underwriters who are writing cyber policies are looking at what types of plans and procedures you have in place," Mr. Dennis said. "And if you've got a cyber incident response plan or already worked on one, I think you've got a pretty good shot of actually being able to secure effective insurance, and it should reflect favorably on the rates you're going to get."

Preparation also has financial benefits. The Ponemon Institute L.L.C.'s 2017 Cost of Data Breach Study found that programs that preserve customer trust and loyalty in advance of the breach will help reduce lost business and customers.

"In this year's research, more organizations worldwide lost customers as a result of their data breaches," the report says. "However, as shown, having a senior-level leader, such as a chief privacy officer or a chief security officer, who is able to direct initiatives that improve customers' trust in how the organization safeguards their personal information will reduce churn and the cost of the breach."

Forty-eight states, the District of Columbia, Guam, Puerto Rico and the U.S. Virgin Islands require private or governmental entities to notify individuals of security breaches of information involving personally identifiable information, according to the Denver-based National Conference of State Legislatures. Alabama and South Dakota do not have these requirements.

Regulations vary, but the conference says these states and territories "have enacted legislation requiring private or governmental entities to notify individuals of security breaches of information involving personally identifiable information."

"The broker typically gets the first phone call, whether it's a fire or a data breach," said John Farley, New York-based vice president and cyber risk practice leader at Hub International Ltd. "We get the call at the broker's level, and we have to help our clients make decisions that day. My role is to make sure a bad day does not become a catastrophic day."

Coordinating the response can sometimes be challenging, Mr. Farley said.

"You may have a spokesperson on your team and you may have general counsel on your team, and it gets interesting," he said. "A spokesperson will want to tell people what happened. They're communicators by nature, whereas you have general counsel who are hard-wired not to say a word if they're not legally obligated to do so."

Katherine Keefe, Philadelphia-based global focus group leader for breach response services with Beazley P.L.C., said the company's cyber liability product, Beazley Breach Response, exists because "many organizations have never been through a data breach before, or maybe they have but they haven't realized it."

The Beazley team has "managed over 7,000 incidents, and every single one of them is different," she said. "While we can't say we've seen it all, we've seen a lot."

In an email, Ms. Keefe said: "On a daily basis, we receive notifications of incidents involving 'unintended disclosures.' These include emails containing personally identifiable information or protected health information sent to the wrong recipient, mailings gone awry, or sensitive information accidentally left open to the internet after network maintenance. The second most frequent category of incidents is 'hack or malware.' Common hack or malware incidents include ransomware, as well as successful phishing attacks where bad actors gain user credentials or the recipient downloads malware from the phishing email."

Ms. Keefe said the team organizes such things as mail houses, call centers, credit monitoring and crisis management so the company doesn't "have to be running around in the heat of the moment looking for these services" and can also connect the company with a data breach law firm where the lawyers "eat, breathe and sleep data breach investigations."

Zach Olsen, San Francisco-based president of Infinite Global Inc., said the communications firm helps companies plan for breaches.

"We'll go in and do a crisis communications audit, essentially, where we'll look at who the organization is, what they care about and who all their audiences are, both internal and external," Mr. Olsen said. "And we'll help them build a plan so that if something does go down, they know what to say, who to say it to and how to do it, so they're not leaving people in the dark."

FOUR STEPS TO TAKE AFTER A DATA BREACH HAPPENS

When dealing with a cyber breach, Jeffrey Dennis, managing partner and cyber security practice lead with Newmeyer & Dillion L.L.P. in Newport Beach, California, recommends a four-step approach.

1. Do initial assessment: Identify what damage has occurred and what the risk is — what type of attack it was, what data has been compromised — and that will dictate the next steps. "When you know what you're dealing with, you know what path to go down in your incident response plan," he said.

2. Take steps to minimize any further damage: Reroute traffic within your operating systems or set up a web filtering system or isolate parts of your network. "It's akin to stopping the bleeding," Mr. Dennis said. "If you've got a problem, you've got to plug the hole and make sure you're not being continuously breached."

3. Record and collect the data related to the type of breach: Image your impacted system in a forensically acceptable manner so you can preserve the data and can figure out — once you stop the bleeding — what happened, how it happened and who's responsible. "You don't have the time to do that during the breach, because you've got to do all these other things," Mr. Dennis said.

4. Notify: This is one of the most challenging steps, Mr. Dennis said, as notification laws vary from state to state. How do you notify your employees? When do you reach out to law enforcement, whether it's the FBI, the Secret Service, the U.S. Department of Homeland Security or local authorities? And what do you tell your customers?

"You can see why it's so important to have a plan in place, because you don't want to get breached and at that point have to figure out where your customers reside and then figure out what law applies to those customers," Mr. Dennis said.

Rob Lenihan

AUGMENTED REALITY MAKES AN APPEARANCE IN THE WORKPLACE

But privacy concerns surround smart-device use

BY ROB LENIHAN
rlenihan@businessinsurance.com

The surge in development and use of wearable technology is helping employers protect workers and encourage healthy behavior, but it's also raising privacy concerns.

As employers use wearable devices — including so-called "smart" vests, belts, watches and helmets — to monitor employee movements and behavior, they can gather vast amounts of personal data that could leave them liable to breach of privacy allegations if they misuse use the data or if the data is accessed by criminals or other entities.

While wearable device makers say they have privacy protocols in place, experts advise employers to restrict their use of wearables and only gather data that's relevant for their health and safety objectives.

Wearable devices have become a huge market over the past several years.

In August, the Stamford, Connecticut-based research and advisory firm Gartner Inc. forecast that 310.4 million wearable devices will be sold worldwide in 2017, up 16.7% from 2016, and that sales of wearable devices will generate revenue of $30.5 billion in 2017.

While corporate use of the devices is often related to employee wellness programs, they are also used to monitor safe employee behavior, such as lifting techniques, and track employee location in potentially dangerous locations, such as construction sites (see related story).

A report last year by financial services firm PricewaterhouseCoopers L.L.P. warned that wearables "have the potential to capture and store more personal data than any other device that we've ever owned," including details about employees' every move, habits, interests and health information.

Rachel Michael, Park City, Utah-based thought leader of the ergonomics practice group within Aon Risk Solutions, defines wearables as technology "with some kind of data feed."

There are three potential outcomes from a wearable campaign, she said: employers want to compare their group with an established threshold, they want to change individual behavior, or they want to change organizational behavior.

"These are the three things we would start our clients with," Ms. Michael said. "Which of these three things are you trying to get by implementing wearable technology?"

Given the rapid development and use of wearables — the next generation will likely include exoskeletons that augment a person's strength and endurance — employers need to be aware of security issues, said Thomas Ryan, New York-based senior principal and director of workers compensation research and integrated casualty consulting at Willis Towers Watson P.L.C.

"There are very viable and potential risks associated with wearables," Mr. Ryan said, "and I think the big one that's at the forefront for a lot of employers is cyber risk, because there are concerns about any type of hacking of the data, privacy invasion and losing control of the data that's been accumulated and having that data compromised."

"Not unlike the early days of laptops and smartphones," the PwC report said, "questions about security and privacy have yet to be resolved for wearables. As wearable technology becomes more ubiquitous in the workplace, transparency and employee education will go a long way toward resolving these issues."

Ms. Michael of Aon said employers should define what they want from their wearable technology campaign before they purchase the devices and "certainly before they go implementing them with employees."

Employers should restrict their data collection to data that they need for legitimate purposes, said employment attorney Kate Bischoff, owner of Thrive Law & Consulting L.L.C. in Minneapolis.

"From a risk management perspective, it becomes an issue of what information do we want, what do we not want, and how do we figure out how to get the right information and use it appropriately?" she said. "I think there are some really great things we can do with wearables; it's just that I'm a little concerned that we say, 'Well, let's track everything and see what information we can get from it,' and I think that's not necessarily the way to go."

