MENTAL HEALTH: Comp sector faces rising PTSD claims amid legislative pressures - PAGE 4

BUSINESS INSURANCE®

www.businessinsurance.com

MARCH 2024

SPECIAL REPORT

CYBER INSURANCE

PAGE 18

GREEN COVERAGE LAGS DEMAND

Risk managers seek recognition from insurers for eco-friendly buildings

PAGE 14

COVER STORY

Businesses that invest in more sustainable materials and technologies are not yet seeing the benefits reflected in the cost of their insurance programs, brokers and risk managers say. In some cases, adding green features to buildings may make them more difficult to insure. **PAGE 14**

INSIDE

SPECIAL REPORT: CYBER INSURANCE

A resurgent threat environment and rising claims activity could cause a rebound in cyber liability pricing this year, experts say. Meanwhile, there's growing concern about cybercriminals' use of artificial intelligence. **PAGE 18**

NEWS ANALYSIS

FOR BREAKING NEWS COVERAGE, VISIT **businessinsurance.com**

PTSD PRESUMPTIONS

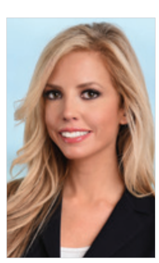
There's a push at the state level to expand post-traumatic stress disorder workers comp presumptions. **PAGE 4**

SECURITIES CLASS ACTIONS

The proposed settlement of two securities cases against Google raises insurance coverage questions. **PAGE 10**

INTERNATIONAL

The nonlife market in Cuba is underdeveloped, comprising just two state-controlled insurers. **PAGE 11**



PERSPECTIVES

The best brokers understand clients' unique cyber risk profiles, write Andrea DeField and Kevin Small of Hunton Andrews Kurth. **PAGE 22**

LEGAL BRIEFS

Recent court opinions **PAGE 12**

OPINIONS

PTSD presumptions warrant scrutiny; cyber risks escalate **PAGE 27**

MARKET PULSE

Products, deals and more **PAGE 28**

PEOPLE

Insurance industry moves **PAGE 29**

OFF BEAT

A golf club maker calls big box retailer Costco out of bounds with its Kirkland Signature irons. **PAGE 30**

VIEW FROM THE TOP

MIKE RICE

Mike Rice joined CAC Specialty at its creation in 2019. Leading the brokerage's drive into D&O and various other specialty insurance lines, the former JLT Specialty and Aon executive is now CEO of CAC Group. Denver-based Mr. Rice discusses CAC's aggressive growth since its founding, how and where it will seek to expand in the future and a possible solution to the ongoing issue of noncompete-related litigation in the U.S. insurance industry. **PAGE 13**

BUSINESS INSURANCE (ISSN 0007-6864) Vol. 58, No. 3, Copyright © 2024 by Business Insurance Holdings, Inc. is published monthly by Business Insurance Holdings, Inc., 1030 Lake Avenue, Greenwich, CT 06831. Accounting, business, circulation and editorial offices: PO Box 1010, Greenwich, CT 06836. Email businessinsurance@omeda.com to subscribe or for customer service. Periodicals postage is paid at Greenwich, CT. Printed in the USA. **POSTMASTER:** Send address changes to Business Insurance, PO Box 260, Lincolnshire, IL 60669.

NEWS ANALYSIS

Rising PTSD claims, wider comp liabilities spotlight importance of treatment guidelines

BY LOUISE ESOLA
lesola@businessinsurance.com

Post-traumatic stress disorder is a commonly misunderstood mental illness that is increasingly a component of workers compensation claims, raising concerns over how to navigate and close the often complex claims.

Mental health experts say that adherence to guidelines for the diagnosis and treatment of PTSD is essential when treating affected workers.

"The prognosis for well-treated PTSD is actually quite good," said Les Kertay, Chattanooga, Tennessee-based behavioral health medical director for Genex Services, an Enlyte LLC company. "People tend to recover."

State lawmakers have repeatedly sought to expand or introduce presumption laws that would make PTSD a compensable illness for some occupations allowing for more so-called mental-mental claims, or mental claims that result from a psychological event.

The push to expand workers comp into the mental health arena has mostly related to first responders, but there's a growing interest in broadening eligibility for all workers (see related story).

The workers comp industry has generally been wary of accepting mental injury claims (see related story).

Reference to the universally accepted checklist in the Diagnostic and Statistical Manual of Mental Disorders, Fifth Edition, is necessary to make a PTSD diagnosis, experts say.

Most checklists start with the question of whether a person experienced a tragic event. Most PTSD presumption laws and proposals mention the DSM-5 and refer to experience of tragedy as a bar for accepting claims.

> "The prognosis for well-treated PTSD is actually quite good. People tend to recover."
>
> Les Kertay, Genex Services

"The No. 1 criterion in the DSM for PTSD is that the individual must have experienced or witnessed traumatic death or serious injury," said Ron Heredia, a psychologist and founder and director of Los Angeles-based Good Mood Legal, which specializes in reviewing psychological evaluations in insurance claims.

After that determination is made, assessors should look at symptoms such as debilitating anxiety, nightmares and flashbacks, said Dr. Elspeth Cameron Ritchie, Washington-based chair of psychiatry at

Workers comp industry cautious in accepting mental health injuries

Historically, the workers compensation industry has sought to avoid mental injury claims, fearing that the subjectivity surrounding the diagnosis of conditions such as post-traumatic stress disorder would result in workers falsifying claims, exaggerating injuries or malingering for financial gain, experts say.

"PTSD has always been a controversial diagnosis," said Dr. Elspeth Cameron Ritchie, Washington-based chair of psychiatry at MedStar Washington Hospital Center.

She cites several reasons: The criteria for PTSD have changed over time; the diagnosis is often misused by claimants; and some of the characteristics of the disorder can be mistaken for other conditions, as the symptoms can overlap.

The expense of treating mental injuries is also a significant concern — most opponents of expanding mental claims in workers comp say unknown costs comprise the top issue. There's also a well-documented shortage of qualified mental health practitioners to diagnose and treat PTSD.

> "Employers don't like PTSD or mental claims. They're inherently subjective. You can't point to an MRI … and say the person has this problem."
>
> Brad Young, Harris Dowell Fisher & Young

"Employers don't like PTSD or mental claims," said Brad Young, St. Louis-based member at Harris Dowell Fisher & Young LC, which represents employers. "They're inherently subjective. You can't point to a test. You can't point to an MRI … and say the person has this problem."

Mr. Young noted that prior stressors and mental issues can be at work.

"They may have had other trauma in their life," he said. "When you have a mental injury on the job, that mental injury that's being treated is not just for that injury, but it's also encompassing all of the prior stressors."

So-called mental-mental claims are those caused by a mental stimulus — such as something a person experienced — and result in a mental injury. A physical-mental claim is precipitated by a physical injury. States vary on how claims are accepted, with most states strictly prohibiting mental-mental claims, but that is slowly changing.

Les Kertay, Chattanooga, Tennessee-based behavioral health medical director for Genex Services, an Enlyte LLC company, said the expansion of presumptions is "problematic" because they imply that all people who experience trauma will develop a potentially long-term mental condition.

"We have all experienced at least one (traumatic) event by the time we are 40 years old," he said, referring to what many existing and proposed presumptions list as qualifying events for eligibility. But he cautions insurers and employers to not dismiss the claims without careful review.

"You don't want to turn it into a battle," Dr. Kertay said. "If somebody has an event, they do meet the criteria, they actually have PTSD, and they're being treated, don't turn it into a fight. Don't turn it into an adversarial relationship because that just makes people dig in further. It's a real thing; it really does happen."

Louise Esola

PTSD HITS A SMALL MINORITY

Most people who go through a traumatic event will not develop post-traumatic stress disorder. About 6% of the U.S. population will have PTSD at some point in their lives.

- About **5% of adults in the U.S.** have PTSD in any given year. In 2020, about 13 million people in the U.S. had PTSD.
- **Women are more likely** to develop PTSD than men. This is in part due to the types of traumatic events that women are more likely to experience — such as sexual assault — compared with men. About 8% of women and 4% of men will have PTSD at some point in their life.
- **Military veterans are more likely** to have PTSD than civilians. Veterans who deployed to a war zone are also more likely to have PTSD than those who did not deploy.

Source: The National Center for PTSD

MedStar Washington Hospital Center, who spent part of her career as a U.S. Army doctor treating veterans with PTSD.

Under the DSM-5 checklist, a person needs to have a certain number of symptoms over a long period to receive a PTSD diagnosis and the symptoms should not be confused with temporary discomfort after a traumatic event, Dr. Cameron Ritchie said. A key distinguisher is seeing, smelling or hearing triggers that ignite PTSD symptoms, she said.

PTSD may not show up immediately, Dr. Cameron Ritchie said, recalling working in South Korea with veterans who had served during the Vietnam War and began experiencing PTSD symptoms years later.

"Korea is an Asian country that has many of the same sights and smells … which brought them back to Vietnam. Some of them had been symptom-free for 20 years and then they started to develop some symptoms, and those symptoms are normally the flashbacks and the nightmares."

David Faust, professor emeritus in the Department of Psychology, Clinical Psychology, at the University of Rhode Island in Kingston, Rhode Island, called PTSD "a condition of suffering."

"Some of the symptoms, for example, include intense anxiety and hyper vigilance — that is, looking around you everywhere for something that might be threatening and so on," he said. "That can cause significant disruptions and affect focus and concentration, (which) can lead to errors on the job or just intolerable levels of discomfort."

Experts say PTSD is treatable and most sufferers get better. They point to such treatments as talk therapy, medications and emerging methodologies — technological developments have helped PTSD patients in recent years, for example — as best practices.

"It's going to depend on the person and how resilient they are," Dr. Cameron Ritchie said, adding that preparation is also key. "How prepared they were for the stressor counts. For example, if you're in the Army, you go to basic training and you get a lot of preparation; you know you're going into war."

Recovery is possible and very likely, but sometimes PTSD is in "remission" and can reoccur with triggers, Mr. Heredia said. "It's different for everybody," he said, adding that adherence to guidelines and documenting progress are vital, especially for workers comp patients.

> "The individual must have experienced or witnessed traumatic death or serious injury."
>
> Ron Heredia, Good Mood Legal

Mr. Faust said that "getting better means improving, and there are plenty of people with PTSD who can work, and it depends a lot on the nature of the job. With all the caveats … most workers want to get back to work."

STATES CONTINUE EFFORTS TO EXPAND PTSD ELIGIBILITY TO MORE WORKERS

Three months into 2024 and the years-long trend to expand, amend or introduce legislation involving post-traumatic stress disorder and other mental injuries as occupational diseases continues.

More than a dozen new and revived bills have been filed for consideration this year. Some call for new presumptions or add types of workers that would qualify; some deal with diagnoses and treatments for mental injuries; and some offer new parameters for qualifying for benefits.

As examples:

- Colorado lawmakers are considering a bill that would authorize benefits for all workers who are repeatedly exposed to trauma.
- Arizona and Virginia lawmakers have introduced bills that would expand presumptions to include emergency dispatchers.
- West Virginia lawmakers are considering a bill that would expand which professionals can diagnose a first responder with PTSD.
- Kentucky lawmakers are considering amendments that would make off-duty work compensable for PTSD.

"There's a lot of expansion in the presumption space," said Brian Allen, Salt Lake City-based vice president of government affairs for Enlyte LLC, which provides workers compensation services.

This year looks much like 2023 in terms of the wave of bills introduced, according to annual analyses by the National Council on Compensation Insurance in Boca Raton, Florida. Last year's results were mixed, with most bills introduced failing to gain traction. In 2022, only three states enacted changes after more than 60 bills were introduced, according to two analyses by NCCI.

In 2023, the trend of expanding PTSD presumptions beyond first responders was successful in two states: Connecticut now allows all workers who witness harrowing events to qualify for PTSD presumption, and Washington allows nurses the same benefits as first responders.

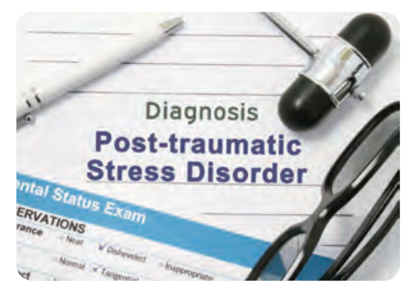
The costs of implementing presumptions are unknown as data is limited, experts say.

A spokeswoman for the NCCI wrote in an email that "first responders are typically employed by municipalities who are often self-insured and therefore are not required to report data to NCCI. … This limits the amount of information available to NCCI since this population of employees may represent a greater proportion of work-related PTSD claims."

Aiming to take the issue out of the workers compensation system, where the industry is wary of the unknown costs, lawmakers in Georgia, Indiana and Mississippi have introduced bills that would create programs for first responders suffering from PTSD that include such parameters as benefit limits and treatment options.

John Hanson, Atlanta-based vice president at Alliant Insurance Services Inc., said the Georgia bill to create an alternative program for first responders with PTSD is in response to the unknown costs associated with keeping the claims in the workers comp system.

California and Minnesota have reported high volumes of claims of PTSD that typically include frictional costs such as litigation associated with claim acceptance, he said.



"All of the costs associated with investigation, with litigation or arbitration are growing very quickly as opposed to just the claim costs," said Mr. Hanson, who supports the Georgia bill.

Steven A. Bennett, vice president of workers compensation programs and counsel for the Washington-based American Property Casualty Insurance Association, said the industry needs strict standards for claiming PTSD.

"Mental injuries are subjective. … It's unclear whether this injury is due to work or due to something in the person's private life or something hereditary," he said. "That's why mental claims are problematic."

APCIA advocates for changes to presumptions so that they "have limitations on the scope of employment on the type of situations recoverable," and, for proof of mental illness, "we would like a clear and convincing standard, and we would want it to be for very specific, egregious circumstances," Mr. Bennett said.

Florida, for example, in 2019 modified its PTSD presumption for first responders to require that the worker witness a so-called "qualifying event" to receive care and income benefits. That change went into effect one year after the state passed the original presumption bill.

Louise Esola

Exposure growth drives costly storm losses

BY MATTHEW LERNER
mlerner@businessinsurance.com

Rising insured losses caused by severe convective storms can largely be traced to substantial expansion in exposure values in affected geographies rather than significant meteorological shifts, experts say.

The tornadoes, hailstorms and high winds produced by such storms are tearing through areas with higher insured values as a result of several factors, including population expansion and inflation.

Losses due to severe convective storms have been driving annual catastrophe losses for several years, and 2023 marked the first time insured natural catastrophe losses topped $100 billion without a single, larger event driving the total.

