March/April 2023 RMmagazine.com

RISK MANAGEMENT

Using Artificial Intelligence in Employment Decisions
pg. 4

Employer Obligations in Disaster Response
pg. 26

BACKUP PLANS

How to Preserve Institutional Knowledge as Employees Depart

A publication of RIMS

Real stability isn't just measured by size

A+
AM BEST RATED

FORTUNE 100
COMPANY

A+
STANDARD & POORS

Management Liability and Specialty

We are proud to be part of a company that's among the largest in our industry. But we take the greatest pride in the strong, stable relationships we've built with our partners through our commitment to service.

nationwide-mls.com

Nationwide®

Volume 70, Issue 2

contents

22

FEATURES

Backup Plans • 22

With more workers retiring or leaving for new opportunities, how can organizations ensure that vital knowledge and experience are not lost?

by TREVOR TREHARNE

Employer Obligations in Disaster Response • 26

As organizations navigate increasingly frequent and severe natural catastrophes, there are several employment law considerations they must take into account.

by SALLY R. CULLEY

26

COVER: SHUTTERSTOCK/TREETY
THIS PAGE: TOP: SHUTTERSTOCK/BAKHTIAR ZEIN; BOTTOM: SHUTTERSTOCK/STOKKETE

FOREFRONT

4 Using AI in Employment Decisions
Regulators are scrutinizing the use of AI-based technology for potential bias.

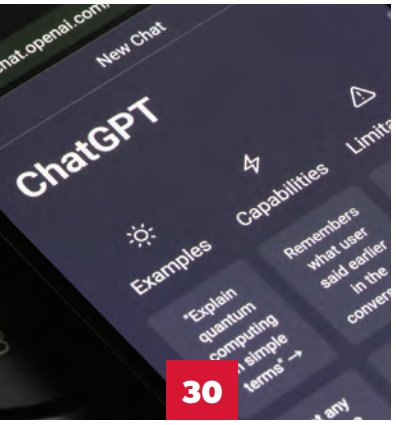
8 Assessing Third-Party ESG Risks
Companies need to protect themselves from inheriting unknown ESG risks from partners.

12 6 Tips for Improving Network Security
These best practices can help organizations boost security and control insurance rates.

16 How to Create Greater DEI Accountability
By demonstrating accountability, companies can enhance DEI initiatives and mitigate risks.

RISKWORLD PREVIEW

20 A World of Resilience at RISKWORLD
What to expect at this year's RISKWORLD conference and exhibition in Atlanta.



DETAILS

3 Preface
Taylor Swift fans take on Ticketmaster.

30 Findings
Risks of ChatGPT, new business email compromise scams, and rising civil unrest.

32 Hindsight
The latest facts and figures on risk.

RISK MANAGEMENT

Editor in Chief
Morgan O'Rourke, *morourke@RIMS.org*

Managing Editor
Hilary Tuttle, *htuttle@RIMS.org*

Art & Production Manager
Andrew Bass, Jr., *abass@RIMS.org*

ADVERTISING
Account Executive
Ted Donovan, *tdonovan@RIMS.org*
T: (212) 655-5917

CIRCULATION
Quality Circulation Services
Carole Ireland, *carole@qcs1989.com*
T: (413) 442-7300

Risk Management
P.O. Box 3, Congers, NY 10920
Customer Service: (866) 512-3111
Local: (845) 267-3004
Fax: (845) 267-3478

A publication of RIMS

Chief Executive Officer
Gary LaBranche, *glabranche@RIMS.org*

Member of BPA WORLDWIDE

THIS PAGE: TOP PHOTO: SHUTTERSTOCK/PROSTOCKSTUDIO; BOTTOM PHOTO: SHUTTERSTOCK/TADA IMAGES

Risk Management Magazine (ISSN 0035-5593) is published 7 times per year, with combined issues in Jan./Feb., Mar./Apr., May/June, July/Aug., Sept./Oct., Nov./Dec., and a special issue in April, by the **Risk and Insurance Management Society, Inc.** Offices at 228 Park Ave S, PMB 23312, New York, NY 10003-1502; (212) 286-9364; Fax (212) 922-0716. Volume 70, Issue 2.