Under laws in most states, employees have a reasonable expectation of privacy, Ms. Bischoff said.

"We might not want to know where employees are when they're not on duty," she said. "If we go beyond gathering things for the workplace, but we're gathering information about the employee, that makes me nervous."

Brett Kelsey, Plano, Texas-based chief technical officer for McAfee Inc., said he is a proponent of wearable technology, "but I'm a guy who likes to play the devil's advocate from a security perspective."

"The concern I have is, one, what data are they actually storing? And second, what level of protection do they have — not just of the data itself, but for the device?" Mr. Kelsey said. "All-around usage and availability security is a complete afterthought — that's not even a consideration in the creation of the device."

Collecting employees' medical information could lead to legal concerns surrounding the Health Insurance Portability and Accountability Act of 1996, which provides data privacy and security provisions for safeguarding medical information.

"Don't collect the information if you don't need to use it," said Ms. Michael of Aon Risk Solutions. "Unless you are going to command a million-dollar assembly line project from collecting this data, why are you measuring employee sleep cycles? Why are you measuring employee heart rates? You're collecting what could be considered personal medical information? Why?"

Ms. Michael also noted that companies can resolve many issues related to posture without using wearables.

The U.S. Occupational Safety and Health Administration's general duty clause could also cause problems for companies, Ms. Michael said, since it states that the burden is on the employer to make a place of employment that it is

> "From a risk management perspective, it becomes an issue of what information do we want, what do we not want, and how do we figure out how to get the right information and use it appropriately?"
>
> Kate Bischoff,
> Thrive Law & Consulting L.L.C.

safe from reasonable and known hazards.

If a company collects data through wearables that shows the workplace is unsafe but does not make any changes, "you just told us you have a really bad place to work and you haven't done anything about it," Ms. Michael said.

Karla Grossenbacher, a partner with law firm Seyfarth Shaw L.L.P. in Washington, said companies need to obtain their workers' consent when collecting sensitive information.

"If it's voluntary," she said, "and you got their consent and you use it for a purpose that you didn't tell them about when you got their consent, then the consent isn't effective and you're looking at potential invasion of privacy issues. And then if you don't take reasonable precautions, then you can find yourself in a data breach type situation and open to a negligence claim."

Manufacturers of wearables say they take measures to protect privacy.

Gaia Dempsey, co-founder and vice president of corporate affairs at Los Angeles-based Daqri L.L.C., which manufactures smart glasses and helmets, said the company asks for consent from the end user for all the data it collects. Enterprise customers — which the company defines as a company with 10,000 employees or more — using the devices with their workers are contractually required to create privacy policies that are in line with industry standards, be transparent with the data they collect and how it will be used, and communicate that information to the end users, she said.

Eric Martinez, CEO and founder of Modjoul Inc. in Clemson, South Carolina, said his company restricts the data it collects through its smart belts to a worker's location, motion and environment.

"What we were advised was not to put biometric sensors on our belt," he said. "We don't touch skin, so it was hard for us to do it anyway. At work, you just want to know if you're busy and you're doing the job right. We don't care about how many calories you burn — what we care about is are you safe or can we help you be safe by telling the supervisor there might be an unsafe act going on."

Chad Hollingsworth, CEO and co-founder of Triax Technologies Inc. in Norwalk, Connecticut, said the company's spot-r system is strictly for the workplace.

"The way we approach wearables is we want them to work well and protect workers when they're on the job site, which is the most dangerous part," he said. "But when they leave, I don't need to know what they're doing or where they're going or how they're going about their day."

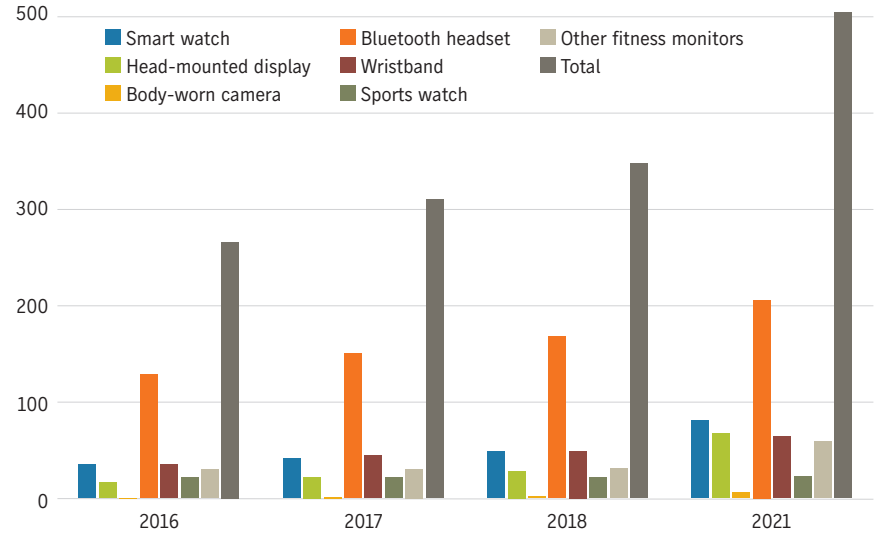
Douglas Turk, chief marketing officer with JLT Specialty USA, a unit of Jardine Lloyd Thompson Group P.L.C. in Los Angeles, said he believes that "the privacy concerns will be traded off with some kind of economic or health benefit" for the end user. Mr. Turk is the firm's expert in this area and leads the development of JLT's partnerships around wearables.

"The best kind of example," Mr. Turk said, "is there are millions of people wearing some form of physical activity tracker, managing their activity, and many programs today reward people for their results."

In June, JLT Specialty USA announced it was partnering with insurtech company Altumai L.L.C. on a program aimed at reducing worker injuries in the food and agriculture industry. Wearables are included in this program, and Mr. Turk said that "the data is currently anonymous when analyzed in the aggregate and it is specific to the employee when dealing with claims and loss and safety in the field."

A WORLD OF WEARABLES

Forecast for wearable devices worldwide (in millions of units)



Source: Gartner Inc., August 2017

Smart devices surround workers with 3-D info

Wearable technology is creating a new working environment for many employees.

Los Angeles-based Daqri L.L.C. describes its smart helmet as "a visionary tool for the 21st-century worker."

The helmet, a wearable device equipped with augmented reality technology, can provide workers with 3-D information, data visualization and work instructions that appear on transparent stereoscopic optical displays right before their eyes in a factory, lab or plant.

Gaia Dempsey, co-founder and vice president of corporate affairs at Daqri, said the helmet and Daqri's smart glasses are part of the company's plan to bring augmented reality "into the workplace in a way that is meaningful, that fits with existing workflows and molds to the way people are already working."

The device helps employees make critical decisions more safely, Ms. Dempsey said. "You know you're plugged into the most important data and all the critical business information that you need to make decisions in the moment. With step-by-step AR work instructions, nothing is falling through the cracks. I'm not relying on my fallible memory from training I had a year and a half ago. The information I need is right in my view, in an intuitive and interactive interface."

TWITTER.COM/DAQRI

Daqri's smart glasses help bring augmented reality to the workplace.

Wearable devices can help improve safety for a vast number of workers, said Eric Martinez, CEO and founder of Modjoul Inc. in Clemson, South Carolina. His company's smart belt collects such data as a worker's location, motion and environment, including temperature, and can be used in a variety of workplaces ranging from warehouses to airlines to retail.

"Most of the wearables you see are on a hard hat or a vest, and that kind of limited the size of the market," he said. "There are 60 million blue-collar workers in the U.S. It's not who puts on a hard hat or a vest every day, but who wears a belt every day. Our electronics are in the buckle that we designed, we use almost the entire real estate of the belt with sensors."

Mr. Martinez is former head of claims at American International Group Inc. — "I know a little bit about the claims side," he quipped.