Global insured losses from natural catastrophes totaled an estimated $123 billion in 2023, according to a report from Gallagher Re, the reinsurance brokerage of Arthur J. Gallagher & Co. Severe convective storm losses accounted for about 58%, or $71 billion, of the total, with $60 billion of the losses arising from claims in the United States, where six of the year's top 10 costliest insured events were severe convective storm events.

"There's just more of an expanding target of exposure, meaning more people and stuff that's in harm's way that can be affected by these events," said Steve Bowen, Chicago-based chief science officer with Gallagher Re.

Nine of the nation's 15 fastest-growing cities in 2022 were in the South, according to the U.S. Census Bureau. Six of those are in Texas, with Georgetown having the highest rate of growth among all U.S. cities and towns with at least 50,000 people.

"Severe convective storms are relatively small-scale events. The size of SCS losses therefore depends quite a bit on the density of exposed value in the area affected by SCS," said Elisabeth Viktor, Zurich-based senior natural catastrophe specialist for Swiss Re Ltd.

"The expansion of urban areas, especially in regions prone to SCS, such as Texas, is certainly a driving factor of the increase of insured SCS losses we've seen in recent years," Ms. Viktor said.

Homeowners are seeing the impact from North Carolina, where the North Carolina Rate Bureau filed a request with the state insurance department for an average 42.2% increase in homeowners insurance rates, to Oklahoma, where policyholders are seeing double-digit property insurance increases and the nation's tallest structure, at some 1,900 feet, has recently been proposed for Oklahoma City. The North Carolina Rate Bureau request was rejected by North Carolina Insurance Commissioner Mike Causey on Feb 6.

Michal Lörinc, head of catastrophe insight in Prague for Impact Forecasting, a unit of Aon PLC, said some data suggests that up to 80% of the increase in insured losses from severe convective storms is due primarily to factors such as increasing population exposure and inflation driving up the cost to repair or replace structures due to increased costs of materials, labor and transportation, among other things.

While much of this increased loss activity is occurring in the U.S., Mr. Lörinc said Europe is seeing some similar dynamics. He noted that Italy sustained a major loss event from severe convective storms in 2023.

"Certainly, the population has grown in the interior part of the U.S. and also the southeast," said Gregory Mann, Atlanta-based U.S. property placement leader for Marsh LLC.

Inflation has also played a role, Mr. Mann said. "As far as what a loss was five years ago, it has certainly increased dramatically to what it is today," he said.

"The individual size of a loss has been increasing, caused by, among other things, more valuable buildings and a rise in material costs," Ms. Viktor said.

Insurers have reduced limits, as they practice "capital management" to avoid larger concentrations of risk on their books, Mr. Mann said. A policyholder might still be able to secure desired limits in the marketplace but might have to build the tower with capacity from several insurers instead of a single, large limit from one, he said.

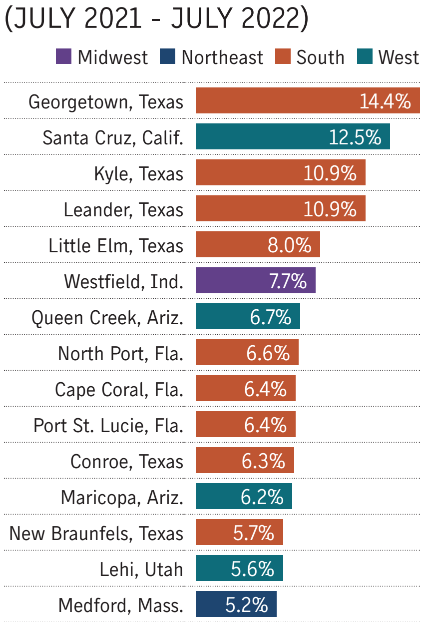
"Each of them brings a minimum premium and a minimum fixed cost … so that adds overall cost to the program," he said.

"There's essentially more targets that are now vulnerable to those natural hazards" such as severe convective storms, said Sarah Dillingham, Atlanta-based senior director of meteorology for the Insurance Institute for Business & Home Safety, an independent, nonprofit research organization supported by the insurance industry.

In addition, the resilience of buildings varies due to the labyrinth of building codes and enforcement at the state and local levels. "In places like the Southeast and Ohio Valley … we see some vulnerable housing, and that has to do with the building code environments and potentially local construction practices," Ms. Dillingham said.

The IBHS does substantial research on roof tiles' hail resiliency, as well as tile and metal roofs, and is expanding that research to exterior wall coverings, Ms. Dillingham said. More defensive roofing materials may cost more but show evidence of added resilience.

15 FASTEST-GROWING LARGE CITIES IN THE U.S.
(JULY 2021 - JULY 2022)



Note: "Large cities" were those with populations of 50,000 or more on July 1, 2021.
Source: U.S. Census Bureau

MORE DENSELY POPULATED AREAS AT RISK AS TORNADO ALLEY SHIFTS EAST

Although the principal driver behind the rising insured losses due to severe convective storms is increasing exposure values, evidence suggests that the most commonly affected region may have expanded eastward.

Commonly called "tornado alley," the region previously largely comprised sparsely populated areas of the U.S., but an eastward shift would be toward more populous areas with greater exposure values.

"There are indications that the region of high SCS activity could be moving towards the east and southeast of the U.S. With this potential shift, it could become more likely for SCS events to affect regions that are more densely populated and generally less prepared to withstand such events," said Elisabeth Viktor, Zurich-based senior natural catastrophe specialist for Swiss Re Ltd.

From 1950 to 1980, large outbreaks of tornadoes occurred most often in the region encompassing northern Texas, eastern Oklahoma and Western Arkansas and Missouri, according to a recent paper in Scientific American. Between 1989 and 2019 the locus shifted eastward, covering western Kentucky and Tennessee, plus northern Mississippi and Alabama, it said.

"We have noticed that the areas in which things occur is expanding eastward — we're seeing an increasing frequency in places east of the Mississippi like the Southeast and Ohio Valley," said Sarah Dillingham, Atlanta-based senior director of meteorology for the Insurance Institute for Business & Home Safety, an independent, nonprofit research organization supported by the insurance industry.

Matthew Lerner

DOL rule set to broaden liability for employers

BY JON CAMPISI
jcampisi@businessinsurance.com

A U.S. Department of Labor rule that takes effect this month may result in more contract workers being classified as employees, potentially requiring employers to provide benefits and insurance coverage such as workers compensation and possibly exposing them to employment-related lawsuits.

The Employee or Independent Contractor Classification Under the Fair Labor Standards Act rule, which was finalized Jan. 10 and rescinds a Trump administration rule, covers employment classification under the FLSA, but employers worry it might have broader influence.

Government officials say the rule provides a clearer analysis for employers to use to determine a worker's employment status. It re-adopts an enhanced economic realities test for worker classification that was in effect under an Obama administration rule.

The new rule contains a six-factor test to guide employers in determining a worker's employment status under the FLSA (see box), whereas the Trump administration rule had a two-factor test.

The Labor Department says misclassification of employees as contractors may deny workers a minimum wage, overtime pay and other protections.

Some experts say the change is narrowly tailored and limited in scope, a view shared by the Labor Department.

"The rule is how the Department of Labor is going to interpret who is an employee under the Fair Labor Standards Act," said Todd Lebowitz, an attorney with Cleveland-based Baker & Hostetler LLP who represents employers. "So, one agency, one law."

One group that came out in support of the new rule is the National Electrical Contractors Association, which said the change is a win for its member contractors because it would address the "rampant misclassification across industries, particularly the construction sector."

But others are concerned the change may have consequences beyond just minimum wage and overtime pay protections.

"Once you're an employee for wage and hour reasons then I think everything else just starts to morph into the rule," said Robert Boonin, a labor and employment attorney with Ann Arbor, Michigan-based Dykema Gossett PLLC.

The rule faces court challenges, but if it proceeds, certain workers would be considered employees for wage and hour purposes, a change that some labor unions and others support.

App-based gig workers, though, may prefer to remain independent contractors, some business advocates say.

Karolis Kavolelis/Shutterstock

"The concern if gig workers were suddenly reclassified would be that there would be fewer opportunities and less flexibility, which we know that they value," said Ruth Whittaker, director of civic innovation policy for the Washington-based Chamber of Progress, a technology trade association.

Possible confusion could result if workers are classified as independent contractors under one statute and as employees under another, said Alex MacDonald, a shareholder with Washington-based law firm Littler Mendelson P.C. and a core member of the Workplace Policy Institute, a division of the firm.

"It gets very confusing very quickly, and it is even different from state to state and within a state," Mr. MacDonald said. "So, there's like a Byzantine web of classification tests."

This confusion, experts say, could lead to more employment-related litigation.

Mr. MacDonald is lead attorney in *Coalition for Workforce Innovation et al. v. Walsh et al.*, one of the lawsuits challenging the rule.

The suit, which is pending in the Eastern District of Texas and targets procedural issues associated with the law, was filed by various groups, including an organization representing independent workers, small businesses, start-ups, entrepreneurs and technology companies.

Advocates of the new rule say many workers themselves pushed for reclassification. Some say the federal rule was inspired by California Assembly Bill 5, which was passed in 2019 and created a new test for determining employee classification (see related story).

Those who pushed for AB 5 to become law included labor unions and legislators who voiced concern that independent workers were being deprived of employment protections such as overtime pay and sick leave.

Matthew Estipona, director of government affairs and community engagement for the Northern California chapter of the Associated Builders and Contractors, said if the federal Labor Department rule proceeds, it may lead to more confusion and potentially expensive litigation as employers navigate how to determine employee status. He said that has been the effect of the California law.

"The final rule will jeopardize the ability of construction firms to continue the industry's longstanding practice of utilizing legitimate independent contractors," Mr. Estipona said. "Under the rule's multifactor test, employers will now be forced to guess which factors should be given the greatest weight in making the determination."

Some experts said the DOL rule will have employers rethinking insurance coverage.

"There may be more confusion about whether certain claims are covered by a policy that the employer has or whether employers would consider getting additional coverage," said Bill Kennedy, a partner with Philadelphia-based Montgomery McCracken Walker & Rhoads LLP.

Experts say companies may consider adding employment practices liability insurance or directors and officers liability insurance.

SIX FACTORS

The new U.S. Department of Labor rule designed to provide employers with enhanced guidance when determining employee classification is slated to take effect this month.

The rule applies six factors to determine worker status:

- Opportunity for profit or loss depending on managerial skill
- Investments by the worker and potential employer
- Degree of permanence of the work relationship
- Nature and degree of control
- Extent to which work performed is an integral part of the business
- Skill and initiative

Source: U.S. Labor Department

CALIFORNIA LAW PAVED WAY FOR FEDERAL CHANGE

In 2019, California Gov. Gavin Newsom signed into law Assembly Bill 5, which created a new test for employers to determine whether workers should be classified as employees or independent contractors.

As the U.S. Department of Labor prepares to implement a similar rule at the federal level, opponents are pointing to the impact of the California law.

Matthew Estipona, director of government affairs and community engagement for the Northern California chapter of the Associated Builders and Contractors, said the law has led to a drop in employment.

Mr. Estipona cited a January study from the Mercatus Center at George Mason University in Arlington, Virginia, that found California self-employment fell by 10.5% and overall employment dropped by 4.4% following the passage of AB 5.

The study, however, noted that a drop in employment due to the pandemic could also be taken into consideration.

Alex MacDonald, a shareholder with Washington-based law firm Littler Mendelson P.C. and a core member of the Workplace Policy Institute, a division of the firm, said the belief that employment would rise as companies classify more workers as employees is a "reductive way to think about it."

"If businesses stop using contractors, that reduces overall economic activity, which could affect the number of traditional employee jobs in that industry," he said.

Fallout from California's AB 5 passage has included lawsuits by the trucking industry, which claims the law represents a huge cost burden for employers forced to cover independent drivers with workers compensation insurance, and by the ride-sharing industry, which contends the law has negatively affected its business.

In December, the U.S. Court of Appeals for the Ninth Circuit agreed to rehear a case by Uber Technologies Inc. seeking to overturn a judge's dismissal of the company's challenge to AB 5.

Jon Campisi

NEWS ANALYSIS

Google class-action settlement shines light on D&O exposures, cyber liability coverage

BY SHANE DILWORTH
sdilworth@businessinsurance.com

achinthamb/Shutterstock

The recent $350 million preliminary settlement of two securities class actions resulting from a cyber incident involving the Google+ social media platform raises questions as to which insurance policies might cover such payments, legal experts say.

Companies should review their cyber and directors and officers liability policies as case law builds around cyber breaches and regulators increase scrutiny of companies' responses to the attacks, they say.

The resolution of *In re Alphabet Inc. Securities Litigation* last month could trigger coverage provided by D&O and cyber liability policies, experts say, since the underlying securities class actions potentially fall under each type of insuring agreement.

"This matter concerns a product that no longer exists, and we are pleased to have it resolved," a Google spokesperson said in an email.

> "The underlying securities class actions seem to be the very kind of suits that hit the core of what D&O policies are intended to cover."
>
> Peter Halprin,
> Haynes Boone LLP

The spokesperson said the company regularly identifies and fixes software issues, discloses information about them and takes the issues seriously.

Representatives for the plaintiffs did not respond to requests for comment.

Alphabet, the Mountain View, California-based technology company that owns Google, was named in two securities class actions after a 2018 Wall Street Journal article revealed the company's knowledge of a software bug that allowed developers unauthorized access to some users' data. According to the article, the company knew about the bug in its now defunct Google+ platform as far back as 2015 but did not disclose information about the breach to investors or government regulators.

Shareholders lodged securities class actions against Alphabet and individual directors and officers in federal courts in New York and California in October 2018. The cases were later consolidated.

A lower-court judge dismissed the case in February 2020, but the 9th U.S. Circuit Court of Appeals in San Francisco partially revived the case in June 2021 after finding that some of the statements in Alphabet's filings were misleading.

The parties began settlement negotiations after the suits were returned to the trial court. A preliminary settlement agreement was filed Feb. 5.

The proposed settlement raises questions over insurance coverage for such cases, according to several legal experts who were not involved in the dispute.

Peter Halprin, a New York-based insurance recovery partner at Haynes Boone LLP, said a D&O policy should clearly provide coverage for settlement of the securities class actions.

"The underlying securities class actions seem to be the very kind of suits that hit the core of what D&O policies are intended to cover," he said. "The core of D&O coverage is for securities claims that seek to hold a corporation and its directors and officers responsible for fluctuations in market value due to perceived issues with reporting and disclosures."