Subscription rate: $80. Periodicals postage paid in New York and additional mailing locations. POSTMASTER send change of address notices to *Risk Management Magazine*, P.O. Box 3, Congers, NY 10920.

AN AWARD-WINNING PUBLICATION

AZBEE AWARDS WINNER · EXCEL AWARDS WINNER · FOLIO: EDDIES WINNER · GD:USA AWARDS WINNER

CONTACT US

All submissions and letters should be sent to:

Morgan O'Rourke
Editor in Chief
Risk Management
228 Park Ave S, PMB 23312
New York, NY 10003-1502
morourke@RIMS.org
T: (212) 655-5922

www.RMmagazine.com

A Swift Reaction

This year, RISKWORLD comes to the Georgia World Congress Center in Atlanta from April 30 to May 3. Everyone who is anyone will be there in Atlanta, including, apparently, mega-star Taylor Swift, who will be performing at the nearby Mercedes-Benz Stadium from April 28 to 30.

While the education session lineup at RISKWORLD is impressive, it is safe to say Taylor already has more than enough on her mind. Her previous concert tour in 2018 broke the record for the highest-grossing tour in U.S. and North American history, bringing in more than $260 million. Her follow-up tour in 2020 was canceled because of COVID-19, so excitement and hype for these shows has been building for about five years.

However, getting a ticket to one of her concerts on this tour has been a nightmare. When millions of fans tried to buy tickets during a Ticketmaster presale in November, many encountered site crashes, endless wait times and tickets that appeared to be available but had already been purchased, often by scalpers or bots. The demand was so high and the site issues so pervasive that Ticketmaster cancelled the general public sale. Fans then turned to the secondary ticket market, only to find tickets selling for thousands of dollars apiece.

Due to serious concerns about the questionable business practices underlying this mess, a group of prospective ticket buyers sued Ticketmaster and its parent company, Live Nation, for fraud, price fixing, misrepresentation and antitrust violations. The lawsuit seeks to prevent Ticketmaster from engaging in similar practices in the future and asks that the court assess a civil penalty of $2,500 against the company for every violation of California's Unfair Competition Law.

The fiasco also prompted the Senate Judiciary Committee to hold hearings in January to look into anticompetitive behavior in the ticketing industry. Live Nation was reportedly also the subject of an antitrust investigation by the Justice Department that began even before the Taylor Swift situation.

This is the latest in a long list of Ticketmaster and Live Nation controversies. Thirty years ago, Pearl Jam testified before Congress about Ticketmaster's pricing policies and essentially scrapped a tour at the height of their popularity because they refused to perform at Ticketmaster-affiliated venues. In recent years, the company practice of "dynamic pricing" has drawn ire from fans as it pushed ticket prices for countless artists ranging from Bruce Springsteen to Harry Styles to stratospheric levels. This time, however, Taylor Swift's immense popularity may mean that it won't be so easy for Ticketmaster to just "Shake It Off."