"I think you're going to see wearables become ubiquitous in a lot of labor jobs," said Chad Hollingsworth, CEO and co-founder of Triax Technologies Inc. in Norwalk, Connecticut. "We're really focused on construction. I think you're going to see a lot of different wearables looking at different things."

Triax developed the spot-r wearable system, which is a 2017 *Business Insurance* Innovation Awards winner that provides a worker's location, identifies slips, trips and falls, and emits a warning in the event of an evacuation.

Rob Lenihan

COMMENTARY

Paying the price of lax security

Governments around the world routinely proclaim they don't negotiate with terrorists. Yet, as official archives released years later sometimes reveal, they often do.

While the principle of not encouraging more terrorist activity by offering any concessions may be laudable, when it comes down to specific cases, the consequences of not talking may be impracticable or unpalatable.

The same appears to be true in the world of cyber crime. As we have seen over the past couple of years, and particularly over the past six months, ransomware attacks are becoming an increasing problem for companies and individuals. Apparently easily available if you know where on the dark web to look, ransomware programs can be used to lock up computers and hold them as virtual hostages until the ransom is paid. Usually demanded in bitcoin, the ransoms may be just a few hundred dollars, but they can add up to considerable sums if they are paid by enough people with captured data.

Gavin Souter
EDITOR

And for some companies, paying the ransom is worth it. As we report on page 27, while major ransomware attacks such as WannaCry and NotPetya grab most of the attention, companies are being hit by a steady stream of smaller attacks and must face the decision of either losing their data or paying up. Given the importance of data in today's commercial world, it's understandable that some organizations feel that they really have no choice in the matter.

While they may resent making any payment to criminals on principle — and fear that their data won't be unencrypted even if they do pay — companies must act in the real world. They have to continue operations uninhibited and must do whatever it takes to keep their businesses running.

Given the volume of attacks, though, they also must take measures to at least reduce or even eliminate the impact if they are held to ransom.

The first step should be having backup protocols in place. By frequently backing up their data, organizations should be able to isolate ransomware attacks when they occur and draw on their backed-up data to continue their operations. With Plan B in place, organizations should then be able to concentrate on installing high-quality cyber security programs and training employees, regularly and consistently, in cyber security best practices.

Insurance can also play an important role. Coverage for ransomware attacks is available under both kidnap and ransom policies and cyber liability policies, so policyholders should be able to secure coverage in the event their security efforts fail. And as the cyber liability market matures, with more underwriters offering broader coverage and higher limits and pricing cyber risks into more coverages, they should be able to offer lower premiums to better-protected risks. At least, that's how it should work in principle.

SCHILLERSTROM

VIEW FROM WASHINGTON

More action on opioids

The opioid crisis is getting a lot of attention at the highest levels of the U.S. government — but it still may not be enough to stop the epidemic.

President Donald Trump issued a memorandum on Oct. 26 stating it will be "the policy of the United States to use all lawful means to combat the drug demand and opioid crisis currently afflicting our country."

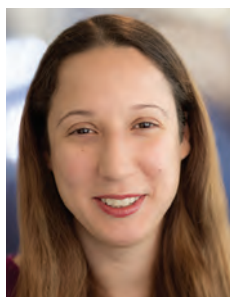
In 2016, 64,000 Americans died of drug overdoses, primarily from opioids, according to the U.S. Centers for Disease Control and Prevention, meaning overdoses now kill more Americans than motor vehicle crashes or gun-related incidents. Since 2000, more than 300,000 Americans have died from overdoses involving opioids.

And it's not just the death toll, although that certainly should be the main concern. About $55 billion in health and social costs are related to prescription opioid abuse each year while another $20 billion is spent in emergency department and inpatient care for opioid poisonings, according to the CDC.

I'm heartened that President Trump understands the severity of the epidemic. He has spoken directly about it, telling personal anecdotes of friends struggling with addiction. He has declared the drug demand and opioid crisis a public health emergency, which will mobilize the considerable resources of the federal government to attack the problem, including cutting red tape to more quickly allow addiction specialists to come to the aid of the addicted. And he noted that it's a problem that may take decades to solve.

Still, government officials on the front lines don't think the Trump administration has gone far enough. The National Association of County and City Health Officials, representing nearly 3,000 local health departments, said the "declaration of an opioid public health emergency and not a state of national emergency does not go far enough" because it only lasts 90 days and does not provide additional federal funds. The association encouraged the president to make the national emergency declaration, which would facilitate more federal dollars to local health departments.

Every day, 91 Americans die from opioid overdoses, according to the CDC. That death rate should alarm all of us, including those in Washington who are in a position to do something about it. The Trump administration and the U.S. Congress must act quickly to give these local officials the tools and freedom they need to fight the crisis.



Gloria Gonzalez
DEPUTY EDITOR

As of August, 31 bills had been introduced in Congress to address the opioid epidemic, according to an analysis by law firm Squire Patton Boggs. Some bills would increase funding to proactively combat the crisis, including providing grants to train health care practitioners in best practices in pain management and substance abuse recognition. Others would tackle the current flood of addicted patients to treatment centers and substance abuse programs by paying for increased clinical services. While it is highly unlikely all these bills would pass, given everything else Congress is working on, surely some of them have enough bipartisan support to get them to the president's desk.

Many people, including the president, understand opioid addiction is a significant problem for our country. Let's not let politics get in the way of a solution.

Keys to negotiating indemnity agreements

The effective management of indemnification and related insurance obligations is an active agenda item for top-level business leaders, including any CFO, CEO and general counsel. It is, therefore, imperative, whether you are a Fortune 500 company or a small business, that your company's risk management and legal departments strategically manage indemnification and insurance obligations to minimize the always increasing cost-of-business demands.

Commercial, construction and professional services contracts commonly include indemnification provisions, along with the requirement that an indemnified party be named as an additional insured on any applicable insurance policy. When a defense and indemnity claim is subsequently made, however, these apparently straightforward agreements often are subject to interpretation, which can lead to significant disputes among the parties and their respective insurers. As a result, nearly every state's judiciary and/or legislature are undertaking a concerted effort to limit, and sometimes altogether invalidate, indemnity agreements. As new laws are passed and groundbreaking judicial decisions are issued, the insurance industry responds with frequent modifications to the language utilized in the standard ISO Additional Insured Endorsement Form. Companies, and their respective legal and risk management departments are, therefore, confronted with increasing challenges in keeping up with changes in the law to ensure their company's indemnity agreements are enforceable.

While the issues that arise in indemnity and insurance coverage disputes cannot be comprehensively addressed in a single article, there are common pitfalls that can be avoided. Focusing on five key issues can help to ensure that your company is well protected.

1. The language of the indemnity agreement

The party with a stronger bargaining position — often referred to as the "upstream" party, such as an owner or contractor — is often the drafter of a commercial contract and tends to initially control the indemnity obligations of the less powerful or "downstream" party, such as subcontractors and suppliers. One commonly overlooked issue by a downstream party, or even an upstream party in the case of mutual indemnification, centers upon the use of the language "arising out of" versus "to the extent caused by."

Some courts interpret the "arising out of" language to stand for a "but for" causation theory of liability. In other words, any remote causal relationship between the upstream party's liability and the incident in question will suffice to trigger the downstream party's indemnity obligations.

More recently, however, sophisticated companies are requesting that the phrase "to the extent caused by" be utilized in the indemnity agreements in place of the "arising out of" standard. "To the extent caused by" has been interpreted by some courts to mean legal and proximate causation. From a practical standpoint, this often results in no duty to defend or indemnify if the claimant does not allege the injuries or damages were caused, in whole or in part, by the upstream party's negligence.