The allegations in the underlying class actions concerning the failure to disclose the software glitch are an important concern for companies that suffer a breach because the U.S. Securities and Exchange Commission has recently increased scrutiny of when and how a company must inform the public and regulators about data breaches, hacks and other cyber events, Mr. Halprin said.

"Any publicly traded company that faces the risk of some kind of securities-related lawsuit needs to pay attention to these developments," he said. "Insurers are certainly paying attention to these developments, and the government is closely monitoring compliance with the SEC's guidance and regulations. So, it's going to be really important for businesses, brokers, insurers and everyone in this space to really stay on top of these changes."

> "It's imperative for public companies to make sure that their insurance is going to respond to these types of incidents, whether it's a D&O policy, a cyber policy, or both."
>
> Michael Savett,
> Butler Weihmuller Katz Craig LLP

Ideally, D&O and cyber policies "would be seamless together," however, insurers have started broadening cyber exclusions in D&O policies, said Meghan C. Moore, a shareholder at Flaster Greenberg P.C. who represents policyholders.

A cyber policy may cover claims arising from the breach but may not provide coverage to the individual directors and officers, she said.

Cyber policies typically have securities law violation exclusions that would not provide coverage for settlements such as Alphabet's, said Matthew Bricker, an Austin, Texas-based partner at TittmannWeix LLP, who represents insurers.

In addition, allegations of intentional conduct in the underlying securities class actions could give rise to insurance coverage issues because most policies have intentional acts exclusions, he said.

Section 533 of California's insurance code provides that an insurer is not liable for loss caused by a willful act of the insured.

While D&O policies typically cover securities suits, "given the defendants expressly denied any wrongdoing in the settlement agreement, coverage would depend on the policy wording," Mr. Bricker said.

The proposed settlement highlights the importance of having sufficient coverage for D&O exposures related to disclosing and reporting data privacy breaches and cyberattacks, said Michael Savett, a Philadelphia-based partner at Butler Weihmuller Katz Craig LLP who represents insurers.

Some D&O policies carve out coverage for cyber events, while some cyber policies do not extend coverage to directors and officers.

"It's imperative for public companies to make sure that their insurance is going to respond to these types of incidents, whether it's a D&O policy, a cyber policy, or both," Mr. Savett said.

"From an industry standpoint, it's incumbent upon carriers and underwriters to get as much information on the company's data privacy practices and cybersecurity practices before issuing policies."

Mr. Halprin of Haynes Boone said there is a lesson to be learned for both insurers and policyholders from the proposed settlement.

"This is a clear wakeup call that it is really important to analyze D&O exposures, including privacy and cyber-related D&O exposures, and to work with brokers and insurers to ensure robust coverage, because the financial implications of these kinds of suits are very significant," he said.

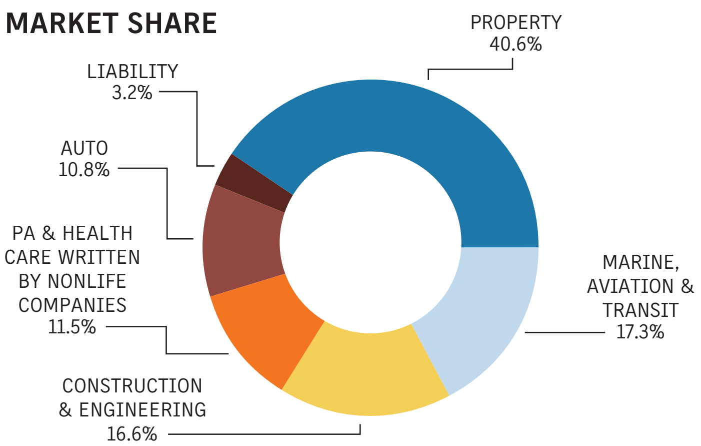
PROFILE: CUBA

125

GLOBAL P/C MARKET RANKING

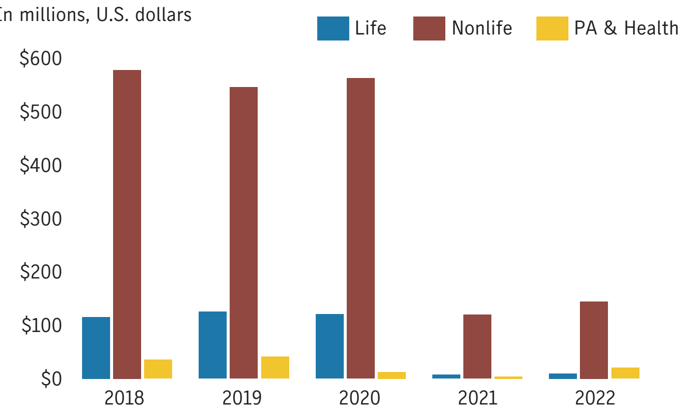
The nonlife market in Cuba is traditional and underdeveloped, comprising just two insurers — both ultimately state-owned — offering relatively standard products and operating almost entirely in different market segments. In a society in which the state makes provision for most aspects of life and few segments of the population have disposable income, market concerns center on the need for growth and where it will come from. While windstorm and earthquake exposures may deter some foreign players, and U.S. insurers and reinsurers are currently not allowed to be involved, the market could be seen as attractive in a Caribbean context as the largest in terms of size and population. Although in theory it is open to foreign entrants, and some insurers and intermediaries have reportedly shown an interest, the one firm application made by a Brazilian insurer in 2013 was withdrawn in 2015.

MARKET SHARE



MARKET GROWTH

In millions, U.S. dollars



Source: Axco Global Statistics/Industry Associations and Regulatory Bodies

AREA

42,803

square miles

POPULATION

11

million

MARKET CONCENTRATION

100%

market share of top two insurers

2024 GDP CHANGE (PROJECTED)

N/A

MARKET DEVELOPMENTS

Updated February 2024

- Since November 2020 the Insurance Superintendency of Cuba has been working with existing market players to implement a new state policy for insurance and reinsurance. This involves developing new products in both the nonlife and life sectors, with the overall goal of increasing market penetration and the capacity of insurance to help against natural disasters such as hurricanes or epidemiological ones such as the COVID-19 pandemic. The SSC has approved new nonlife products for agricultural risks, loss of profits and unemployment.
- The local industry continues to be open and amenable to foreign investment, most likely to be approved on a joint-venture basis with existing local insurers. A Brazilian company was said to have expressed interest last year.
- Hurricane Ian, one of the costliest in history mainly because of its impact on the United States, struck western Cuba as a Category 4 storm on Sept. 26, 2022. A leading international reinsurance broker reported five fatalities and economic losses in excess of $500 million. The local nonlife market account reportedly sustained losses of between CUP 90 million and CUP 100 million (around $4 million), excluding agriculture insurance.
- Apart from losses caused by Hurricane Ian, there were two major fires with some impact on the insurance industry in 2022. On May 6, an explosion reportedly caused by a gas leak ruined the luxury Hotel Saratoga in Old Havana, killing 46 people. On Aug. 5, a lightning strike caused a series of explosions in two oil storage units in the supertanker base at Matanzas. Some 17 firefighters were thought to have lost their lives fighting the fires.

COMPULSORY INSURANCE

- Workers compensation (state social security)
- Medical expenses insurance for visitors to Cuba or those temporarily resident
- Property/casualty risks for foreign and mixed investors, and concessionaires or users of the Mariel Special Development Zone
- Auto third-party liability for professional drivers of state and non-state vehicles
- Aviation liability insurance
- Third-party liability for operators of drones

NONADMITTED

Nonadmitted insurance is not permitted in Cuba because the law provides that insurance must be purchased from local authorized insurers, with some exceptions. Unauthorized insurers are not permitted to carry on insurance activity in Cuba.

INTERMEDIARIES

Brokers and agents must be authorized to handle insurance business. Locally registered brokers may not place business with nonadmitted insurers inside or outside the country.

MARKET PRACTICE

Authorization to place business overseas has been granted on several occasions but is an exceptional event. Local insurance companies do not engage in fronting activities.

Keenan faces suit over cyber breach

■ Keenan & Associates, a unit of AssuredPartners Inc., faces a class-action lawsuit on behalf of clients alleging that the brokerage failed to implement sufficient cybersecurity measures and was too slow to disclose a 2022 data breach.

The suit, *Matthew Rutledge, individually and on behalf of all others similarly situated v. Keenan & Associates*, was filed Feb. 2 in U.S. District Court for the Central District of California. It stems from a cyber breach last summer that Keenan notified affected individuals about on Jan. 26.

The breach may have affected more than 1.5 million individuals.

The suit alleges the data breach "was a direct result of Keenan's failure to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect consumers' Private Information."

In addition, "Keenan has acknowledged that the cybersecurity attack occurred at various times between August 21, 2023, and August 27, 2023, but that it waited until January 26, 2024, to begin contacting Class Members," the suit states.

The suit seeks statutory, actual and punitive damages, attorneys fees and costs, and credit-monitoring services, among other things.

Captive manager pleads guilty

■ A Beaufort, South Carolina-based captive manager pleaded guilty to helping a client shield funds from the FBI during a fraud investigation and agreed to pay $2.7 million in restitution in connection with an alleged money laundering scheme.

Peter J. Strauss, founder of Strauss Law Firm LLC and founder and CEO of Hamilton Captive Management, based in Hilton Head, pleaded guilty to removal of property to prevent seizure. He faces a maximum penalty of five years in federal prison and a fine of up to $250,000, the U.S. Attorney's Office for the District of South Carolina said in a statement.

Evidence revealed that Mr. Strauss "knowingly transferred millions of dollars" for Jeff and Paulette Carpoff, who were convicted and sentenced to prison in 2020 and 2022, respectively, in the Eastern District of California for their roles in an investment fraud and money laundering scheme, according to the statement.

The couple had owned and operated DC Solar Solutions Inc. and DC Solar Distribution Inc., now defunct Benicia, California-based solar power companies that were seized by the FBI in 2018.

As the investigation into the couple's businesses unfolded, Mr. Strauss received $11 million from them, according to the statement. Mr. Strauss used the funds to pay various criminal defense attorneys and bankruptcy counsel and transferred funds into a captive insurer operated by the couple, which he also managed.

By pleading guilty, Mr. Strauss admitted that by the time of a $3 million transfer on Jan. 15, 2019, "he knowingly transferred and aided and abetted the transfer of funds from Carpoff to prevent and impair the government's lawful authority to take such property into its custody and control," the statement said.

U.S. District Judge Richard M. Gergel accepted the guilty plea and will sentence Mr. Strauss after receiving and reviewing a sentencing report prepared by the U.S. Probation Office.

Bank wins appeal in Ponzi scheme case

■ An Ohio bank can claim insurance coverage from an American International Group Inc. unit for a settlement it paid to end litigation related to a Ponzi scheme it was caught up in in the early 2000s, a federal appeals court ruled.

In overturning a lower court decision in favor of the unit, the U.S. 6th Circuit Court of Appeals in Cincinnati ruled in *Huntington National Bank v. AIG Specialty Insurance Co. et al.* that Ohio law did not bar the Columbus-based bank's $15 million claim on its bankers professional liability policy.

The claim stemmed from a Ponzi scheme perpetrated by Barton Watson through two fraudulent companies, Cyberco Holdings and Teleservices Group Inc. Huntington served as Cyberco's bank from 2002 to 2004 and extended the company multiple loans, the ruling states.

Mr. Watson set up a web of loans with Teleservices and financing companies purportedly to pay for computer equipment and deposited the money in Cyberco's account with Huntington, court papers say.

Huntington became suspicious of Mr. Watson's banking activity in 2003 and learned from the FBI that he had previously served time for fraud-related crimes. From May 2004 to October 2004, Cyberco gradually repaid its entire loan. Later the FBI raided Cyberco's offices, and Mr. Watson committed suicide shortly afterwards, court papers say.

Creditors of Cyberco and Teleservices discovered the companies were bankrupt, and trustees of the companies claimed Huntington put its desire to be repaid ahead of concerns over Mr. Watson's fraud.

After lengthy bankruptcy proceedings, in 2018 Huntington settled with the trustees for $32 million without admitting liability. At various points during the bankruptcy proceedings, Huntington sought $15 million in coverage under its policy with AIG and the insurer denied the claim.

Huntington sued AIG, and a lower court ruled in the insurer's favor, stating the claim was uninsurable under Ohio law and also barred under a policy exclusion for "unrepaid, unrecoverable, or outstanding credit."

Reviewing the case, the appeals court stated that only two categories of claims are uninsurable under Ohio law: claims for punitive damages and intentional torts.

Nursing assistant can pursue COVID claim

■ An Alabama appellate court ruled that a trial court wrongly dismissed a workers compensation claim filed by a nursing assistant who said she was left permanently disabled after contracting COVID-19 at the nursing home where she worked.

The Court of Civil Appeals ruled the trial judge improperly found that COVID-19 was not compensable under state law when it ruled for the employer, Opp Health and Rehabilitation LLC.

Rena Meeks filed a workers comp claim in May 2021, saying she suffered injuries to her lungs and airway that left her permanently disabled.

The company challenged the claim as non-compensable, and the trial court agreed.

In reversing the decision and remanding the case for further proceedings, the appellate court ruled that Ms. Meeks was entitled to pursue her claim because her job duties exposed her to a "danger or risk materially in excess of that to which people are normally exposed in their everyday lives."

DOCKET

JURY AWARDS $1.7M IN EEOC ADA CASE

A jury in Syracuse, New York, awarded a job applicant $1.7 million in damages following a distribution company's refusal to interview her after it discovered she was deaf. The award against a McLane Co. Inc. unit in a lawsuit brought by U.S. Equal Employment Opportunity Commission comprised $25,000 in back pay, $150,000 in damages for emotional distress and $1.5 million in punitive damages. The EEOC contended the company violated the Americans with Disabilities Act by "failing to interview and failing to ultimately hire" the applicant because of her disability. The applicant applied for two warehouse selector positions at McLane's Baldwinsville, New York, facility in 2018.

AMPUTATION CLAIM IMPROPERLY DENIED

The Appellate Division of the Supreme Court of New York ruled that the state's Workers' Compensation Board improperly denied a claim filed by a construction worker whose toe had to be amputated following a workplace injury. The board had affirmed a workers comp judge's decision to disallow the claim of Eddy Irizarry, an employee of Lopez Matos Construction Inc. who was injured in February 2021 when he stepped on a nail at a construction site. The appeals court ruled the board erred by focusing on a procedural issue and not the merits of the claim.