–Morgan O'Rourke
Editor in Chief

ADVERTISERS INDEX

Liberty Mutual, **9**
www.business.libertymutual.com

Nationwide, **2nd Cover**
https://nationwide-mls.com

Old Republic Insurance Group, **4th Cover**
www.orgig.com

Philadelphia Insurance Companies, **17**
www.PHLY.com

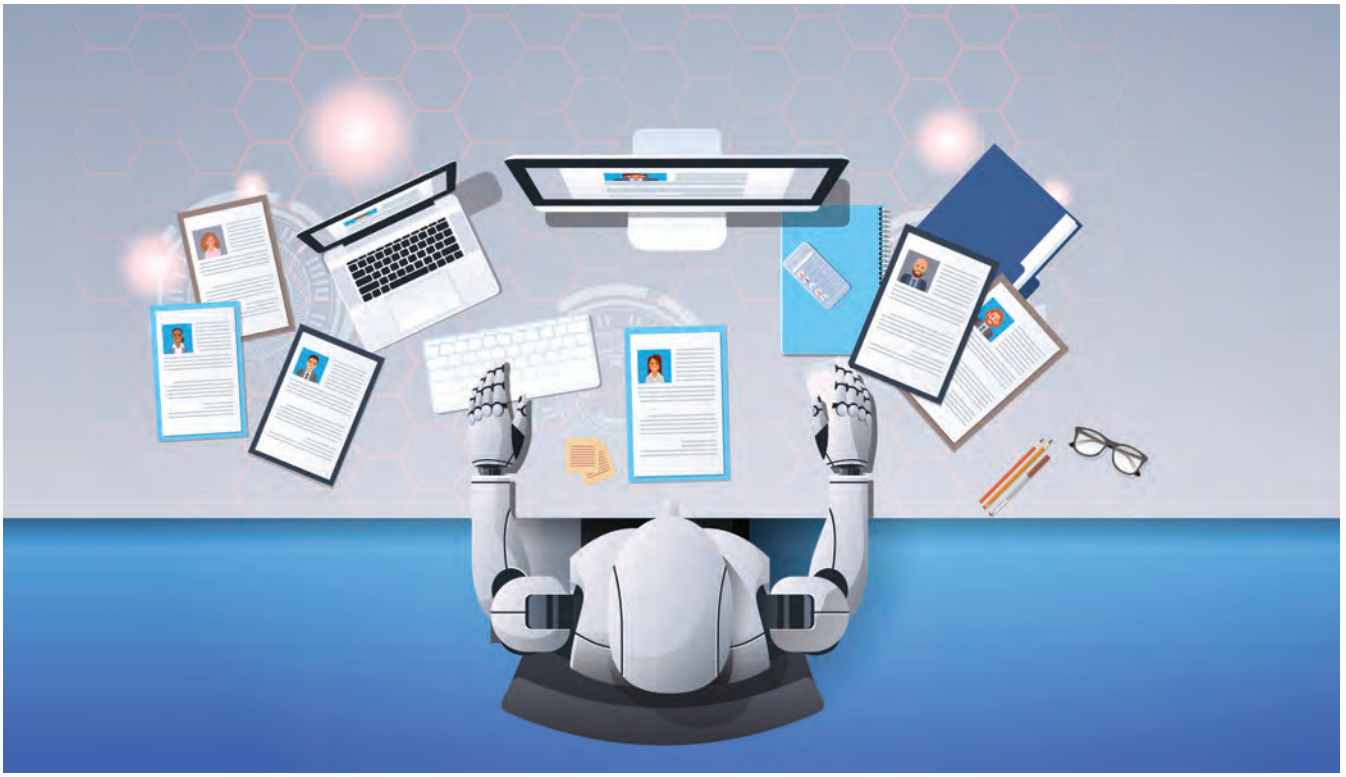
Riskonnect, **5**
sales@riskonnect.com

The Hartford, **3rd Cover**
www.TheHartford.com/specialization

Zurich North America, **11**
www.zurichna.com

INSIDE

Third Party ESG Risks 8
Improving Network Security ... 12
DEI Accountability 16
RISKWORLD Preview 20



Using Artificial Intelligence in Employment Decisions

by Laura Lapidus

Artificial intelligence has been defined as a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations or decisions influencing real or virtual environments. Research by the Society for Human Resource Management found that approximately 25% of organizations use AI for human resources processes including recruitment, hiring, performance and termination decisions. This has caught the attention of the Equal Employment Opportunity Commission (EEOC), the agency that enforces federal anti-discrimination laws in the United States.

The draft EEOC Strategic Enforcement Plan for 2023 to 2027 indicates that its enforcement priorities include "employment decisions, practices or policies in which the use of technology contributes to discrimination based on protected characteristics, such as the use of software that incorporates algorithmic decision-making or machine learning, including [AI]."

On January 31, 2023, the EEOC held a public hearing to explore the benefits and risks of employer use of AI, software and other emerging technologies that use algorithms in employment decision-making, collectively known as automated decision-making (ADM) tools. The hearing followed the May 2022 EEOC guidance titled "The Americans with Disabilities Act and the Use of Software, Algorithms, and Artificial Intelligence to Assess Job Applicants and Employees." The hearing and the guidance are part of an EEOC initiative that focuses on ensuring that the use of emerging technologies in employment decisions complies with federal civil rights laws.