2. Selecting the governing law

While obvious, it cannot be stressed enough that parties negotiating a commercial contract should carefully consider which state's law will control any subsequent contractual dispute. If there is no governing law provision in the contract, the laws of the state in which the incident occurred or where the service was performed will typically control. If you conduct business nationally, a governing law provision is critical because nearly every state has enacted anti-indemnification legislation.

In 45 states, anti-indemnification legislation has passed to protect parties with the weaker bargaining position in industries such as construction, transportation and oil field services. Depending on where you sit, that can be good, bad or both, but regardless it is always best to know how you may be impacted. It is critically important to thoroughly understand the language of these statutes; they are not consistent, do not always affect the same industry, and/or follow the same framework. Some states' laws prohibit indemnification for another's sole negligence, while others permit indemnification, but only for the negligence of the downstream party.

A majority of anti-indemnification statutes do not affect insurance coverage. Although the indemnity obligation may be void under a particular state's law, additional insured coverage may not be prohibited. This result is typically referred to as the "additional insured loophole."

3. Specificity in insurance obligations

Failure to include specific language identifying the type of insurance policy and the specific additional insured endorsement to be used can also lead to significant and costly coverage disputes.

When negotiating insurance obligations, it is always best practice to request the policy terms that your business requires. It is critical to define: whether the coverage should be occurrence-based or claims-made; what the per-occurrence or per-claim limits are; what the general aggregate limits are; and whether the limits must be satisfied through a primary, excess and/or umbrella policies. In doing so, consider whether the second layer of coverage is a true follow form policy, and if not, ensure the umbrella policy is designed to provide the same or substantially similar type of coverage as the primary policy. Gaps in coverage can be unintentionally created if these issues are not addressed in the original contract, and disputes often arise between primary and excess insurance carriers as a result.

4. Requesting the appropriate additional insured endorsement

The initial additional insured endorsement form was introduced in 1985, which is commonly referred to as "broad form" coverage. The 1985 endorsement provides the additional insured blanket coverage, but only with respect to a liability arising out of their work. Due to the "arising out of" language often being interpreted consistent with a "but for" causation standard, the insurance industry was saddled with unanticipated exposure. Subsequent endorsement forms introduced in 1993 through 2001 focused on terminating coverage after the additional insured's work is "complete" and/or put to its "intended use." In 2004, the revised endorsement incorporated "to the extent caused by" language and closed the perceived never-ending defense and indemnity obligation under the "arising out of" standard.

In 2013, however, the ISO endorsement was drastically revised to link the additional insured coverage to the insurance obligations, and if drafted properly the indemnity obligations, in the commercial contract, as well as to specifically address anti-indemnification legislation. In short, the additional insured endorsement will not expand the amount of coverage required under the commercial contract. Indeed, the 2013 ISO endorsement only permits coverage to the "extent permitted by law."

Selecting the specific additional insured endorsement that best suits your company's demands may ultimately depend upon your bargaining position. While upstream parties may still be demanding blanket coverage, the 1985 endorsement has quickly become obsolete, and the 1993 through 2001 endorsements are starting to follow suit. Regardless of whether you are an upstream or downstream party — and particularly if mutual indemnification is required under the contract — the 2013 endorsement may prove to be the ideal option. This principle holds particularly true if careful consideration is given to selecting the appropriate state's law to govern contractual disputes.

5. Communication between legal and risk management departments and brokers

Holding open communications between the legal and risk management departments in your company is a cornerstone to success. The risk managers need to be informed of the terms and conditions of each contract drafted by the legal department. Similarly, the risk managers need to advise the legal department as to insuring obligations. While each department has their own priorities, a symbiotic working relationship between the two departments is truly an important key to effectively managing potential indemnity and insurance exposure. One big loss with indemnification consequences will prove this point.

It is equally important to provide your company's insurance broker with all contracts in existence at the time of obtaining new policies of insurance and/or while renewing existing policies. While most companies are not willing to share their private business deals with third parties, including insurance brokers, having your broker sign a nondisclosure agreement to maintain confidentiality can easily alleviate this concern. Unless your broker is aware of your company's specific contractual obligations, he or she will be unable to effectively obtain the right type of coverage.

Conclusion

Negotiating enforceable indemnity agreements and mirroring your company's insurance program to the indemnity obligations is becoming increasingly more difficult in light of anti-indemnification legislation and the more recent evolution of the additional insured endorsement. If, however, your company's risk management and legal departments focus on these five key areas, most of the potential pitfalls that lead to protracted litigation may be avoided.

James Buldas is a partner at Pietragallo Gordon Alfano Bosick & Raspanti L.L.P. in Pittsburgh. Mr. Buldas focuses his practice in insurance coverage, construction, professional liability, transportation and other various commercial disputes. He can be reached at 412-263-1814 or at jjb1@pietragallo.com.

MARKET PULSE

Ironshore increases political risk capacity

■ Ironshore Insurance Ltd.'s Singapore branch has increased capacity for political risk business lines within its political risk and trade credit unit.

Its political risk unit offers international policy protection for in-country or cross-border exposure to government actions and political risk events. Available capacity are $50 million, up from $15 million, the Ironshore International unit said in a statement.

Ironshore is also expanding its political risk and trade credit team in Singapore, appointing Sam Lim to the new position of underwriter, political risk and trade credit, Asia-Pacific. He joined Ironshore from American International Group Inc.

Swiss Re offers nonprofit professional liability cover

■ Swiss Re Corporate Solutions Ltd., a unit of Swiss Re Ltd., has introduced SwissGuard, a management liability policy for nonprofit and private companies.

SwissGuard includes directors and officers liability, employment practices liability and fiduciary liability coverage for U.S.-domiciled companies, offering protection against claims derived from mergers and acquisitions activity, financial performance, employment matters and breach of fiduciary duty, among other things, Swiss Re said in a statement.

The coverage can be purchased individually or on a combined basis, according to the statement.

IBM launches cloud-based platform for insurers

■ International Business Machines Corp. has partnered with MetLife Inc. to build a platform on the IBM Cloud intended to improve the processes and economics for new product development, underwriting, and benefits delivery for the insurance industry.

The IBM Insurance Platform will feature cognitive computing, data analytics and integration and security capabilities designed to help insurers expand access to their products. It was built in collaboration with MetLife and software provider Majesco Inc., Armonk, New York-based IBM said in a statement.

The platform will be delivered as a service and will also help insurers sense and respond to the market faster while reducing information technology infrastructure and maintenance costs, according to the statement.

Insurers "will be able to inject greater innovation and speed into their operating models, and consumers will experience a broader range of products tailored to their individual needs," Bridget van Kralingen, senior vice president of IBM industry platforms, said in the statement.

PRODUCTS & SERVICES

Aon offers AI-driven comp claims tools

■ Aon Benfield and Santa Clara, California-based CLARA Analytics have teamed up to offer artificial intelligence tools to U.S. workers compensation insurers.

The tools use predictive analytics and AI to address the challenge of helping claims operations make decisions for injured workers quickly, Aon Benfield said in a statement.

The tools include PUMA, which connects injured workers to appropriate medical providers; and CATT, which helps claims managers focus their efforts on priority cases. Machine learning algorithms provide insights through "pattern recognition" based on a dataset, according to the statement.

"For carriers balancing C-suite and board level interest in innovation and cost management, CLARA can be a quick and easy win with minimal impact to expenses," George deMenocal, Stamford, Connecticut-based president and CEO of Aon Benfield U.S., said in the statement.

Law firm unveils blockchain consultancy

■ Clyde & Co has launched Clyde Code, a consultancy to advise insurers and clients in other sectors on issues related to smart contracts, blockchain and distributed ledger technologies.

Clyde Code will advise clients on legal and technical matters and provide services related to smart contracts, including smart contract creation, existing contract enhancement, contract verification to ensure that contracts work as intended legally and technically, contract enforcement and dispute resolution, and forensic investigations in relation to smart contract failures, the London-based law firm said in a statement.