APPELLATE COURT RULES FOR COMP INSURER

A workers compensation insurer that paid $1.1 million in benefits to a bartender accidentally shot by an off-duty police officer may continue to pursue a subrogation claim against the city of Honolulu even after the worker's third-party suit against the city was dismissed, the Hawaii Supreme Court ruled. The high court sided with Dongbu Insurance Co. Ltd. in the case that began with the April 2015 shooting of Hyun Ju Park at Kings Sports Bar & Grill.

Mike Rice

CAC GROUP

Mike Rice joined CAC Specialty as CEO at its creation in 2019 after spending four years leading JLT Specialty USA. Prior to that, he was at Aon PLC, where he began in management and professional liability and took on roles of increasing responsibility over 23 years. CAC Specialty began as a sister company of Birmingham, Alabama-based Cobbs Allen, a well-established small- and middle-market brokerage, and the companies merged in late 2022 to form CAC Group, with Mr. Rice as CEO. CAC Specialty had about $200 million in revenue in 2023 and CAC Group more than $260 million. Denver-based Mr. Rice recently spoke with *Business Insurance* Editor Gavin Souter about the company's strategy and outlook. Edited excerpts follow.

Q You've seen some significant growth since the company was formed. Where did it come from?

A We picked our spots, we did our homework, we knew what regions of the country we wanted to operate in, we knew we wanted to be specialists, not all things to all people, and we stuck to that strategy.

We entered the market when the market was getting a little bit more difficult, but five months after we started the business we sent everybody home for COVID. That's a really daunting prospect when you've recruited 100 people to join a firm. One thing that turned out to be really fortuitous for us was we … had a bankruptcy practice and as COVID hit we started to pick up a lot of business. I would much rather COVID had never have happened, and I still think we would have grown at the pace we are growing, but our growth was maybe a little bit different than what we expected.

Q What sort of coverages come into play there?

A 90% of it is on the D&O side. You need to bring in new leaders, and they want to make sure they have D&O coverage for them and it isn't tied to the former leadership team.

Q What are some of the other areas where you've seen growth?

A Our biggest single product line is our directors and officers liability practice. Our next biggest practice is transactional liability, which specializes in reps and warranties, tax indemnities and contingent liability. We had a stellar year last year, despite the fact there wasn't a lot of M&A. The fact that we had such a strong tax practice and contingent liability practice really carried the day, and that practice more than doubled in size.

The next biggest practice is probably our property/casualty practice and after that our natural resources practice. Cyber has been a really interesting topic, and we're growing very well on the cyber side. We invested in a senior living and health care team and that's really starting to grow, and there are other specialty practices we're involved in.

One of the things about us that makes us different is this investment we have in Dorset Peak, which is our investment banking operation that specializes in insurance transactions, at the intersection of traditional insurance markets and capital markets. It can do very interesting things with captives and financings around insurance products and debt. It's really allowed us to be creative in our insurance placements.

Q&A

Q D&O rates have been declining, so how are you managing to grow that practice?

A It's a tough one. Rates went up tremendously but much of that rate has been given back since 2022. When rates are coming down by 20% to 30% a year you need to be able to add new business, and so we have this phenomenal distribution network of producers.

Q Looking forward, where do you see opportunity for growth?

A We're four years into this business at CAC and we aren't done building out those practices, so a lot of our growth is going to be from those very same practices. There's lots more growth to be had in natural resources, particularly in the renewables field. Health care is a huge part of the economy in the U.S., and we're at the early stages of our investment in health care. D&O is a product that most companies can't live without, so we feel like more investment there is going to allow us to continue to grow. But we'll continue to look at industries where we see non-commodity-like features.

Q You say all your growth so far has been organic. Will that change?

A That could change. Our eyes are open to opportunities for tuck-in type investments. We can cross sell specialty products into (Cobbs Allen), and we feel that there are similar entities in other cities in the U.S. where this network that we built at CAC can be very valuable to them, so maybe getting more into the middle market in other cities is something that we'll take a look at. Brokers that have heavy specialty lines investments or have specialty products, those are of great interest to us at this point in our existence.

We've got a lot of dry powder, but organic is always going to be a big part of our story.

Q To do that often requires a fair amount of recruitment, which has its own challenges, particularly the litigation that often follows.

A Recruiting people is not for the faint of heart. Our strategy when we do it is to abide by the agreements that people have. For some unknown reason, in our industry we have lots and lots of noncompetes and nonsolicits way above and beyond any other industry that I look at. I don't think that's great for buyers of insurance and I don't think it's great for professionals in the insurance field, but it's an environment that we have to operate in, so we've got to be very careful.

Q In the past, you've suggested that maybe the way to go would be something like gardening leave like they have in the U.K. Do you see any prospect of that happening in the U.S.?

A Every once in a while, you see it. Maybe because insurance is a much older, more established industry in the U.K., they got to a methodology that has a lot less litigation tied to it by forcing people to sit in the garden for six months or 12 months. I think it's probably the most elegant solution I've seen thus far.

For some unknown reason in our industry we have lots and lots of noncompetes and nonsolicits way above and beyond any other industry that I look at.

GREEN BUILDING OWNERS CONFRONT INSURANCE HURDLES

Buyers seek credit for improved safety of sustainable construction materials; insurers wary of new risks, higher costs

BY CLAIRE WILKINSON
cwilkinson@businessinsurance.com

Insurers have offered specialty coverage for green buildings for years, but businesses that invest in more sustainable materials and technologies are not yet seeing the benefits reflected in the cost of their insurance programs.

Adding green features such as vegetated roofs, rooftop solar and alternative energy systems to properties can improve their efficiency but may make them more difficult to insure, brokers and risk managers say.

Designers should document expectations to cut E&O risks

As demand for green buildings continues to grow, design professionals should have contracts and documents in place that clearly define the scope of their services, industry experts say.

Design professionals should document their communications with clients to clearly establish expectations as to what they are and are not going to do related to a green building project, said Yvonne Castillo, director of risk management at Victor Insurance Managers LLC, a Marsh LLC unit in Bethesda, Maryland.

"What is your responsibility versus the contractors' responsibility, particularly when you think about the physical risks of climate change?" Ms. Castillo said.

For example, clients might assume that design professionals are building in data based on future climate projections, she said.

"That may not yet be the case for many firms, so document and have communications about that particular project site, what those perils and risks might be as relates to weather conditions 10, 15, 50 years down the road," she said.

Design professionals should also stay up to date on new materials, technologies and codes, and avoid contractual requirements to provide performance guarantees, said Doug Strong, Exton, Pennsylvania-based head of design professional at Axa XL, a unit of Axa SA.

"They can warrant their professional services, but they really can't guarantee necessarily the performance of the building," Mr. Strong said.

The same holds true for so-called green certifications and meeting a certain level of efficiency, he said.

Reviewing contractual obligations with insurers and general counsel can help design professionals ensure that they're not expanding their standard of care regarding the design of resilient and sustainable buildings, he said.

Dennis Artese, a shareholder in the New York office of Anderson Kill P.C., said the proliferation of green buildings may result in additional errors and omissions claims arising out of faulty or defective design of the buildings.

"Architects and engineers are now called to have very specific designs that meet various LEED certifications," Mr. Artese said.

A building that is designed appropriately and functions properly but doesn't meet thresholds to earn a specific certification could result in E&O claims, he said.

In addition, in green building construction, the effectiveness of new materials and techniques is an issue that can generate litigation, if some of the materials don't last as long as expected or perform as well, said Carol Sigmond, New York-based partner at Greenspoon Marder LLP.

Claire Wilkinson

Insurers are more educated than they used to be about green buildings, but they're still not there, said Kevin Bates, group head of risk and insurance for Australian construction company Lendlease Corp. in Sydney, and a Risk & Insurance Management Society Inc. board director.

"They haven't got their heads around the fact that green buildings are designed differently," Mr. Bates said.

A green building constructed in a flood plain, for example, may have been engineered so that it's a meter and a half higher than the surrounding area and not damaged in a flood, he said.

"It doesn't matter how often you explain that. It still gets treated the same. You get slapped for valuation but not the benefit yet from a rating perspective," he said.

Michael Lubben, Chicago-based vice president, risk management and benefits, at Henry Crown and Co./CCI, said the company added solar panels to a manufacturing facility in Livermore, California, two years ago, as it looked to become more energy efficient.

Even though the panels were highly resistant and constructed, installed and maintained properly, its insurer increased the maximum foreseeable loss on the building

See **GREEN** next page

GREEN

Continued from previous page

dramatically and reduced its capacity to 35% from 100%, Mr. Lubben said.

"It left us having to scramble to find the needed capacity for that building," he said.

Henry Crown, which has a global property program, tried more than 20 different insurers, and finally secured coverage for the facility on a standalone basis with FM Global, he said.

> "[Insurers] haven't got their heads around the fact that green buildings are designed differently."
>
> Kevin Bates, Lendlease

There's a lot of uncertainty around green building technologies and their effect on insurance coverage, said Penni Chambers, Dallas-based vice president of risk management at real estate developer Hillwood, a Perot company, and a Risk & Insurance Management Society Inc. board director.

From an environmental, social and governance perspective, if a business uses leading-edge technologies, it can benefit insurers' portfolios because it is positive for their own ESG disclosures, Ms. Chambers said.

"But when the claim happens, are they really going to be happy? Do we understand what that replacement cost is going to be? Do we understand the after-effects?" she said.

Putting out a solar panel fire takes significantly more water than a conventional property fire, for instance, Ms. Chambers said, adding, "What does that social impact and that climate impact do not only to risk management and our company's story but also to the insurer's story? We don't know that yet."

Green technologies change risks

Green building practices are becoming more widespread as legislative and regulatory changes require real estate owners to minimize the environmental impact of buildings as climate concerns rise.

In 2023, there were more than 6,000 LEED-certified commercial projects worldwide representing 1.36 billion gross square footage, according to the U.S. Green Building Council. The Inflation Reduction Act, signed into law in 2022, which offers various tax credits to encourage sustainable construction and the adoption of green technologies, is driving increased interest in Leadership in Energy and Environmental Design projects, a rating system for green buildings.

Construction companies will be required to innovate rapidly to meet greenhouse gas emission reductions that align with science-based targets, but innovations can introduce new risks, said Chris Semlies, New York-based assistant vice president for construction project and business resilience at Zurich North America. Globally, greenhouse gas emissions from the built environment represent 39% of gross annual carbon emissions, he said.

Mass timber can reduce a building's embodied carbon emissions significantly compared with conventional steel and concrete construction, but it can also introduce fire, supply chain and water damage risks, Mr. Semlies said.

Insurers should conduct due diligence of green building risks and understand how the different risks associated with the material are being addressed, he said.

The more sustainable a business can be the better from an environmental point of view, but sometimes that comes with some unintended consequences, said Sam Iannucci, Philadelphia-based fire protection lead at Chubb Ltd.

Vegetated roofs, for example, can reduce the heat island effect in which heat becomes trapped in dense urban areas, but whether it's a vegetated or solar roof, the building structure must be able to hold the additional weight of the materials, he said.

A hospital that received medical helicopters for trauma patients wanted to install a vegetated roof, Mr. Iannucci said. "What we didn't think about at first was the downdraft from the propellers would blow the growing material up, so before we went live, we talked about changing the flight path of the medical helicopters," he said.

Policyholders should speak with their insurers about green initiatives before they start selecting materials, Mr. Iannucci said.

More policyholders are considering sustainable building materials that can improve insulation, said Amy Brown, vice president, manager of natural hazard underwriting, at FM Global in Johnston, Rhode Island.

They should find a balance between installing insulation that is sustainable and will improve the wear of the building

GREEN BUILDING

The U.S. Environmental Protection Agency defines green building as "the practice of creating structures and using processes that are environmentally responsible and resource-efficient throughout a building's life cycle from siting to design, construction, operation, maintenance, renovation and deconstruction."

GREEN BUILDING COMPONENTS:

Energy efficiency and renewable energy: Using energy-efficient designs and renewable power sources that help lower costs and reduce energy consumption.

Water efficiency: Implementing technologies and using alternative sources that reduce water consumption.

Environmentally preferable building materials and specifications: Using products made with recovered or recycled materials in construction.

Waste reduction: Implementing practices that preserve natural resources and prevent waste and pollution, and using materials that can minimize, reuse and recycle waste.

Toxics reduction: Developing alternative practices and selecting materials that minimize environmental impact.

Indoor air quality: Using construction practices that can improve air quality, influencing human health, productivity and wellness.

Risk mitigation, data crucial in securing insurance capacity

Businesses investing in green technologies should prioritize risk controls and harness data to differentiate their risks to insurers, according to industry experts.

Making solar power assets more resilient so they can withstand hail and other severe convective storm events is critical, said Jason Kaminsky, CEO of kWh Analytics Inc., a San Francisco-based managing general agency.

"If you're in an area exposed to high winds, maybe you use a different method to attach the modules that's more secure, or maybe you pick a module that has thicker glass and is more resilient to vibrations when the wind or hail comes," Mr. Kaminsky said.

For Texas locations, installing solar panels on the ground rather than on a roof could have a dramatic effect on a loss profile, because if the panels catch fire the building would likely not be damaged, he said.

Building codes set a minimum standard for construction, but companies should consider exceeding the minimum requirements, said Ian Giammanco, managing director for standards and data analytics and a lead research meteorologist at the Insurance Institute for Business & Home Safety based in Richburg, South Carolina.

"It's really important that, as our materials change, the testing standards that the building codes reference keep up with all of that. There's where we can get ourselves into trouble if we don't and you introduce a material that has a vulnerability that we don't know about," Mr. Giammanco said.

To achieve decarbonization goals in the built environment, a significant amount of testing, learning and experimentation will be needed, said Charlie Sidoti, Cambridge, Massachusetts-based executive director at InnSure Corp., an industry-funded climate nonprofit.

"It just requires a higher level of due diligence by the industry, as opposed to walking away and saying, 'We're not going to do this,'" Mr. Sidoti said.

Advances in artificial intelligence and the greater availability of data will help insurers price risks more accurately for future climate scenarios, said Richard Hartley, CEO of London-based insurtech Cytora Ltd.

If a property owner is building in an environmentally friendly way, that additional data should mean that more insurers will be willing to quote or offer coverage, Mr. Hartley said.

Claire Wilkinson

and using a material that is fire resistant and resilient, she said.

Green building materials tend to be more expensive than standard construction materials, which can increase the risk of cost overruns and have a significant impact on a project's time schedule, said Jon Peeples, vice president of environmental at Philadelphia Insurance Co.