CHALLENGES OF ADM TOOLS

Human resources departments use ADM tools in many forms, such as resume scanners, video interviewing and testing software, as well as monitoring software to screen or evaluate applicants and employees. During the hearing, proponents noted

SHUTTERSTOCK/PROSTOCKSTUDIO

Covering *Every* Risk, *Every* Business Faces.

At Riskonnect, we believe that seeing all your risk data should be as easy as putting on your pants. Our integrated software brings everything you need, into one place, so you can collaborate, act – and protect your business from anything.

Button up your approach to risk management at Booth #1031

Connect with us!
sales@riskonnect.com | +1 770.790.4700

riskonnect
Integrated Risk Management Solutions™

that ADM tools are more efficient and less costly, and remove human bias from employment decisions.

Others argued that the use of ADM tools in employment decisions may mask and perpetuate bias or create new discriminatory barriers. One problem is that decisions about candidates are based upon data that is input into the ADM tool. If the data is biased, the resulting decisions based upon that data may reflect and/or reinforce that bias. For example, some ADM tools try to predict which applicants will be good employees by comparing them to current successful employees. As Amazon found after implementing a now-discontinued AI-based recruiting tool, if a company hires predominantly white men, the algorithm may conclude that white men will be more successful and rate them higher than others, perpetuating bias.

Some of the characteristics for which ADM tools screen could also be proxies for protected classes such as gender, race and age. For example, Black and Latino applicants are often overrepresented in data regarding records of criminal legal proceedings, evictions and credit histories. An algorithm that screens out candidates based on these data points may have a disparate impact on those protected classes and violate Title VII of the Civil Rights Act of 1964.

BEST PRACTICES FROM THE EEOC

The EEOC guidance focuses solely on factors that employers should consider when using ADM tools in order to prevent disability discrimination under Title I of the Americans with Disabilities Act of 1990 (ADA). The EEOC notes that ADM tools may violate the ADA when an employer:

- Fails to provide a reasonable accommodation necessary for an applicant/employee to be rated fairly and accurately by the algorithm
- Relies on an ADM tool that intentionally or unintentionally screens out an individual with a disability, even though that individual can do the job with a reasonable accommodation
- Uses an algorithmic decision-making tool for job applicants or employees that violates the ADA's restrictions on disability-related inquiries and medical examinations

The guidance maintains that an employer must provide a reasonable accommodation to an individual with a disability so that they can be rated fairly and accurately, absent an undue burden on the employer. For example, when a company administers a knowledge test that uses a keyboard and an applicant with limited dexterity requests an accommodation, the employer should provide an accessible version of the test. If one is not available, it should consider providing an alternative test.

The guidance also states that an ADM tool may violate the ADA if it screens out individuals with disabilities by lowering their performance or by causing them to fail to meet a selection criterion, resulting in a lost job opportunity. For example, a chatbot that screens out applicants with employment history gaps may violate the ADA if the gaps were due to a disability or the need to undergo treatment for a disability.

Another concern is that a disability may reduce the accuracy of an assessment if the circumstances of the disability are not considered. An ADM tool that screens out an individual with a disability because the individual cannot perform a job under typical working conditions may fail to take into account the possibility that the individual may be entitled to an accommodation that would enable them to do the job.

Importantly, the EEOC advises that employers may be liable for discrimination even if the ADM tools are designed or administered by a vendor or other entity. The guidance also states that employers cannot simply rely on a vendor's statement that the tool is free of bias, as those assessments may only focus on protected characteristics other than disability. Because each disability is unique, a general assessment for bias may not reveal all the potential ways someone with a disability may interact with the tool, and the ways in which the tool may impact that individual.

The guidance takes the position that any test or tool may violate the ADA if it poses disability-related inquiries or seeks information that is considered a medical examination prior to a conditional offer of employment. The guidance notes that an assessment includes disability-related inquiries if it asks job applicants or employees questions that are likely to elicit information about a disability or directly asks whether an applicant or employee is an individual with a disability. It qualifies as a medical examination if it seeks "information about an individual's physical or mental impairments or health."