"Blockchain provides the rails that smart contracts run on, and together they have the potential to radically change and simplify legal contracts and transactions, but legal and technical advice is needed to ensure that workable agreements are reached and enforced," Lee Bacon, a partner at Clyde & Co, said in the statement.

Karen Clark updates convective storm model

■ Catastrophe modeler Karen Clark & Co. has released Version 1.0 of its Severe Convective Storm Reference Model.

The multiperil KCC SCS model is licensed as part of the RiskInsight open loss modeling platform, the Boston-based company said in a statement. Hazards of hail vs. tornadoes and straight-line winds are simulated separately.

Along with a catalog of over 33,000 events used for pricing and reinsurance decision-making, the model includes over 100 historical SCS events, according to the statement.

Beazley offers portal for data breach response

■ Beazley P.L.C. has launched a cyber and breach response portal exclusively for its U.S. brokers.

The portal leads to a set of resources designed to keep brokers informed and educated on cyber risk and data breaches, London-based Beazley said in a statement.

Brokers will have access to information ranging from cyber basics to industry-specific issues, regulatory updates, product information, breach and claim examples, and risk insights.

The portal has a "cyber basics" section that introduces insurance brokers to the essentials of cyber and data breach insurance, a Beazley spokeswoman said.

The area also provides webinars to help brokers sell the insurance coverage to policyholders with industry-specific claims examples.

Brokers will also be able to ask questions of Beazley's teams directly from the site and access external sources.

DEALS & MOVES

EPIC to acquire rival broker Frenkel

EPIC Insurance Brokers & Consultants has agreed to buy rival brokerage Frenkel & Co. for an undisclosed amount.

New York-based Frenkel will operate as Frenkel & Company — a division of EPIC, according to the statement issued on the transaction.

Frenkel ranked as the 48th largest brokerage of U.S. business in *Business Insurance*'s latest ranking with $76.5 million in 2016 brokerage revenues. About 50% of its business is derived from commercial retail business and about 30% from employee benefits business.

AmWINS acquires WTW specialty programs

Specialty broker AmWINS Group Inc. acquired 15 insurance programs from Willis Towers Watson P.L.C.

Terms of the deal, expected to close Oct. 31, were not disclosed.

The acquired programs cover a wide range of industries, including ski resorts, auto dealers, recycling, medical facilities, workers compensation, dairy farms, pizza delivery restaurants and more, Charlotte, North Carolina-based AmWINS said in a statement.

Ryan Specialty buys Houston wholesale broker

Ryan Specialty Group L.L.C. reached a definitive agreement to acquire Houston-based wholesale insurance broker Oxford Insurance Services L.L.C.

Terms of the deal were not disclosed.

Oxford specializes in energy, construction, environmental and other complementary markets and will become part of R-T Specialty L.L.C., Ryan Specialty Group's wholesale brokerage unit, Chicago-based Ryan said in a statement.

Gallagher acquires Florida property/casualty broker

Arthur J. Gallagher & Co. acquired Naples, Florida-based Premier Insurance L.L.C., which does business as Lutgert Insurance, for an undisclosed amount.

Lutgert Insurance, which was founded in 1953, is a retail property/casualty broker and benefit consultant, Gallagher said in a statement. Lutgert President Bud Hornbeck, Senior Vice President Steve Benza, Vice President Marc Williams and their associates will continue to operate from their current offices. Lutgert has 85 employees in seven locations, according to its website.

BUSINESS INSURANCE®

BEST PLACES TO WORK 2017

Best Places program lists leading insurance industry firms

Insurance at first glance may appear to be an old-fashioned business. The industry today is attracting talent, however, by offering flexible and innovative work that makes a positive difference to individuals and communities.

Best Places to Work in Insurance is an annual feature presented by *Business Insurance* and Best Companies Group that ranks the agents, brokers, insurers and other providers with the highest levels of employee engagement and satisfaction.

The 2017 report features 75 companies of various sizes, from 25 employees to more than 4,000. What these honorees have in common is a commitment to attracting, developing and retaining great talent through a combination of benefits and other programs that their employees value.

Harrisburg, Pennsylvania-based Best Companies Group identifies the leading employers in the insurance industry by conducting a free two-part assessment of each company. Through an employer questionnaire on policies, practices and demographics and a confidential employee survey, Best Companies Group takes the data and analyzes them according to eight core focus areas: leadership and planning, corporate culture and communications, role satisfaction, work environment, relationship with supervisor, training, development and resources, pay and benefits, and overall engagement.

The program divides employers into the categories of small, or 25-249 employees; medium, 250-999 employees; and large, 1,000 or more employees. The 2017 overall winners, by employer size, are:

Small: **SIG (Silberstein Insurance Group)**
Medium: **Assurance Agency Ltd.**
Large: **AF Group**

The following report highlights what makes these and other companies in the insurance industry among the best places to work.

L
AF Group

M
Assurance Agency Ltd.

S
SIG

AF Group — Individual focus. Collective strength.
LOCKTON
WEST BEND — A MUTUAL INSURANCE COMPANY
Assurance — Minimizing risk. Maximizing health.™
FCCI INSURANCE GROUP — More than a policy. A promise.
HYLANT
SIG — AN ALERA GROUP COMPANY
BALDWIN KRYSTYN SHERMAN — insight beyond insurance
RELIANCE PARTNERS

LARGE EMPLOYER CATEGORY (1,000+ U.S. Employees)

Rank	Company	U.S. Employees
1	AF Group	1160
2	Lockton Companies	4115
3	West Bend Mutual Insurance Company	1240
4	CBIZ Benefits & Insurance Services, Inc.	1388
5	NFP	2670
6	Philadelphia Insurance Companies	1890
7	Shelter Insurance Companies	1868
8	Crum & Forster	2264

MEDIUM EMPLOYER CATEGORY (250-999 U.S. Employees)

Rank	Company	U.S. Employees
1	Assurance	461
2	FCCI Insurance Group	823
3	Hylant	664
4	Lawley	366
5	OneDigital Health and Benefits	864
6	Discovery Benefits	695
7	Amerisure Mutual Insurance Company	743
8	Holmes Murphy & Associates	781
9	TMNA Services, LLC	407
10	Safety National	442
11	The Navigators Group, Inc.	537
12	EPIC Insurance Brokers & Consultants	775
13	Paychex Insurance Agency	860
14	PayneWest Insurance	686
15	Tokio Marine America	373
16	AMERISAFE	449

SMALL EMPLOYER CATEGORY (25-249 U.S. Employees)

Rank	Company	U.S. Employees	Rank	Company	U.S. Employees
1	SIG	50	26	Captive Resources	178
2	Baldwin Krystyn Sherman Partners	145	27	MarketScout	59
3	Reliance Partners	64	28	White & Associates Insurance	67
4	Pritchard & Jerden, Inc.	92	29	The Ashley Group	27
5	Origami Risk	130	30	Venture Pacific Insurance Services, Inc.	36
6	Burnham Benefits Insurance Services	80	31	Gunn-Mowery, LLC	65
7	Mackoul & Associates, Inc.	36	32	Odell Studner Group	52
8	HNI Risk Services	137	33	Rogers & Gray Insurance	154
9	Business Benefits Group	43	34	Lipscomb & Pitts Insurance	125
10	Marsh & McLennan Agency | Michigan Health & Benefits Team	100	35	IPMG	127
			36	The Nitsche Group	124
11	Virtus, LLC	25	37	Syndicate Claim Services	47
12	Simkiss & Block	44	38	McConkey Insurance & Benefits	93
13	ECBM Insurance Brokers and Consultants	71	39	Cambridge Consulting Group	60
14	Costello & Sons Insurance Brokers, Inc.	33	40	Safeware	64
15	Alternative Service Concepts	129	41	AHT Insurance	192
16	Kapnick Insurance Group	158	42	The Plexus Groupe, LLC	104
17	GFI Insurance Brokerage LLC	41	43	TRICOR Insurance	207
18	QEO Insurance Group	59	44	American Integrity Insurance Group	175
19	Fred C. Church Insurance	137	45	Bearence Management Group	91
20	TexCap Insurance	38	46	US Assure	120
21	Alltrust Insurance	38	47	A.I.M. Mutual Insurance Companies	172
22	The Insurance Exchange, Inc.	35	48	Networked Insurance Agents, LLC	110
23	Hoffman Brown Company	56	49	Berkley North Pacific (a Berkley Company)	125
24	Lovitt & Touché	187	50	Falls Lake Insurance Companies	79
25	The Partners Group, Ltd.	140	51	Key Risk	240