In addition, professional liability risks can arise if a green building doesn't meet the owner's expectations by achieving a certain certification or if the cost to maintain the property is higher than expected, Mr. Peeples said (see related story).

TOP 10 STATES FOR LEED RANKING

RANK	STATE	PROJECT COUNT	TOTAL GROSS SQUARE FOOTAGE	SQUARE FOOTAGE PER CAPITA
1	New York	201	93,548,625	4.63
2	Illinois	101	41,174,946	3.21
3	Maine	105	22,538,269	3.21
4	Washington	91	23,175,771	3.01
5	Georgia	97	27,473,704	2.56
6	Virginia	90	20,969,235	2.43
7	California	402	89,774,704	2.27
8	Colorado	62	11,246,113	1.95
9	Hawaii	10	2,609,493	1.79
10	Maryland	62	10,946,153	1.77

Source: U.S. Green Building Council Inc.

Coverage impact

Green additions and upgrades can be more costly and difficult to insure but not always, according to brokers.

Endorsements can be added to commercial property policies that provide coverage for the increased cost to repair or replace damaged property using materials that are recognized as "green," said Meg Glenn, Denver-based real estate practice leader at CAC Specialty.

The cost of the upgraded coverage varies, depending on the limit, Ms. Glenn said. "The higher the limit, the more expensive the cost will be," she said.

If policyholders using green technologies can show insurers they are controlling or mitigating the risks to the building's overall structure, coverage is readily available, with "little price or rate impact on those assets," said Joe Macejak, Chicago-based Central zone real estate leader in the U.S. property practice at Marsh LLC (see related story).

But there are exceptions, Mr. Macejak said. Solar panels, if they are not correctly installed with the appropriate mitigation processes, present a higher fire risk to an asset, he said, adding, "The same could be said with a grass-type roof."

A green building might cost more to insure in some cases, but "it's not an absolute," said Rick Miller, Boston-based U.S. property leader for Aon PLC's commercial risk solutions business.

> "The higher the limit, the more expensive the cost will be."
>
> Meg Glenn, CAC Specialty

"If you have an old building, it may be cheaper to replace that old building with modern technology," he said.

"The factor is: Does it change the replacement value of that facility going forward? If there's a significant change, assuming that's upward, then it's pressure on premium because, like it or not, in property it's value times a property rate," Mr. Miller said.

Insurance-to-value is a key issue for building owners as they consider the cost of adding green features to properties and how the costs are reflected in their insurance coverage, said Ron Guerena, senior vice president, Southern California practice leader, property & casualty, at Woodruff Sawyer & Co.

Capacity expands as cyber cat bonds take off

INSIDE

PRIVACY LAWS
Overlapping laws complicate breach notification requirements. **PAGE 19**

ZERO-TRUST SECURITY
Businesses tighten defenses to keep on top of ransomware attacks. **PAGE 20**

CYBER RESEARCH & DATA
Largest cyber liability insurers, global coverage trends, breakdown of cyber crimes and more. **PAGE 25**

BY MATTHEW LERNER
mlerner@businessinsurance.com

The cyber liability insurance market softened in 2023 as increased competition and capacity led to lower rates after a short-lived slowdown in ransomware attacks during 2022.

Additional reinsurance capacity was also added as insurance-linked securities markets issued cyber catastrophe bonds last year.

A resurgent threat landscape, however, and rising claims activity could cause a rebound in pricing this year, some experts say.

Cyber insurance rates were generally flat or a few points up or down depending on specific lines and geographies during recent renewals, sources said. The U.S. market was a little softer than overseas, and excess and surplus lines generally saw larger rate decreases than primary lines, they said.

"There have been some fluctuations depending on geography and the size of client but anywhere from positive single digit down to negative single digit," said Anthony Dagostino, New York-based global cyber chief underwriting officer for commercial lines at Axa SA.

Rates, which increased significantly after claims rose during the COVID-19 pandemic, have been tempered by the

competition generated by added capacity for cyber coverage.

"We are seeing new entrants into the market, particularly with new managing general agents bringing new capital into the market," said Washington-based Rachel Lavender, Marsh LLC's U.S. & Canada cyber brokerage leader.

Marsh data showed fourth-quarter 2023 cyber rates down 4% compared with a 6% decrease in the prior quarter.

"Threats are expanding and that attracts capacity to meet the demand," said Mario Vitale, New York-based president of Resilience Cyber Insurance Solutions LLC, a managing general agent that has recently expanded its underwriting authority to include coverage for global companies with up to $10 billion in annual revenue.

"We definitely saw carriers become more aggressive," in deploying capacity, said Nadia Hoyte, New York-based national cyber practice leader for USI Insurance Services LLC. She said insurers appear more comfortable with offering capacity as they gain greater understanding of cyber exposures.

Last year also saw the introduction of insurance-linked securities for cyber coverage, or cyber catastrophe bonds.

Paul Bantick, London-based global head of cyber and technology for Beazley PLC, which issued some of the initial securities, said the added capital markets capacity and new method of risk transfer will help cyber insurance markets continue to grow.

"To meet the emerging demand, we need these vehicles," he said, noting catastrophe bonds have become a staple source of reinsurance coverage for property insurers.

Ransomware and privacy claims, however, are ticking up, which could lead to higher rates, some experts say.

Kristen Peed, Cleveland-based head of corporate risk for San Mateo, California-based Sequoia Benefits and Insurance Services LLC, and vice president of the Risk & Insurance Management Society Inc., said rising ransomware and other cyber exposures present risk managers with an emerging and evolving challenge.

"In 2023, we saw all the hallmarks of a favorable market for cyber insurance. We saw increased competition, we saw rates flat or falling, and we saw generally more favorable terms than in prior years," said John Farley, New York-based managing director of Arthur J. Gallagher & Co.'s cyber practice.

"Ransomware attacks are continuing to rebound. They're increasing not only in frequency but also the sophistication and the severity with which they've hit companies."

Rachel Lavender, Marsh

"Some of that has still continued on into 2024," Mr. Farley said. "But at some point, cyber claims trends will drive the market, and if they continue to increase in frequency and severity, then we're going to see underwriters react. We're not sure where the inflection point is going to be, but at this point we're still in the same pattern we've seen over the last year."

After abating somewhat during 2022, ransomware attacks have returned as a significant exposure for policyholders.

"Ransomware attacks are continuing to rebound. They're increasing not only in frequency but also the sophistication and the severity with which they've hit companies," said Ms. Lavender of Marsh.

"We've seen an increase in loss in 2023 compared to 2022," said Rich DePiero, New York-based executive vice president and head of Sompo Pro, a unit of Sompo International Holdings Ltd.

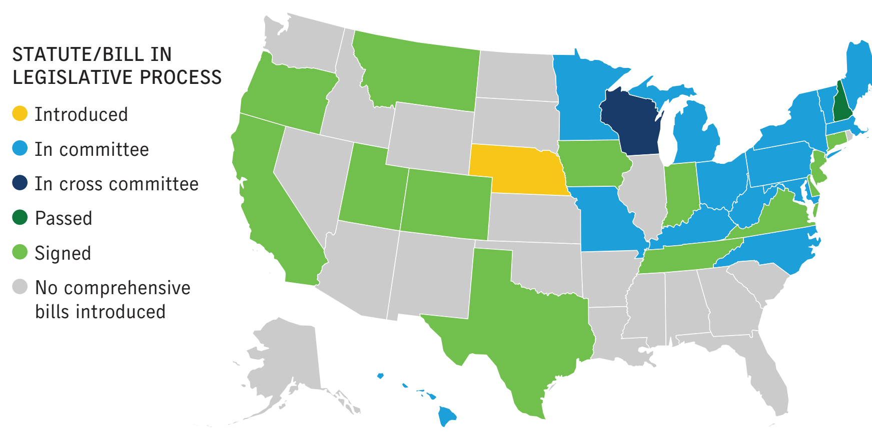
Data privacy is another area of concern, he said.

"We're monitoring that very closely. Those losses are beginning to add up and we expect to probably start seeing a lot of those claims being paid out over the 2024 policy period," Mr. DePiero said.

Emerging technologies such as artificial intelligence can be both part of the threat and part of the solution.

"These things have the potential to be used by cyber bad actors, from an offensive perspective, and they have the potential to be used by cyber defenders," said Patrick Thielen, Chicago-based global head of cyber for Liberty Mutual Insurance Co.

U.S. STATE PRIVACY LEGISLATION TRACKER



Source: International Association of Privacy Professionals

As of 2/9/24

Risk managers, insurers grapple with shifting privacy laws

An increase in online data privacy regulations being introduced at state and national levels is adding another layer of complexity for risk managers trying to master the labyrinth of overlapping or intersecting guidance for cyber breaches and related incidents.

"Navigating country regulation is a test in itself to make sure we have the right people watching it," said Anthony Dagostino, New York-based global cyber chief underwriting officer for Axa SA, adding that both underwriters and policyholders must keep abreast of regulatory issues.

U.S. state regulations pose an additional challenge, as incident notification laws differ, he said.

Thirteen states have enacted comprehensive privacy laws, according to the International Association of Privacy Professionals, a not-for-profit organization based in Portsmouth, New Hampshire. More than a dozen others have legislation in some stage of development, such as in committee (see map).

The differentiation between states presents an added challenge to risk managers.

"That's making it incredibly difficult for risk managers to respond in the event of breaches because we have to engage with third parties like breach coaches, or legal representation that really understands what we need to do in specific states, because it differs so much across the board," said Kristen Peed, Cleveland-based head of corporate risk at San Mateo, California-based Sequoia Benefits and Insurance Services LLC, and vice president of the Risk & Insurance Management Society Inc.

California introduced a mandatory notification requirement in 2003 and all other states followed with their own requirements, said John Farley, New York-based managing director of Arthur J. Gallagher & Co.'s cyber practice.

"Now you have 50 different state notification requirements. A very similar thing is happening around privacy law and data collection. California was the first and now states are following like dominoes," he said.

"The regulatory arena is an evolving arena, not just here in the U.S. but around the world," said Rachel Lavender, Marsh's U.S. & Canada cyber brokerage leader, based in Washington.

Brokers and insurers are spending more time helping policyholders with regulations.

"That's something that we spend lots of time talking to clients about," said Paul Bantick, London-based global head of cyber and technology for Beazley PLC.

Matthew Lerner

SPECIAL REPORT

Cyber defenses ramp up as hacks exploit gaps

BY JUDY GREENWALD

Organizations continue to race against cybercriminals to keep their systems secure by focusing on defensive measures, including addressing supply chain weaknesses, removing software vulnerabilities and exploring alternatives to traditional passwords.

Ransomware remains the predominant attack approach they face. Last year's record number of ransomware attacks included a 67% year-over-year increase in fourth quarter incidents, according to a recent report by Corvus Insurance Holdings Inc.

Experts are also concerned about criminals' use of generative artificial intelligence, although it can also be effectively used by companies as a defense (see related story).

> "We keep forgetting that all the bad guys really need is one little gap."
>
> Ed Dubrovsky, Cypfer

Cybersecurity is simultaneously fast and slow moving, said Chester Wisniewski, Vancouver, British Columbia-based director, field chief technology officer, for cybersecurity company Sophos Ltd.

Criminals and nation states are innovating incredibly quickly, Mr. Wisniewski said. "There's a pace of innovation among those profiting from stealing information that makes it harder for businesses to keep on top of," he said.

Meanwhile, security efforts are held back by long-standing issues, such as reusing passwords and failing to keep patches up to date, he said.

"We keep forgetting that all the bad guys really need is one little gap" to enter systems, said Ed Dubrovsky, Toronto-based chief operating officer and a partner at Cypfer Inc., a cybersecurity company.

The average ransomware model "hasn't changed very much" said Mark Stockley, Oxford, England-based cybersecurity evangelist for Malwarebytes, a cybersecurity company. "We still see criminals sending out malware in waves of email," some of which will get through.

While traditional ransomware "is still very much a thing," it tends to be used to target small and medium-sized enterprises, said John Dwyer, Pittsburgh-based head of research at IBM Security X-Force, a security division of IBM.

In attacking larger companies, criminals often buy readily available company data through the dark web that they threaten to release, he said.

Ryan Witt, Sunnyvale, California-based vice president of industry solutions for Proofpoint Inc., a cybersecurity company, said that while ransomware gets a lot of attention, "there's way more money lost" by companies to broad-based attacks — where payments are redirected, data pilfered or credentials stolen — that permit criminals to navigate networks and determine what to attack or exploit.

An ongoing concern is third-party suppliers. In response to companies' introduction of more rigorous firewalls and employment management systems, criminals have used suppliers as a way into their computer systems, said Eric

CYBERSECURITY TIPS

Experts say effective cybersecurity practices include:

- Conducting an initial risk assessment to identify vulnerabilities.
- Prioritizing risks.
- Developing an incident response plan.
- Training employees.
- Updating and patching apps as needed.
- Monitoring operations.
- Implementing zero-trust policies, limiting system access to an "as-needed" basis.
- Moving beyond traditional passwords.
- Responding nimbly when warning signs emerge.
- Coordinating among company departments.

Source: *Business Insurance* interviews

AI TECHNOLOGIES BOOST COMPUTER SECURITY, BUT ADD TO THREATS

Artificial intelligence is being explored as a tool by corporate cybersecurity experts and cybercriminals.

Cybercriminals are actively using AI "in a whole bunch of ways" and it is being used in companies "partially because this is the only way to keep up with the velocity of the changes that the bad guys are throwing at us," said Alan Brill, Secaucus, New Jersey-based senior managing director and founder of Kroll Cyber Risk, a division of Kroll LLC.

"If you're standing still, you're falling behind," he said.

For criminals, finding a cyber vulnerability is manually intensive, said Andreas Kuehlmann, CEO and executive chair of San Jose, California-based cybersecurity company Cycuity Inc. AI will give them another tool that will increase their productivity, he said.

The technology can also be used to eliminate the revealing mistakes that non-native English-speaking criminals sometimes make in phishing attempts. It turns out AI "is really good at it," said John Dwyer, Pittsburgh-based head of research at IBM Security X-Force.

Meanwhile, "a lot of companies are implementing AI and putting in new processes without a full understanding of what they're doing," said Jeffrey Wheatman, cyber risk expert and evangelist with Boston-based Black Kite Inc.

He referred to a reported instance in which a company official uploaded internal financial data into Chat GPT to help with a financial analysis, unaware it could have been accessed.

But some experts say AI does not yet represent a significant threat to companies.