LOOKING AHEAD

To help mitigate the risk of discrimination while using ADM tools, employers should work with experienced employment counsel to assess the EEOC guidance and consider implementing some of the practices it has outlined. Organizations should also monitor federal, state and local guidance in this area to ensure that any ADM tools that it may use comply with all anti-discrimination laws. Employers should also anticipate additional EEOC guidance and enforcement regarding the use of ADM tools, as well as state and local legislation. For example, New York City enacted a law that will require, among other things, employers to perform a bias audit and to provide notice prior to using artificial intelligence in employment decisions. Although ADM and other emerging technologies may have many advantages, they must be carefully created, implemented and monitored so that the risks do not outweigh the benefits. R

Laura Lapidus is management liability (EPL) risk control director at CNA Insurance.

ATLANTA 2023
RISKWORLD®
APRIL 30–MAY 3

GET AN EDGE IN AN EVOLVING WORLD

RISKWORLD Marketplace is the one-stop shop to learn about solutions and services that cover all aspects of risk management. RISKWORLD is excited to welcome 40+ new exhibitors to the Marketplace. This is the most comprehensive exhibit hall and where you'll discover innovative products, applications, and solutions from a diverse selection of vendors.

INNOVATION HUB
Exciting 20-minute presentations on developments in emerging risks, claims and cyber risks.

Sponsored by wtw

THOUGHT LEADER THEATER
Succinct, interactive discussions on a variety of topics.

Sponsored by Swiss Re Corporate Solutions

GLOBAL STUDIO
Network with attendees from all over the world and hear presentations with a global focus.

Sponsored by TCN Global Risk Consultants

WELLNESS ZENTER
Presentations that can guide your next steps toward health and productivity in the workplace.

Sponsored by sedgwick

MARKETPLACE RECEPTION
ATLANTA CITY FOOD MARKET
MONDAY, MAY 1 | 4:00 PM – 5:00 PM

Atlanta has a diverse culinary scene. Sample a selection of traditional hand-held Argentine empanadas.

MARKETPLACE SOCIAL LUNCHEON
ATLANTA'S FINEST
TUESDAY, MAY 2 | 12:00 PM – 1:15 PM

Take a break and enjoy some of ATL's best cuisine: smoked brisket, barbecue chicken, mac n' cheese, Georgia grown salad, and peach cobbler.

MARKETPLACE SOCIAL RECEPTION
LITTLE FIVE POINTS
TUESDAY, MAY 2 | 4:00 PM – 5:00 PM

Reconnect with your colleagues over barbecue pork sliders from one of Atlanta's coolest neighborhoods.

MARKETPLACE SOCIAL LUNCHEON
"EXPLORE THE GASLAMP DISTRICT" A SAN DIEGO EXPERIENCE: RISKWORLD 2024 KICKOFF
WEDNESDAY, MAY 3 | 12:00 PM – 1:30 PM

Get ready for RISKWORLD 2024 in San Diego with some Gaslamp District favorites: Latin-style rotisserie chicken, beef BBQ, arroz amarillo, cinnamon sugar churros, Baja-style corn, and frijoles charros.

MAKE SURE YOU'RE READY TO MEET THE WORLD'S CHANGING NEEDS.

REGISTER NOW

www.RIMS.org/RISKWORLD

RIMS® the risk management society

Assessing Third-Party ESG Risks

by Marion Jones

Environmental, social and governance (ESG) concerns have never been more important to companies that want to protect against reputation and regulatory risks. However, many companies do not consider how third-party vendors they contract with can affect their ESG profiles. By incorporating basic ESG due diligence evaluations into third-party risk assessments, companies can protect themselves from inheriting unknown risks from vendors and other partners.

A GROWING FOCUS ON ESG ISSUES

The increased public attention on ESG issues is unlikely to be a short-term fad. Global ESG assets are expected to grow from an estimated $35 trillion in 2022 to $50 trillion by 2025, according to a Bloomberg Intelligence report. In addition, a 2022 University of Oxford and Protiviti poll of global business executives found that 64% expected corporate spending on managing environmental risks to increase in the coming years.