BUSINESS INSURANCE®
SPONSOREDSECTION
BEST PLACES TO WORK 2017

Large employer (1,000+ employees)

AF Group

Lansing, Michigan-based AF Group not only was honored as the top large employer in the 2017 Best Places to Work in Insurance, but it also earned honors as the top insurer. Among the things that AF Group's 1,160 employees like most are exceptional benefits for medical, dental and vision care and paid time off; a positive workplace culture that fosters inclusion and innovation; and leadership that inspires involvement and collaboration. In addition to jeans Fridays and fitness Fridays, where jeans or athletic apparel are encouraged, AF also offers employees an Idea Pipeline, an online tool where they can communicate ideas for innovative products and services.

Lockton Companies earned second place in the large employer category in the 2017 Best Places to Work in Insurance. The Kansas City, Missouri-based international retail insurance brokerage, which has 4,115 associates around the world, has been consistently honored in Best Places to Work in each of the last nine years. Ranking third for the second consecutive year in Best Places to Work in Insurance was **West Bend Mutual Insurance Co.** The West Bend, Wisconsin-based property/casualty insurer has 1,240 U.S. employees.

1. **AF Group**
2. **Lockton Companies**
3. **West Bend Mutual Insurance Company**

Employees of AF Group show their love for the insurance company's culture of inclusion, innovation and collaboration.

Medium employer (250–999 employees)

Assurance Agency Ltd.

Schaumburg, Illinois-based **Assurance Agency Ltd.** has earned top honors in the Best Places to Work in Insurance as a medium size employer for five consecutive years. The retail broker provides a broad range of business and personal insurance products, employee and executive benefits, surety bond placement, safety consulting, claims advocacy and wellness programs. Assurance's 461 employees rate the firm highly for its branded perks program, commitment to improving the world through one generous act at a time and its incentive program recognizing colleagues' efforts. The company's culture is marked by flexible work and play. Assurance's Shared Success program provides bonuses for achieving companywide financial and cultural goals.

Second place in the medium size employer category in the 2016 Best Places to Work in Insurance went to **FCCI Insurance Group**, a Sarasota, Florida-based property/casualty insurance company. FCCI's 823 employees appreciate the company's United Way Fall Fest, formal holiday celebrations, wellness and benefits fair, and training and team-building activities.

Assurance encourages its employees to work and play. Social outings and other events are among the team-building activities that employees appreciate about the agency.

Ranked third was **Hylant**, a family-owned retail insurance brokerage based in Toledo, Ohio. Hylant's 664 employees love their employer's deep community involvement, both at local charitable events and companywide initiatives; flexible work hours; and paid time off to meet family needs.

1. **Assurance Agency Ltd.**
2. **FCCI Insurance Group**
3. **Hylant**

Small employer (25–249 employees)

SIG (Silberstein Insurance Group) earned top honors in this category of Best Places to Work in Insurance (see profile, page 3). Runner-up in the small-employer category was Baldwin Krystyn Sherman Partners, a Tampa, Florida–based retail insurance agency with 145 employees. In third place was **Reliance Partners**, a Chattanooga, Tennessee-based insurance brokerage with 64 employees.

1. **SIG**
2. **Baldwin Krystyn Sherman Partners**
3. **Reliance Partners**

Silberstein Insurance Group employees enjoy a night out for group painting. SIG's employees value the retail brokerage's social and community service events.

BUSINESS INSURANCE®
SPONSOREDSECTION
BEST PLACES TO WORK 2017

Insurers/Providers

AF Group

Lansing, Michigan-based AF Group is the top insurance company/provider in the 2017 Best Places to Work in Insurance. AF specializes in workers compensation products and services, including loss control, analytics and risk management. AF Group traces its history back more than 100 years to its founding as Michigan's accident fund. Today, the company has 1,160 U.S. employees and writes workers comp business in all 50 states. Employees' affection for AF Group reflects its culture of open communication, inclusion and innovation.

AF Group gives employees Volunteer Time Off during work hours to support community organizations. In 2016, AF employees' volunteer service exceeded 2,400 hours.

BEST PLACES TO WORK IN INSURANCE 2017: INSURERS/PROVIDERS

Rank	Company	U.S. Employees
1	AF Group	1160
2	FCCI Insurance Group	823
3	West Bend Mutual Insurance Company	1240
4	Amerisure Mutual Insurance Company	743
5	Safety National	442
6	The Navigators Group, Inc.	537
7	Philadelphia Insurance Companies	1890
8	American Integrity Insurance Group	175
9	A.I.M. Mutual Insurance Companies	172
10	Shelter Insurance Companies	1868
11	Berkley North Pacific (a Berkley Company)	125
12	Tokio Marine America	373
13	Falls Lake Insurance Companies	79
14	Key Risk	240
15	AMERISAFE	449
16	Crum & Forster	2264

Agents/Brokers

BEST PLACES TO WORK IN INSURANCE 2017: AGENTS/BROKERS

Rank	Company	U.S. Employees
1	SIG	50
2	Baldwin Krystyn Sherman Partners	145
3	Reliance Partners	64
4	Pritchard & Jerden, Inc.	92
5	Burnham Benefits Insurance Services	80
6	Assurance	461
7	Mackoul & Associates, Inc.	36
8	HNI Risk Services	137
9	Business Benefits Group	43
10	Marsh & McLennan Agency | Michigan Health & Benefits Team	100
11	Virtus, LLC	25
12	Lockton Companies	4115
13	Simkiss & Block	44
14	ECBM Insurance Brokers and Consultants	71
15	Costello & Sons Insurance Brokers, Inc.	33
16	Alternative Service Concepts	129
17	Kapnick Insurance Group	158
18	GFI Insurance Brokerage LLC	41
19	Hylant	664
20	QEO Insurance Group	59
21	Fred C. Church Insurance	137
22	Lawley	366
23	TexCap Insurance	38
24	OneDigital Health and Benefits	864
25	Alltrust Insurance	38
26	The Insurance Exchange, Inc.	35
27	Hoffman Brown Company	56
28	Lovitt & Touché	187
29	The Partners Group, Ltd.	140
30	Captive Resources	178
31	MarketScout	59
32	White & Associates Insurance	67
33	The Ashley Group	27
34	Venture Pacific Insurance Services, Inc.	36
35	Discovery Benefits	695
36	Gunn-Mowery, LLC	65
37	Odell Studner Group	52
38	Rogers & Gray Insurance	154
39	Lipscomb & Pitts Insurance	125
40	Holmes Murphy & Associates	781
41	IPMG	127
42	The Nitsche Group	124
43	CBIZ Benefits & Insurance Services, Inc.	1388
44	McConkey Insurance & Benefits	93
45	EPIC Insurance Brokers & Consultants	775
46	Cambridge Consulting Group	60
47	Safeware	64
48	NFP	2670
49	AHT Insurance	192
50	The Plexus Groupe, LLC	104
51	TRICOR Insurance	207
52	Bearence Management Group	91
53	Paychex Insurance Agency	860
54	US Assure	120
55	PayneWest Insurance	686
56	Networked Insurance Agents, LLC	110

SIG (Silberstein Insurance Group)

For three years in a row, Silberstein Insurance Group has been honored in the Best Places to Work in Insurance. Baltimore, Maryland-based SIG repeated as the top-ranked small employer overall as well as the top employer among agents and brokers in the Best Places to Work program. 2017 marks the eighth year that the employee benefits firm has made the list. Founded in 1999, SIG embraces a Results-Only Work Environment, which features flexible scheduling. Other attributes that SIG's 50 U.S. employees enjoy about their company include onsite fitness classes, community service days and social events, such as family bowling night, Orioles games and a crab feast.