The concern is "a little overblown" at this point, said Daniel Blackford, Pittsburgh-based senior manager, threat research, at Proofpoint Inc.

AI is a two-edged sword that will also benefit companies by helping them improve their cybersecurity, experts say.

"It's going to be an important tool," enabling companies to identify threats as they appear and quickly assess them, said Michael Driscoll, New York-based senior managing director at FTI Consulting Inc., who is a former assistant FBI director.

Cybersecurity teams are trying to use the technology to improve cyber defense and response with automated detection and prioritization of cyber threats, and AI is one of the more popular ways to do so, said Joe Nocera, Chicago-based partner leader, cyber risk and regulatory marketing, for PricewaterhouseCoopers International Ltd.

Companies are still experimenting with AI, but a year from now they will have developed a "clear set of practices" outlining how to leverage it, he said.

Judy Greenwald

Byres, CEO of Victoria, British Columbia-based aDolus Technology Inc.

He pointed to SolarWinds Corp. software which, beginning in 2019, was used in cyberattacks perpetrated by the Russian Foreign Intelligence Service to deploy malicious code into the computers of thousands of companies and government agencies worldwide.

"A zero-trust network is one of the ways to help manage that risk," Mr. Wisniewski said. Such protocols require identity verification for every person and device trying to access a private network, and limiting even legitimate third parties to specific areas of the network.

Corporate software may also be a problem, experts say.

Complex software packages usually include open-source software with a source code that anyone can modify and whose vulnerabilities may be unknown even to the vendors that sell them.

In December 2021, for instance, a critical vulnerability was found in Log4J, a widely used open-source software.

According to Synopsys Inc.'s 2023 Open Source Security and Risk Report, 84% of codebases have at least one known open-source vulnerability, and 48% contain high-risk vulnerabilities.

6 STEPS TO ASSESSING CYBERSECURITY RISKS

1. Name all assets.
2. Prioritize the importance of each asset.
3. Identify all possible threats to your assets.
4. Identify all vulnerabilities in your environment.
5. Determine the likelihood of a threat event occurring.
6. Conduct an impact analysis to estimate the threat event's potential consequences and cost impact.

Source: Hyperproof Inc.

One approach to dealing with the issue is to compile a software bill of materials, a list of all the opensource and third-party components present in a codebase, experts say. President Biden signed an executive order requiring SBOM's use by the federal government in 2021.

This approach, though, is in its early stages of development. "It's not there yet," said Rani Osnat, Tel Aviv-based senior vice president, strategy and business development, for Aqua Security Software Ltd. It still "doesn't necessarily go all the way to the base level," he said.

And companies should prioritize their security concerns, said Andreas Kroier, Vienna-based senior principal, solution lead of application security, at software company Dynatrace Inc.

In analyzing software, it is important to distinguish the exposures that need to be fixed first from those that are relatively harmless and sit "in back of the environment" to avoid "chasing phantom problems," he said.

Companies are also moving away from traditional passwords, which are vulnerable to cybercriminals, and toward using cell phones or biometric devices that may require a fingerprint or facial ID and multifactor authentication.

"I would love to see the password die," Mr. Wisniewski said. "It is a leading way organizations are compromised."

CLASSIFIED

IN THE HIGH COURT OF JUSTICE CR-2023-005956
BUSINESS AND PROPERTY COURTS OF ENGLAND AND WALES
INSOLVENCY AND COMPANIES LIST (ChD)

IN THE MATTER OF ENGLISH & AMERICAN INSURANCE COMPANY LIMITED

AND

IN THE MATTER OF THE COMPANIES ACT 2006

NOTICE IS HEREBY GIVEN that, by an order dated 24 January 2024 made in the above matter, the High Court of Justice of England and Wales sanctioned the Final Closure Scheme of Arrangement pursuant to Part 26 of the Companies Act 2006 between English & American Insurance Company Limited ("**EAIC**") and its Scheme Creditors (the "**Scheme**").

The effective date of the Scheme is 25 January 2024 (the "**Effective Date**").

Scheme Creditors who wish to assert a Scheme Claim under the Scheme must complete and submit or return a Claim Form before 23:59 hours (English time) on the day falling 105 days after the Effective Date, being Thursday 9 May 2024 ("**Bar Date**").

Claim Forms may be accessed on EAIC's website at: https://eaic.co.uk/. Alternatively, Scheme Creditors may request a hard copy or email copy of a Claim From the Scheme Manager at the details below.

If a Scheme Creditor does not complete and submit or return a Claim Form by the Bar Date, in accordance with the instructions on the Claim Form, that Scheme Creditor shall not be entitled to assert any Scheme Claim against EAIC, except in respect of an Existing Scheme ESL.

Unless otherwise defined, capitalised terms in this notice shall have the meanings given to them in the Scheme. The Scheme can be accessed on EAIC's website at: https://eaic.co.uk/.

For further information please contact the Scheme Manager as follows:

Phone: +44 (0) 7795848215

Email: stephanie.wilton@pro-global.com

What the best cyber brokers do to help their clients

As outside insurance, risk management and coverage counsel for companies that run the gamut from small start-ups to Fortune 100 global conglomerates, we work with a lot of clients and brokerages on cyber insurance policy procurements, renewals and claims. Most of our clients have agreements with brokers that address the different services that will be provided for procuring insurance and to handle claims. In our experience, there are a few things that the best brokers do to help their clients navigate the cyber risk landscape. Here they are:

Understand — and anticipate — the costs of a data breach

We all know the common refrain that it is not a matter of "if" your company will be breached but "when." And when that occurs, the first question executives and board members ask is "How much is this going to cost us?"

Fortunately, there are several sources that brokers can share with their clients to ensure they're informed as to what these incidents cost so they can be better informed when deciding what cyber insurance limits to purchase.

First, the best brokers share benchmarking information with their clients as to what other, similarly situated companies in that industry are purchasing for cyber insurance limits.

Second, they point their clients to reliable secondary sources, such as the annual IBM "Cost of a Data Breach Report." The 2023 report found that the average cost of a data breach reached an all-time high of $4.45 million globally. In the United States, it was $9.48 million. The average cost of a mega breach was far larger: $36 million for a breach involving 1 million to 10 million records and $332 million for a breach involving 50 million to 60 million records.

Third, the best brokers help their clients consider what a business income or reputation loss may look like in the aftermath of a major cyber event. For manufacturing, retail and service provider companies, ransomware attacks or voluntary network shutdowns to neutralize the threat actor can be far more expensive than incident response and notification costs combined. Thus, the best brokers encourage their clients to consider retaining a forensic accountant to estimate the potential cost of a shutdown. These loss estimates will better inform a policyholder on limits they need to buy.

Set up a smooth renewal process

While clients must lead the renewal process because they are in the best position to understand their business needs, exposures, risks and finances, and ultimately control what is purchased, brokers should help them understand the process and ensure they have all the information they need.

This begins by ensuring the client starts early and allowing sufficient time — often at least several months — for the renewal process to play out. Brokers should provide new forms and endorsements well in advance of any binding deadlines to allow time for clients to review and understand any changes; encourage all relevant personnel at the company to be involved in the renewal and application process, such as IT, legal, risk and finance teams; ensure the client understands the application questions and answers applications fully; and explain how inaccurate answers or omissions can impact coverage. Indeed, in many jurisdictions, a misrepresentation in the application, even if unintentional, has the potential to void coverage.

The best brokers also help clients anticipate potential underwriter follow-up questions and ensure they are prepared for underwriting calls and bring all the right internal experts to the calls.

Finally, they analyze the policy language of each specimen policy and work with the client and its in-house or outside counsel to seek additional endorsements, enhancements or manuscript language as appropriate.

Cyber insurance is not a one-size-fits-all product, nor should it be. Policies should be tailored to each policyholder's unique risk profile and each insurer's risk appetite. And, all parties should work to avoid ambiguous policy language so that they have shared expectations about how the policy will respond in those critical first hours and days following a breach. The best brokers ensure their clients understand not only pricing differences between quotes, but also how differences in policy language, sublimits, retentions, coinsurance, waiting periods, vendor panels and endorsements will impact coverage and incident response.

Ensure compatibility

The best brokers make sure the policyholder's incident response plan works harmoniously with the policy. Sophisticated policyholders have well-developed and well-practiced incident response plans, which typically call for the retention of specific vendors, such as cyber incident response legal counsel, crisis communications/public relations firms, and incident response IT vendors. Oftentimes, these are vendors that the client has a longstanding relationship with. Unfortunately, we have seen many situations where a new client's cyber insurance policy did not conform with the company's existing incident response plan so that the client may have hired unapproved vendors, for whom the insurer disputed coverage, after the cyberattack.

Brokers should ask clients who their preferred vendors are and confirm they are on the proposed insurer's panel or are otherwise pre-approved on the policy by endorsement.

Avoid privilege issues

The best brokers understand the legal ramifications of their role, including most notably as it concerns protecting clients from a privilege waiver. A policyholder and its insurer share a goal in minimizing potential liabilities, such as claims and regulatory actions, arising from a cyber incident, which gives rise to a "common interest" that, in most situations, protects the disclosure of privileged information between the two.

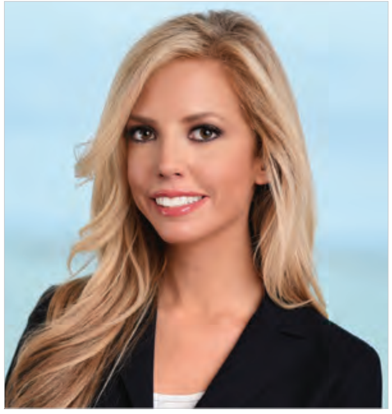
In many cases, this "common interest" does not extend to brokers. Some courts have found the attorney-client privilege or the work product protection is waived by the inclusion of the broker or claims advocate in communications between an insured and its attorneys about legal analysis or strategy.

Several court decisions discuss this issue because third-party claimants have sought communications between policyholders and brokers.

Thus, the best brokers and claims advocates take care to protect their clients and avoid setting up a potential privilege waiver situation. They educate clients on how their inclusion on calls and written communications about legal strategy could impact privilege.

Traditional coverage

Finally, when a breach occurs, the best brokers and claim advocates remember to consider traditional policies such as crime; kidnap, ransom and extortion; and property that may provide additional coverage. Losses resulting from fraudulent transfers, social engineering schemes and business email compromises, may solely be covered under standard or endorsed insuring agreements to a crime policy, rather than a cyber or technology errors and omissions policy.



Andrea DeField is a partner and co-lead of the cyber insurance practice at Hunton Andrews Kurth LLP in Miami. She can be reached by email at adefield@HuntonAK.com.

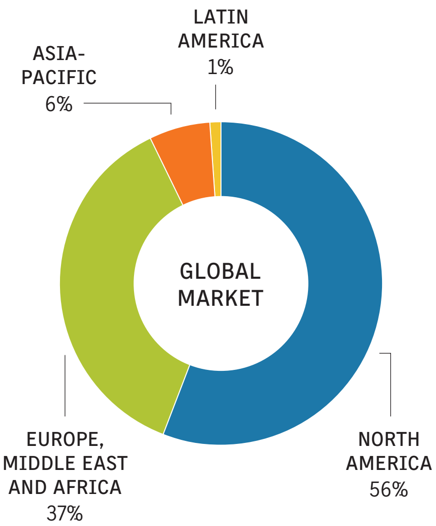
Kevin Small is counsel in the firm's insurance coverage group in New York. He can be reached at ksmall@HuntonAK.com.

These other sources of recovery become particularly important where the policyholder's cyber insurance limits are insufficient to cover the fall-out of a major cyber event. The best brokers know that some K&R policies provide sublimited coverage for cyber extortions and ransomware attacks. They also know that policies such as property, pollution, commercial general liability and professional liability may have endorsements that provide sublimited coverage for certain cyber risks and associated costs. They will also look to D&O insurance to potentially cover follow-on litigation.

In sum, the best brokers understand their clients' unique business and risk profiles in order to help put them in the best position to purchase the best coverage to protect against the ever-evolving cyber threats.

GLOBAL CYBER INSURANCE MARKET

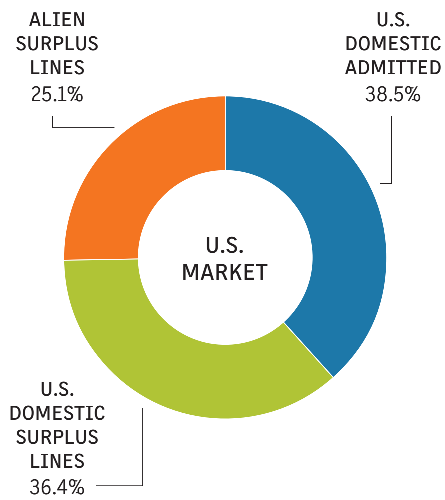
North America accounts for more than half of global cyber insurance gross premium written.



Source: S&P Global

U.S. CYBER INSURANCE MARKET TYPE

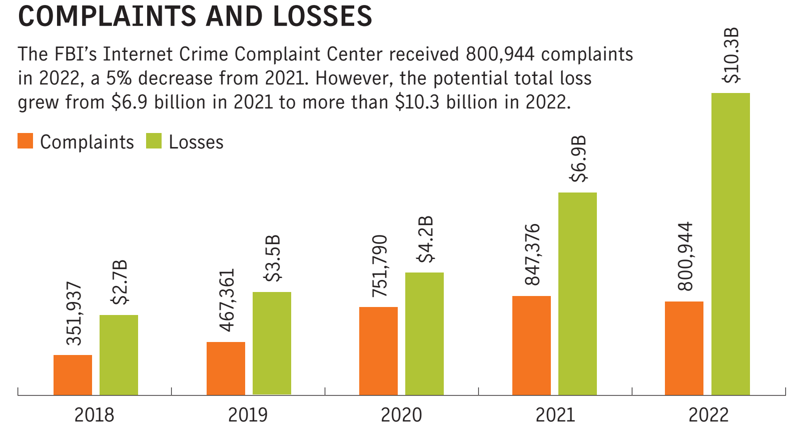
The total U.S. premium for cyber insurance in 2022 was $9.7 billion, according to the National Association of Insurance Commissioners.