Oxford and Protiviti also found that 78% of business executives believe ESG reporting will become mandatory in the next decade. This would further cement ESG as a long-term concern for businesses and could potentially lead to hefty penalties for ESG violations for issues like environmental pollution, workplace harassment and data privacy violations. In fact, regulatory activity has already started to ramp up. In 2021, for example, the U.S. Securities and Exchange Commission (SEC) announced that it was creating an enforcement task force focused on ESG issues, and would be paying particular attention to climate-related risks. It also issued a proposal last year that would require publicly listed companies to include more extensive disclosures on climate-related risks within their regulatory filings.

EVALUATING AND MINIMIZING THIRD-PARTY ESG RISKS

According to a 2020 Mastercard study, the average third-party risk manager was responsible for assessing over 50 new vendors each year in addition to managing already contracted vendors. And some companies can have more than 5,000 third-party vendors. Such large volumes of third-party relationships mean third-party risk evaluations are often limited to immediate security concerns like ensuring third parties have baseline security controls in place, but do not extend to ESG-related issues.

Organizations cannot assume third parties hold themselves to the same ESG standards they do. They also must remember that they inherit any ESG risk from a third party with which they do business. For example, if a vendor for an organization is found to have violated labor or environmental laws, it can negatively impact the contracting organization's public image in addition to the vendor's. Further, losing a key vendor can seriously degrade the organization's business operations. Under some circumstances, such as cases of human trafficking or violations of the Uyghur Forced Labor Prevention Act, the organization could also be held at least partially criminally or civilly liable for the vendor's misconduct.

Organizations can begin to evaluate

SHUTTERSTOCK/SUTTHIPHONG CHANDAENG

third-party ESG risks by taking the following steps:

1. Identify the ESG risks that are relevant to your organization and important to your stakeholders. Companies should first determine which ESG risks their company may be exposed to and which issues are important to their employees, board members, customers and other stakeholders. Companies should also understand what ESG-related regulations, if any, they may need to follow. The identification step is especially important if an organization has limited resources and needs to understand which areas have the greatest risk exposure and must be prioritized.

ESG issues are constantly changing, so it is essential to regularly reevaluate ESG priorities and obligations. For example, following Russia's invasion of Ukraine in February 2022, doing business with firms affiliated with the Russian government became unpalatable to many companies and their investors. New legislation and regulations may also force businesses to reevaluate ESG risks.

2. Gather ESG risk information on vendors from internal and external sources. Once companies identify which ESG issues are most important, the next step is to gather data on vendors to evaluate risks associated with these issues. This data collection should be conducted through both internal or external sources. For example, companies often have vendors complete questionnaires to identify and evaluate security concerns and controls. Including ESG-related topics in these questionnaires could help organizations understand how a third party evaluates its ESG risks and any mitigation steps it takes.

Organizations are increasingly releasing their own ESG reports, which can also be a good starting point when evaluating a vendor's ESG profile. According to the Governance and Accountability Institute, more than 90% of S&P 500-indexed companies and a growing number of companies in the Russell 1000 index now publish sustainability reports.

Organizations can also utilize outside auditors to help evaluate a third party's ESG risks and mitigation efforts. Many organizations have emerged in recent years that regularly evaluate and score companies on their ESG exposure and mitigation efforts. Outside evaluation and auditing can provide another level of assurance to an organization's stakeholders that is it taking ESG risks seriously.

3. Assess ESG risks systematically. Once companies have a system in place to collect data on a third party's ESG risks, they should use a standardized scoring method to assess the data and determine an acceptable level of risk. A systematic scoring method will help companies evaluate a third party's inherent risk, which is the risk posed by the third party absent any controls. It will also help identify the residual risk, or the risk level that remains from the third party after controls and other mitigation efforts are in place. Multiple tools are available that integrate and evaluate third-party data to improve risk assessment and decision-making.

Using a standard scoring mechanism to assess third parties can help companies determine if a vendor poses enough ESG risk to require further evaluation, assess how effective mitigation efforts are, and ensure that the risk posed by the third party does not exceed the organization's risk appetite.