Silberstein Insurance Group hosts community service days, a program in which SIG employees enthusiastically participate.

BUSINESS INSURANCE®
SPONSOREDSECTION
BEST PLACES TO WORK 2017

How insurance firms attract talent

What does it take to join the list of the Best Places to Work in Insurance? A number of characteristics set apart the companies that appear on it this year.

Perks such as office celebrations, social outings and recreational programs can contribute to team building, but a longer-term impact comes from an employer's commitment to a culture of employee engagement and satisfaction. For that reason, Best Companies Group analyzes the responses to confidential employee surveys in eight core areas. It is in these areas where significant differences exist between the best employers and those that did not make the 2017 list:

Leadership and planning. This area includes understanding of the company's strategy, confidence in leadership, adequate planning and follow-through and care about employees' well-being. For all companies on this year's list, the number of positive responses in this area averaged 90%, vs. 80% for companies that failed to make the list.

Corporate culture and communications. Components of this area include clear and frequent communication, trust, a spirit of cooperation, a feeling that employees are valued and a culture of diversity. Positive responses in this area averaged 89% for companies on the list, and 79% for other companies.

Role satisfaction. This area looks at how employees like the work they do, their ability to balance work and life, and whether they feel valued and part of a team. Positive responses averaged 91% for the Best Places to Work in Insurance, whereas that figure was 86% for others.

Work environment. Positive responses about physical working conditions, comfort and safety averaged 91% for the top employers and 88% for employers not on the list.

Relationship with supervisor. Fairness, respect, trust and feedback are elements of this area. For the Best Places to Work, positive responses averaged 91%, vs. 87% for other employers.

Training, development and resources. Initial and ongoing training, adequate and dependable equipment, room to advance and promotions for good work are among the components of this area. Positive responses for the top employers averaged 85%, while that figure was only 77% for others not on the list.

Pay and benefits. Fair compensation and satisfaction with benefits such as paid vacation, health care, dental and retirement plans are among the components of this area. For the Best Places to Work in Insurance, positive responses averaged 87%, and 81% for other employers.

Overall engagement. This area includes employees' overall satisfaction with the employer, a sense of pride in working there, willingness to give extra effort, willingness to recommend the employer's products or services, and recommend working there to others. Positive responses here averaged 92% for the Best Places to Work in Insurance, and 86% for employers not on the list.

Lockton Summer Party on June 17, 2017 in Kansas City, MO. Photographer/Lauren Frisch Pusateri

Employees of Captive Resources enjoy an evening of laser tag, one of various social events the brokerage hosts for team members.

HOW TO GET IN

To participate in the Best Places to Work program, an organization must:

- **Be a for-profit or non-profit business**
- **Be publicly or privately held**
- **Have a facility in the United States**
- **Employ at least 25 people in the United States**
- **Be in business for at least 1 year**

Eligible insurance organizations are: retail agents/brokers, wholesale brokers/managing general agents, reinsurance intermediaries, claims services companies, benefit brokers and consultants, property/casualty insurers, group life/health insurers, and reinsurers. Non-profit insurance associations or service organizations aligned with the commercial insurance industry also are eligible.

For more information or to participate in the 2018 program, please visit www.bestplacestoworkins.com.

It's tough to get off the grid. We seem to have unlimited access to emails and other notifications via smartphones, tablets and wearable technologies.

UP CLOSE

Chris Swensen

NEW JOB TITLE: Salt Lake City-based property/casualty practice leader for USI Insurance Services L.L.C.

PREVIOUS POSITION: Salt Lake City-based vice president of marketing and sales at WCF Insurance

LOOKING FORWARD TO: Returning to the exciting and ever-changing landscape of the insurance retail marketplace and contributing with the support and resources of a premier insurance brokerage like USI Insurance Services.

ON LEADERSHIP: One's ability to effectively inspire others

CHALLENGES FACING INDUSTRY: Addressing the ever-changing demographics of the workforce and effectively attracting, developing and maintaining an emerging workforce of young professionals to this exciting (but not always thought-of) industry of insurance.

CRYSTAL BALL: The continual emergence of new technology risk, such as autonomous vehicles, drones, cyber liability, etc. ... and the challenging task of how we underwrite, determine liability and adjudicate claims with respect to these types of risks.

WHAT SURPRISED ME: The vast amount of career opportunities within the industry.

ADVICE: Never burn a bridge. You never know who you could be working with or for in the future.

FAVORITE QUOTE: "Before you are a leader, success is all about growing yourself. When you become a leader, success is all about growing others." — Jack Welch

OUTSIDE THE INDUSTRY, A DREAM JOB: Fly fishing guide

HOBBIES: Hunting, fly fishing, cheering on my favorite sports team.

THING MOST PEOPLE DON'T KNOW ABOUT ME: I'm fluent in Spanish!

DON'T LEAVE THE HOUSE WITHOUT: Cellphone

BIGGEST OBSTACLE FOR WORK-LIFE BALANCE: It's tough to get off the grid. We seem to have unlimited access to emails and other notifications via smartphones, tablets and wearable technologies.

CORPORATE IMPROVEMENT: More community outreach. We need to make giving back and serving our community a standard.

PET PEEVES: Self-victimization

WHEN I RETIRE: I'm going to spend as much time with my family as possible.

FAVORITE MEAL: Sushi

FAVORITE BOOK: "1776" by David McCullough

ON MUSIC: "Don't Stop Believing" by Journey

CAN'T-MISS TELEVISION SHOW: "Seinfeld"

BEST CITY: Salt Lake City

ON A SATURDAY AFTERNOON: I spend a lot of time watching my sons play AAU basketball.

MONDAYS: Read the newspaper — it will quickly put into perspective and minimize the problems you think you have compared to the problems of others.

SEE MORE ONLINE

Visit *www.businessinsurance.com/ComingsandGoings* for a full list of this month's personnel moves and promotions. Check our website daily for additional postings and sign up for the weekly email. *Business Insurance* would like to report on senior-level changes at commercial insurance companies and service providers. Please send news and photos of recently promoted, hired, or appointed senior-level executives to *editorial@businessinsurance.com*.

ON THE MOVE

American International Group Inc. named former Connecticut Insurance Commissioner **Thomas Leonardi** to the newly created position of executive vice president for government affairs, public policy and communications, effective Nov. 1. Based in New York, Mr. Leonardi joins AIG from Evercore Partners Inc., where he was senior adviser to the firm's investment advisory business. He was insurance commissioner from February 2011 to December 2014.

Pina Albo was named CEO of Bermuda-based Hamilton Insurance Group Ltd. Ms. Albo, who will join Hamilton from Munich Reinsurance Co. on Feb. 1, succeeds interim group CEO David Brown, who has held the position since Brian Duperreault's departure to lead AIG. Currently she is a member of Munich Re's executive management board, overseeing property/casualty operations in Europe and Latin America.

Aon Benfield named **Catherine Mulligan** managing director and U.S. cyber practice group leader. Previously, she was head of professional liability at Zurich North America, where she managed miscellaneous and health care professional liability and security and privacy portfolios and had "driven the public-sector dialogue around cyber insurance on a national scale," Aon Benfield said in a statement.