Source: National Association of Insurance Commissioners

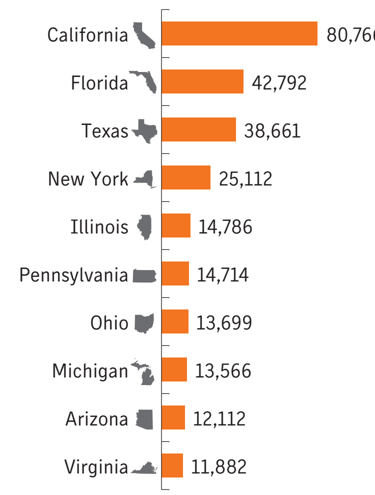
COMPLAINTS AND LOSSES

The FBI's Internet Crime Complaint Center received 800,944 complaints in 2022, a 5% decrease from 2021. However, the potential total loss grew from $6.9 billion in 2021 to more than $10.3 billion in 2022.

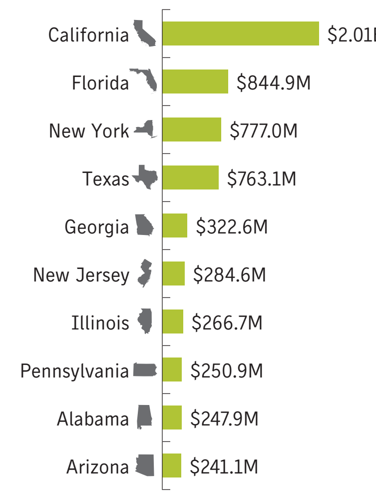


Source: FBI

TOP 10 STATES BY NUMBER OF VICTIMS



TOP 10 STATES BY VICTIM LOSS



Source: FBI

LARGEST CYBER INSURERS*

The top 20 U.S. insurers wrote 78.2% of the cyber insurance market in 2022, down from 83% in 2021. The loss ratio for 2022 for the top 20 averaged 44.6%, compared with 66.4% in 2021.

2022	2021	Group name	Direct written premium	Market share	Loss ratio
1	1	Chubb Ltd.	$604,926,658	8.4%	53.8%
2	2	Fairfax Financial Holdings Ltd.	$562,995,303	7.8%	54.0%
3	3	Axa Insurance Group	$527,441,693	7.3%	66.2%
4	4	Tokio Marine Holdings Inc.	$367,607,130	5.1%	57.8%
5	9	Arch Insurance Co.	$346,374,212	4.8%	52.3%
6	6	The Travelers Cos. Inc.	$315,324,617	4.4%	34.8%
7	5	American International Group Inc.	$299,011,690	4.1%	47.6%
8	34	Nationwide Mutual Insurance Co.	$257,312,784	3.6%	12.5%
9	11	Zurich Insurance Group Ltd.	$252,514,546	3.5%	68.2%
10	13	Sompo Holdings Inc.	$247,978,386	3.4%	50.1%
11	8	CNA Financial Corp.	$228,933,184	3.2%	26.5%
12	20	Berkshire Hathaway Inc.	$228,495,397	3.2%	48.1%
13	12	Liberty Mutual Holdings Co. Inc.	$208,204,580	2.9%	57.5%
14	17	Swiss Re Ltd.	$207,013,991	2.9%	19.6%
15	10	Axis Capital Holdings Ltd.	$195,746,593	2.7%	85.9%
16	7	Beazley Group	$174,628,461	2.4%	19.6%
17	22	Ascot Group	$166,556,438	2.3%	30.2%
18	32	Randall & Quilter Investment Holdings Ltd.	$161,653,538	2.2%	10.7%
19	27	Markel Group Inc.	$152,886,167	2.1%	40.1%
20	15	Hartford Fire and Casualty Group	$152,339,006	2.1%	15.5%

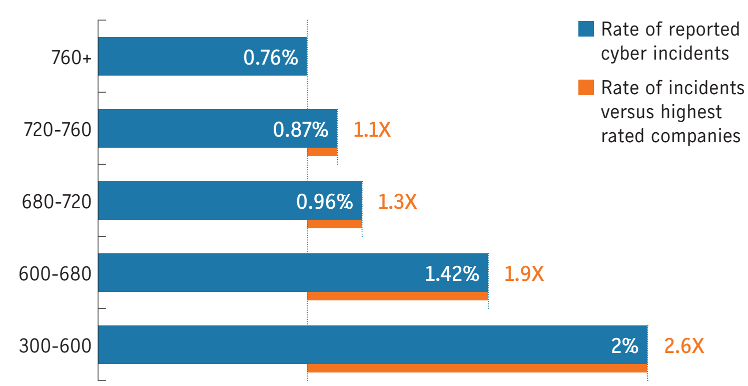
*Does not include alien surplus lines

Source: National Association of Insurance Commissioners

POOR CYBER PRACTICES LEAD TO MORE INCIDENTS

According to an analysis of monthly data from 2,571 public companies from 2015 to 2023, those in the quintile with the lowest Bitsight ratings experienced an incidence rate 2.6 times higher than those in the quintile with the highest ratings.

BITSIGHT CYBERSECURITY RATING BRACKET*



*Bitsight rates the cybersecurity performance of companies on a scale of 250 to 900.

Source: Bitsight and Moody's Analytics

CYBER CRIME TYPES

Cyber crime types by the number of complaints received

Rank	Crime type	Victims
1	Phishing	300,497
2	Personal data breach	58,859
3	Nonpayment/nondelivery	51,679
4	Extortion	39,416
5	Tech support	32,538
6	Investment	30,529
7	Identity theft	27,922

Rank	Crime type	Victims
8	Credit card/check fraud	22,985
9	Business email compromise	21,832
10	Spoofing	20,649
11	Confidence/romance	19,021
12	Employment	14,946
13	Harassment/stalking	11,779
14	Real estate	11,727

Rank	Crime type	Victims
15	Government impersonation	11,554
16	Advanced fee	11,264
17	Overpayment	6,183
18	Lottery/sweepstakes	5,650
19	Data breach	2,795
20	Crimes against children	2,587
21	Ransomware	2,385

Rank	Crime type	Victims
22	Threats of violence	2,224
23	IPR/copyright/counterfeit	2,183
24	SIM swap	2,206
25	Malware	763
26	Botnet	568
	Other	9,966

Source: FBI

2024-2025 BUSINESS INSURANCE®

BusinessInsurance.com/events

EVENT SCHEDULE

2024

BREAK OUT AWARDS
JUNE 20 (CHICAGO) | JUNE 25 (NEW YORK)
BusinessInsurance.com/BreakOut

U.S. INSURANCE AWARDS
JULY 18 | NEW YORK
BusinessInsurance.com/USIA

INNOVATION AWARDS
JULY 18 | NEW YORK
BusinessInsurance.com/Innovation

DIVERSITY, EQUITY & INCLUSION CONFERENCE
OCTOBER 17-18 | NEW YORK
BusinessInsurance.com/Diversity

WOMEN TO WATCH AWARDS & LEADERSHIP CONFERENCE (US)
NOVEMBER 19 | NEW YORK
BusinessInsurance.com/W2W

WOMEN TO WATCH AWARDS & LEADERSHIP CONFERENCE (EMEA)
DECEMBER 5 | LONDON
BusinessInsurance.com/W2WEMEA

2025

WORLD CAPTIVE FORUM
FEBRUARY 5-7, 2025 | ORLANDO
WorldCaptiveForum.com

**Event dates and formats are subject to change.*

CONTACT US

SUSAN STILWILL
HEAD OF SALES - EVENTS
(312) 833-4099
sstilwill@businessinsurance.com

BI EVENTS TEAM
events@businessinsurance.com

#BI_Events

OPINIONS

COMMENTARY

Care required in solving PTSD puzzle

More than 40 years after the American Psychological Association first included post-traumatic stress disorder in its manual for health care practitioners, the medical condition is becoming a source of increasing concern in the workers compensation sector.

In earlier eras, and under different names, PTSD was most closely associated with the exposure of military personnel to violence during combat, such as soldiers suffering from "shellshock" during World War I. And often sufferers toiled with untreated symptoms for years.

Now, PTSD is recognized as a mental injury that is suffered by many more people — often first responders but also victims of violent attacks and others — and one that can be sustained in a wide variety of situations, including in the workplace.

Gavin Souter
EDITOR

As recognition of the condition has grown, treatment protocols have evolved to the extent that many medical professionals view PTSD as a condition that can be effectively treated. As we report on page 4, talk therapy, medication and technological tools are all used to treat PTSD.

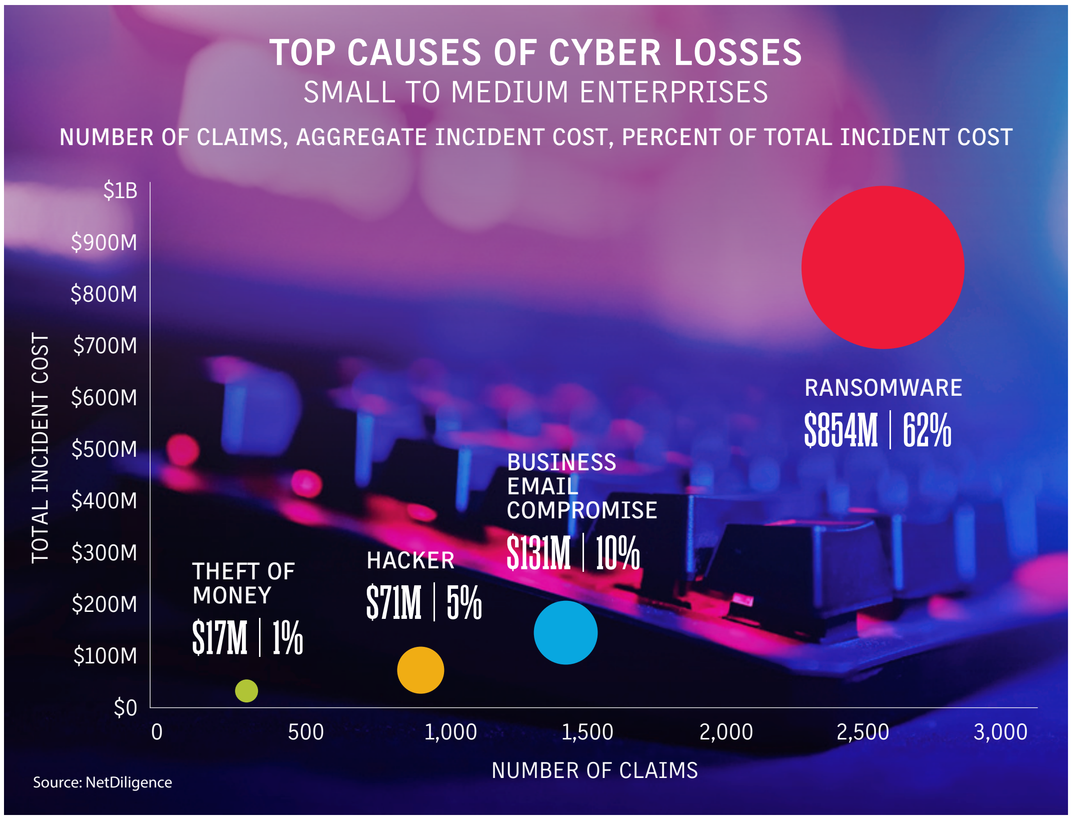
Relatively few people suffer from PTSD — about 6% of the U.S. population will suffer from the condition at some point during their lives — but the number of people in the workers comp system that are treated for PTSD has grown and is likely to grow further. That's because an increasing number of states are introducing and sometimes passing legislation that would extend PTSD presumptions to a wider group of workers, beyond the usual categories such as cops and firefighters. For example, Connecticut last year extended its presumption law to all workers who witness harrowing events, and Washington added nurses to its category of workers.

But many of the proposed presumptions have not made it through the various legislatures. Notably, in California Gov. Gavin Newsom vetoed a bill that would have expanded the state's PTSD presumption to various nurses and other medical staff. In his veto message, the governor noted the "proven difficulty of establishing a direct relationship between a disease or injury and the employee's work."

Therein lies the rub, when you have different systems that are tapped to treat a medical condition that is difficult to conclusively prove is tied to a discrete cause — should PTSD treatment be paid for through workers comp, employee medical benefits or another program?

In cases where states conclude they have sufficient evidence to link medical conditions to certain occupations, there's no getting around the financial consequences for employers and workers comp insurers.

Of course, most PTSD presumption bills pending in state houses are well intended, but lawmakers must consider all the implications of expansion provisions and base their decisions on scientific analysis before approving measures that will have far-reaching consequences for many employers.



VIEWPOINT

AI, deepfakes ominous

BY CLAIRE WILKINSON
cwilkinson@businessinsurance.com

Organizations face a momentous challenge in building cyber defenses to ward off the next generation of cyberattacks. It seems that just as they find a way to close off one avenue of attack, cybercriminals have already shifted their approach and found a new vulnerability.

Some businesses are exploring new methods, such as alternatives to traditional passwords, as they step up efforts to keep their systems secure. As we report on page 20, organizations are increasingly moving away from traditional passwords altogether, instead using cellphones or biometric devices that may require fingerprint or facial ID and multifactor authentication.

Such developments are a positive move toward addressing shifting cyber threats but may introduce additional risks. Last month, a finance worker at a multinational company was duped into paying out $25 million to cybercriminals using "deepfake" technology to pose as the organization's chief financial officer in a video conference call, according to news reports citing authorities in Hong Kong. The incident was one of a growing number of cases in which a sophisticated digital forgery of an image, audio, or video has been used to disrupt business operations or to facilitate fraud.

Deepfakes are proliferating and becoming more sophisticated, supported by advances in artificial intelligence. AI misinformation and deepfakes in the political arena are a persistent concern in an election year in which synthetic content can be manipulated to disrupt democratic processes. The Federal Communications Commission recently outlawed robocalls that use voices generated by AI. The FCC's announcement followed a robocall in January that appeared to have been a deepfake purporting to be President Biden that urged voters not to participate in New Hampshire's Jan. 23 GOP primary election. Major technology companies including Google, Meta, and TikTok have pledged to crack down on AI-generated deepfakes that could undermine the integrity of democratic elections in the U.S. and elsewhere.

Deepfakes are also catching up with biometric security, with researchers pointing to emerging hacking incidents in which criminals use social engineering to steal facial recognition data and then create deepfakes to gain unauthorized access to individuals' bank accounts, for example. By 2026, attacks using AI-generated deepfakes on facial biometrics will mean that 30% of businesses will no longer consider these identity verification and authentication processes alone to be reliable, according to Gartner Inc. research. It highlighted the difficulty in being able to tell whether the face of the individual being verified is a live person or deepfake.

Businesses will need all their wits and available detection technologies about them to mitigate the risks of a wide range of emerging cyberattacks, including deepfakes, in the months and years ahead. Fortunately, technologies that can distinguish between live and fake human presence are becoming more advanced, which will help shore up cybersecurity defenses. Multifactor authentication — an account login process that requires users to enter multiple forms of identification, not just a password, for access — has long been touted as a tenet of robust cyber hygiene. In a password-free future, MFA will be an even more important deterrent.

MARKET PULSE

Aurenity adds excess lines program for public entities

■ Managing general agent Aurenity said it is launching an excess lines program for public entities.

Coverage will be provided by specialty insurer and reinsurer Vantage Risk through its Vantage Risk Specialty Insurance Co., West Hartford, Connecticut-based Aurenity said in a statement.

Aurenity will offer a mix of standalone and pool business on an excess basis with casualty limits up to $5 million for public entities as well as some scholastic, higher education and other nonprofit business, the statement said.

MGA launches parametric coverage for cyber risks

■ Descartes Insurance said it would offer companies in France parametric-based coverage for cyber risks with limits of €5 million ($5.4 million) per policy.

The trigger for the cyber shutdown coverage is a “cyber encryption incident” as part of a ransomware attack “as evidenced by the encryption of an initial file stored on a computer, server or (programmable logic controller) administered by the insured company,” a spokesman for Descartes said.

Third-party cyber specialists will determine whether an attack has taken place.

The policy is designed for small and medium-sized businesses and offers coverage based on predefined daily limits for business interruption losses, according to a statement from the insurer, which is a unit of Paris-based Descartes Underwriting SAS.

Former Dual team launches R&W MGA

■ A team of transactional risk underwriters who left Dual North America Inc. last year has launched a private-equity-backed managing general agent.

Sands Point Risk, backed by Stamford, Connecticut-based Avesi Partners LLC, will offer representation and warranties, tax liability and contingent liability coverage and other lines, the company said in a statement.

Dennis Kearns, previously president of Dual Transaction Solutions, is CEO of Sands Point. Patrick Darragh and Dan Simnowitz, also previously at Dual, are executive vice presidents. JoAnna Conte, previously a senior vice president at QBE North America, is chief operating officer.

Dual sued its three former executives and Avesi in October alleging breach of nonsolicitation agreements. The suit was settled in December, court records show.

PRODUCTS & SERVICES

Upland launches E&O, excess cyber products

■ Upland Capital Group Inc. said it has added underwriters and expanded its product offerings to include professional liability errors and omissions and excess cyber liability coverage.

The professional liability team is led by West Hartford, Connecticut-based Kate Walas, who joined Upland from Indigo Specialty Underwriters last fall. The product offers up to $10 million in limits to professional service firms. The minimum deductible is $2,500 and the minimum premium is $1,500.

Other staff on the team, who all previously worked at Indigo, are Steve Adam, senior vice president; Kevin Kiernan, vice president; and Roberta Loura, senior underwriter.

The excess cyber liability team is led by Miami-based Jackie Lee, who joined from Validus Specialty Underwriting Services Inc. in January. The product offers up to $10 million in capacity to financial services, technology, retail, construction and manufacturing risks.

The coverage can be blended with technology E&O and miscellaneous professional liability coverage, Upland said in a statement.

Thomas Riley, who also came from Validus, is senior underwriter on the excess cyber team.

WTW adds cyber cover for SMB enterprises

■ Willis Towers Watson PLC said it has launched cyber coverage for small and medium-sized enterprises in North America with annual revenue under $50 million.

Potential policyholders include startups and pre-revenue accounts, WTW said in a statement. Businesses can access quotes through self-service quoting platforms.

Typical limits of at least $5 million in any one placement may vary depending on industry and size, according to an email from a WTW spokeswoman.

WTW added that it has also allocated dedicated underwriting staff to focus on small and medium-sized enterprises and will offer tools and support on cybersecurity measures.

Origami Risk unveils work safety mobile app

■ Origami Risk LLC, a Chicago-based risk management software company, announced the launch of its cellphone app Origami Mobile, designed for use by industry safety professionals.

The app enables risk professionals, employees and contractors to conduct job site audits and inspections and report incidents from locations nationwide even in instances where Wi-Fi is unavailable, Origami said in a statement.

Users will be able to detect and report workplace operational hazards and behavior trends, monitor the effectiveness of safety programs, gather real-time incident data and provide training services to workers, according to the statement.

Safety team members will be able to use the cellphone app to tap into claims data, checklists, metrics and analytics.

Hub introduces coverage for multinational clients

■ Hub International Ltd. announced the launch of Hub Multinational Protection, a risk management services and insurance product for multinational clients that operate in five countries or fewer.

The coverage can extend to companies that have employees who travel or work abroad, sell products globally, sponsor international trips, or have physical offices, manufacturing facilities and warehouses outside the United States, Hub said in a statement.

Coverage can include global property, general liability, employee benefits liability, excess auto, foreign voluntary workers compensation, business travel accident, and kidnap and ransom.

General aggregate limits are typically $2 million, with up to a maximum of $5 million, according to an email from a Hub spokeswoman.

DEALS & MOVES

Truist agrees to sell brokerage unit

Truist Financial Corp. has agreed to sell its remaining stake in Truist Insurance Holdings Inc. to private-equity investors in a deal that values the insurance brokerage at $15.5 billion.

The bank expects to receive $10.1 billion in cash from the sale to Stone Point Capital LLC, Clayton, Dubilier & Rice LLC and other investors.

Truist sold a 20% stake in Truist Insurance, which is the world’s eighth largest insurance brokerage and the fifth largest brokerage of U.S. business, to Stone Point last year.

Heffernan purchases California brokerage

Heffernan Insurance Brokers Inc. said it has acquired Calco Commercial Insurance Services, a Sherman Oaks, California-based brokerage.

Terms of the deal were not disclosed.

Established in 2008, Calco places coverage for small businesses in the vape, medical spa and cryotherapy sectors.

Calco has joined Heffernan’s small-business division, HeffDirect.

Gallagher buys broker focusing on real estate

Arthur J. Gallagher & Co. said it has acquired John Galt Commercial Insurance Agency LLC and John Galt Insurance Agency Inc., collectively known as The John Galt Insurance Agency.

Terms of the deal were not disclosed.

The Fort Lauderdale, Florida-based broker specializes in commercial and multifamily real estate across the state, a Gallagher statement said.

John Galt has about 25 employees who are expected to transition to Gallagher, according to an email from a Gallagher spokesman. They will work under the direction of Bumpy Triche, head of Gallagher’s Southeast retail property/casualty brokerage operations.

Risk Strategies expands into Michigan with buy

Risk Strategies Co. said it has acquired Southfield, Michigan-based Ralph C. Wilson Agency Inc., its first buy in the state.

Terms of the deal were not disclosed.

Founded in 1923, Ralph C. Wilson Agency places commercial property/casualty insurance, employee benefits and personal lines. It has about 20 staff.

PEOPLE

> "We're in the middle of a very dynamic time — new technology, like how to use and react to artificial intelligence, the impact of the climate, the way we work now (in person, virtual) — the commonality is change, and the outlook for the industry is continued change."

UP CLOSE

Melissa Schellinkhout

NEW JOB TITLE: Portland, Oregon-based regional growth leader for the Pacific Northwest, Woodruff Sawyer & Co.

PREVIOUS POSITION: Portland, Oregon-based client relationship director, national middle markets, Woodruff Sawyer & Co.

OUTLOOK FOR THE INDUSTRY: We're in the middle of a very dynamic time — new technology, like how to use and react to artificial intelligence, the impact of the climate, the way we work now (in person, virtual) — the commonality is change, and the outlook for the industry is continued change. Those who are adaptable will thrive.

GOALS FOR YOUR NEW POSITION: We have built a very successful team and client base over the past two decades in the Pacific Northwest. My goal is to continue the momentum by focusing on the team. I plan to bring operational efficiencies, support and resources to ensure we are leveraging their expertise in the markets we serve. I also plan to be intentional around our brand awareness and making connections with strategic partners where our value propositions align.

CHALLENGES FACING THE INDUSTRY: How do we retain employees and challenge them to stay in the business and to be intrigued by the business? At the same time, new employees are looking for development and training. How do we as an organization adapt to those needs quickly and help our employees develop the skill sets of today?

FIRST EXPERIENCE: My first job was as an underwriter trainee in the executive protection department of Chubb Ltd., where I learned all about D&O.

ADVICE FOR A NEWCOMER: Take time to listen and observe. This business is so varied and relies on experiential learning, so open yourself to listening and learning through those experiences.

DREAM JOB: I would love to have a more formal role around coaching. Someday I'd like to create a nonprofit, to help young athletes play softball and develop in the game longer before they join club sports. So many kids, especially girls, self-select out of sports early.

COLLEGE MAJOR: I had a double major in marketing and information systems at the Dolan School of Business at Fairfield University.

LOOKING FORWARD TO: We have an exceptional team in the Pacific Northwest, and I am eager to continue strengthening the group while leveraging Woodruff Sawyer's broader organizational resources and expertise.

FAVORITE MEAL: Fresh Dungeness crab, preferably that I helped catch on the Oregon coast.

FAVORITE BOOK: "Wild," by Cheryl Strayed. Her journey, and the risks she took on the Pacific Coast Trail, was so inspiring.

HOBBIES: For the past six years, I've coached Little League softball. I played softball for Fairfield University for four years, and teaching the game is so rewarding. I also love gardening.

FAVORITE TV SHOW: "Friends." I grew up with it, it makes me laugh and feel good, and it's short. I go back to it time and again.

ON A SATURDAY AFTERNOON: You can find me at a field, gym or pool watching my girls participate in sports. I have two active teenagers, and they play softball, volleyball and swim.

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

Marsh LLC named **Susan Gonzales** Houston energy hub and office leader. She succeeds Greg Larson, who was named South Central sales leader for Marsh. Previously, Ms. Gonzales was U.S. head of energy casualty at American International Group Inc. She was a 2020 *Business Insurance* Women to Watch winner.

Burns & Wilcox Ltd. appointed Chicago-based **Andy Wood** vice president and practice group leader, professional liability. Previously, Mr. Wood was a senior vice president at Hiscox Ltd.

Axa XL, the commercial insurance and reinsurance business of France's Axa SA, named New York-based former Zurich North America executive **Michelle Chia** chief underwriting officer for cyber in the Americas. Ms. Chia was most recently head of professional liability and cyber for Zurich North America.

Chubb Ltd. named **Seth Gillston** executive vice president, head of North America industry practices. Mr. Gillston, who will be based in New York, will continue to serve as private equity industry practice leader. He joined Chubb in 2000.

Zurich North America named Chicago-based **Carrie Goesel** head of excess and surplus financial lines, a newly created position. Previously, Ms. Goesel was vice president, national financial institutions leader, at CNA Financial Corp. Prior to that, she was senior vice president, financial institutions, at Chubb Ltd.

Alliant Insurance Services Inc. hired former USI Insurance Services LLC executive **Michael Lezynski** as executive vice president in its Alliant Americas division. Red Bank, New Jersey-based Mr. Lezynski was previously president of USI's New Jersey operations.

OFF BEAT

Judge to tribute band: Let´s groove

An Earth, Wind & Fire tribute band wants the real band to remember all the times it has supposedly allowed other such bands to use its name and music, and a federal judge said the dupe band should have its day in court to prove so.

Sued by the holding company that owns the name and rights of the legendary R&B group, the tribute band "Earth Wind & Fire Legacy Reunion" is accused of trademark infringement for using the name to promote shows, arguably aiming to confuse fans, according to Billboard magazine.

The tribute band's counterargument was that the real group, which continues to tour, abandoned the intellectual property rights to its name because it had allowed plenty of other tribute bands to use its name without repercussion — so many, in fact, that it could no longer claim any exclusive legal rights to it, according to the magazine.

What would George Carlin say?

One has to wonder what series of well-curated expletives the late comedian George Carlin would use in a rant if he knew he was brought back to life for a comedy program featuring his likeness created using generative artificial intelligence.

Mr. Carlin's estate had its own response: a lawsuit filed in federal court in California over the release of the comedy special that used technology to mimic the comedian's unique voice and style of humor for "'George Carlin: I'm Glad I'm Dead," according to The Hollywood Reporter.

The lawsuit accuses the company and its creators of using without consent or compensation Mr. Carlin's "entire body of work consisting of five decades of comedy routines" to train an AI chatbot to write the script.

GOLF CLUB MAKER TAKES SWING AT BIG BOX STORE

Joining the ranks of five-pound mayonnaise jars, couches and gooey chicken melts, golf clubs are the new thing at Costco and not everybody is playing fair, according to a lawsuit filed by equipment manufacturer TaylorMade Golf Co., claiming the wholesale company copied its designs.

Kirkland Signature irons were a much-anticipated addition to Costco's offerings, and the new product line allegedly hit the market out of bounds when TaylorMade discovered that the $499 clubs — which sold out "within hours" — were similar to its own designs, according to Golf magazine.

TaylorMade, in a lawsuit filed in federal court in California and accessed by the publication, alleges the iron's design infringes on several patents tied to the company's popular P790 iron that has a similar hollow-cavity design. Also named in the suit is Southern California Design Co., which designed the Costco versions.

Happy customers cozy up to fraud

So-called "friendly fraud" is not so friendly to the bottom line of businesses grappling with such issues as bogus returns and credit card chargebacks, according to a report from online security company Sift.

As reported in Fast Company, legitimate customers participating in first-party fraud is on the rise. The incidents occur when customers file a fraud claim or chargeback despite being satisfied with a purchase.

"Sometimes it can be done unintentionally — when, for example, a family member makes a purchase with someone's credit card without their knowledge. Other times, friendly fraud is committed intentionally," Sift CEO Kris Nagel explained.

Rappers allege their cereal was dissed

Rappers Snoop Dogg and Master P have sued Post Consumer Brands and Walmart, alleging both companies reneged on a marketing agreement and kept their cereal off shelves to sabotage their brand, according to NPR.

The lawsuit documents how Calvin Broadus, known as Snoop Dogg, and Percy Miller, known as Master P, created Broadus Foods in 2022 to inspire opportunities for minority-owned brands.

The suit argues that when the two rappers approached Post to get support for Snoop Cereal, the food manufacturer attempted to outright buy the brand, which the rappers rejected, saying they believed it would "destroy the whole purpose of leaving the company to their families."

Post then entered a partnership promotion agreement with Broadus Foods, an agreement that was never honored and resulted in fans unable to locate boxes of Snoop Cereal, the lawsuit contends. The rappers argue Post "pretended to be on board" with the duo's goals.