Axis Capital Holdings Ltd. named former Swiss Re Ltd. executive **Steve Arora** CEO of Axis Re. Based in Zurich, Mr. Arora most recently was head of Swiss Re's casualty reinsurance business and a member of its reinsurance executive committee. He replaces Jay Nichols, who left Axis Re in March.

Mike Harnett joined Everest Insurance, a unit of Hamilton, Bermuda-based Everest Re Group Ltd., from Chubb Ltd. in the newly created role of vice president and deputy chief underwriting officer for North America. Based in Liberty Corner, New Jersey, he was Chubb's senior vice president of corporate underwriting.

Port-a-potty firm sued over smells

Several homeowners in Pacific, Washington, are suing a nearby business that cleans and stores portable toilets over smells in the neighborhood, KOMO News reported.

Northwest Cascade Inc., a 50-year-old enterprise, used to be a small sewage treatment facility until a few years ago, when the owners expanded the business to include bathrooms, the station reported

"The smells literally come in, engulf your home, engulf your area, engulf everything. Literally make you physically sick on a regular basis," Samantha Niemi, one of four plaintiffs, told KOMO just before a judge certified the class action lawsuit. "It was morning, noon, and night ... You were literally having to vacate your home."

Company leaders stated they take odor mitigation seriously, per court documents accessed by KOMO News.

Banana firm slips Kmart a lawsuit

The ever-popular, rarely serious yellow banana costume has become a legal flashpoint.

Silvertop Associates, a costume manufacturer that does business as Rasta Imposta, sued Kmart Corp. in a New Jersey federal court, alleging copyright infringement, trade dress infringement and unfair competition, the Chicago Tribune reported.

Rasta Imposta has sold the costume in Kmart stores since 2008, but this year Kmart said it would use another banana costume vendor, says the complaint, accessed by the Tribune.

"Shortly thereafter, Rasta Imposta discovered that Kmart had begun offering ... a direct replication and knockoff of Rasta Imposta's copyrighted Banana Design," the complaint says. Rasta Imposta gained a copyright registration in 2010, the Tribune reported.

NEWS STATION TAKES DAMAGED TV CLAIM VERY SERIOUSLY

Call it the power of the microphone and camera.

A reporter with NBC7 In San Diego proved to have that special touch — the risk of bad publicity — in helping a man in Escondido, California, collect insurance money he said he was owed when a UPS store near his previous home in Illinois failed to properly pack his television set, which arrived damaged in his relocation west.

Noel Rodriguez said he brought his TV and a UPS-purchased box into his local UPS store in Illinois, claiming he told the clerk there that the TV was wrapped in plastic with an added layer of bubble wrap but "knew it wasn't going to be enough" so he enlisted the help of the store to repackage it, according to the news station report.

Mr. Noel told a reporter that a UPS employee added some popcorn inside and sealed the box, charging him for the shipping and insurance for up to $1,000.

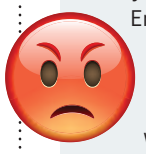
"I was excited, I finally got some TV," Mr. Noel told the reporter. "Opened the box and it was destroyed."

He thought the damage would be taken care of so he filed an insurance claim — but not so, as UPS marked the shipment "self-packed," the station reported. "They denied the claim because I used inferior bubble wrap, non-UPS bubble wrap," Mr. Noel told a reporter.

Mr. Noel then asked NBC 7 Responds, a news segment that helps consumers solve problems, to help him get his insurance money. A spokesperson for UPS responded quickly with a statement: "According to the store they say that they sold the box to Mr. Rodriguez but he supplied his own packing materials and packed the box himself at The UPS Store location ... When an item is self-packed the responsibility falls on the shipper/customer to ensure UPS packaging guidelines are followed in order to make the shipment eligible for declared value coverage."

And yet UPS agreed to pay Mr. Noel $1,000 for his TV and refund what he had paid to ship the package, according to NBC7.

Cue angry face: Apple animoji suit



Apple Inc. is facing a lawsuit over the face-recognition, expression animoji feature set to be introduced with the iPhone X.

Tokyo-based software company Emonster k.k. filed its suit in federal court in San Francisco claiming it holds the U.S. trademark on the term animoji, which Apple is marketing as an upcoming feature that will allow users to animate the facial expressions of emojis using facial recognition technology, according to Reuters.

An Apple spokesman declined to comment.

Phil Schiller, Apple's chief marketing officer, introduced the animoji feature during the iPhone X launch event on Sept. 12, calling it a "great experience" for communicating with family and friends, according to Reuters. In 2014, Emonster Chief Executive Enrique Bonansea introduced an animated texting app, Animoji, and registered a trademark on the product name, according to the lawsuit.

Freeway nails likely to puncture insurer

How many insurance claims will emerge out of an incident where a massive load of nails spilled onto a busy freeway just outside of New Orleans during a busy afternoon rush?

WWL-TV reported that in the days following the incident, drivers were still finding nails in their tires from the spill on Interstate 10 and that authorities are expecting an onslaught of insurance claims to be filed for tire blowouts and more.

Louisiana State Police told reporters the nails fell out of a flatbed trailer being pulled by a truck registered with OCL Transportation. Police Trooper Melissa Matey told the TV station she doesn't have an estimate of how many cars ran over the nails, but she expects several insurance claims will be filed with the insurer, Hallmark Specialty Insurance Co.

BUSINESS INSURANCE®

2018 EVENTS CALENDAR

BUSINESS INSURANCE WORLD CAPTIVE FORUM

World Captive Forum | **January 31 - February 2**
Fort Lauderdale Marriott Harbor Beach Resort & Spa, Florida | Businessinsurance.com/conference/WCF

Retail, Restaurant & Hospitality Conference* | **February 7-9**
Renaissance Dallas Hotel, Texas | BusinessInsurance.com/conference/RRH

Workers Compensation Conference* | **May 22-24**
Westin Chicago River North | BusinessInsurance.com/conference/WC

BUSINESS INSURANCE BREAK OUT AWARDS

Break Out Awards | **June 2018**
Regional events | BusinessInsurance.com/conference/BreakOut

Construction Conference* | **September 26-28**
Chicago Marriott Downtown Magnificent Mile | BusinessInsurance.com/conference/Construction

BUSINESS INSURANCE DIVERSITY+ INCLUSION INSTITUTE

Diversity & Inclusion Institute | **Dates TBD**
Regional events | Businessinsurance.com/conference/diversityinclusion

Risk Management Roundtable | **October 10**
New York | BusinessInsurance.com/conference/RMR

BUSINESS INSURANCE INNOVATION AWARDS

Innovation Awards | **October 10**
New York | BusinessInsurance.com/conference/Innovation

Cyber Summit* | **October 10-11**
New York | BusinessInsurance.com/conference/Cyber

BUSINESS INSURANCE + CLM WOMEN TO WATCH

Women to Watch Conference & Awards EMEA* | **November 15-16**
London | BusinessInsurance.com/conference/WomentoWatchEMEA

Women to Watch Conference & Awards* | **December 13-14**
New York | BusinessInsurance.com/conference/WomentoWatch

*CLM partnered event

ATTEND & LEARN MORE:
businessinsurance.com/events

Sponsorship Opportunities
Jeremy Campbell | jcampbell@businessinsurance.com

Speaking Opportunities
Joanne Wojcik | jwojcik@businessinsurance.com

BETTER UNDERSTOOD

BETTER PROTECTED™

Tailored coverage as unique as your business.

As the ***#1 preferred business insurer,****** we listen carefully to your unique needs and tailor coverage and services to fit them. To learn more, talk to your broker or visit libertymutualgroup.com/businessprotected.

Liberty Mutual INSURANCE

Commercial Auto | General Liability | Property | Workers Compensation

*Based on 2016 survey of business insurance buyers on preference of national carriers sold via independent agents.