Evaluating ESG risks can seem like a daunting task to already overworked risk management teams. However, by incorporating systematic ESG-related assessments into already established due diligence procedures, organizations can add a layer of protection to ensure they are not exposed to unknown ESG risks from third parties. R

Marion Jones, CISSP, CRISC, is a technology consultant focused on third-party risk management and cybersecurity, and previously worked for the U.S. federal government in the intelligence and law enforcement fields.

RIMS-CRMP

RIMS-Certified Risk Management Professional

Get Certified

Start Your Application Today

Validate your performance ability, technical knowledge, and commitment to excellence—earn the RIMS-Certified Risk Management Professional (RIMS-CRMP) certification.

Add the only competency-based risk management credential to your professional profile to:

- Stand out in the job market
- Increase your earning potential
- Elevate your status
- Show your commitment to ethics
- Raise the standards of your profession

ANSI Accredited Program
PERSONNEL CERTIFICATION
#1223

Learn more and apply **www.RIMS.org/Certification**

RIMS
the risk management society

6 Tips for Improving Network Security

by Karen Kukoda and Monica Shokrai

In recent years, the rising cost of cyber insurance premiums has become a major concern for enterprises of all sizes. This rate environment has been driven, in part, by the drastic increase in cyberattack claims globally. In fact, S&P Global analysts recorded a staggering 232% increase in ransomware claims from 2019 to 2021. Due to the interconnected nature of cyberattacks, cyber insurers are even reevaluating what gets covered—such as social engineering campaigns or state-sponsored attacks—to ensure that they can sustain systemic risks.

Given these market conditions, improving cybersecurity practices is essential for organizations to better manage costs. For example, better cyber hygiene and continuous monitoring can reduce the likelihood of a claim and help companies obtain insurance coverage at more affordable rates. The following are six cybersecurity best practices that can help organizations get started on hardening their networks:

1. Multi-Factor Authentication

Multi-factor authentication (MFA) and two-factor authentication (2FA) have gained widespread adoption over the past few years as companies increasingly require it for both employees and users. MFA is one of the simplest measures to implement for an organization to verify whether a user logging into the network is really who they say they are. Attackers are always looking for ways to bypass security measures or use social engineering tactics like spamming push notifications to a user's device to get into the network. This is why organizations should enforce MFA for all externally accessible login portals and for any sensitive internal applications.

2. Backups and External Storage

Attacks that breach a company's data, encrypt important files or threaten to leak sensitive information can severely disrupt business operations, leading to major financial and reputational costs. According to research from IBM, the global average cost of a data breach in 2022 was $4.35 million, and in the United States, the average was more than double that at $9.44 million. It is critical to have backups and external record storage to use in the event of an attack. This also demonstrates to insurers that the costs can be kept down with this ability to quickly get back up and running. In particular, backup and external storage solutions can help with getting operations restored, decreasing the likelihood of intellectual property loss and ensuring valuable records are secure. Companies are also increasingly using cloud-based services as a way to maintain a copy of their networks in case of a cyberattack that stalls operations.

3. Identity and Access Management

It is critical for organizations to be able to demonstrate the consistent use of identity and access management (IAM) systems. Wherever employees or other seemingly authorized users access the network, IAM helps to monitor for potential unusual or malicious activity. This is important because attackers can dwell in victim networks for weeks at a time without being caught. When left unattended, threat actors can take command of a breached account to infiltrate a company's networks and deploy ransomware,

SHUTTERSTOCK/JIRSAK

ZURICH

Zurich program sessions at RIMS RISKWORLD 2023

60-minute sessions

Claims Management The missing link in workers' comp: How inclusion and belonging affect recovery from injury	**Elise White** Business Practices & Project Consultant, Zurich North America **Daniel Maxson** Corporate Safety Director, New South Construction	**May 1, 2023** **2:45 – 3:45 p.m.** Room 4 GWCC Session code: 590
Claims Management Anti-social behavior: How social trends are causing nuclear verdicts, and how corporations can fight back	**Allen Kirsh** Head of Claims Judicial and Legislative Affairs, Zurich North America **Deborah Broom** VP, Risk Manager, Tutor Perini	**May 3, 2023** **1:45 – 2:45 p.m.** Room 10 GWCC Session code: 406

20-minute sessions

Claims Event-driven litigation: Building a defense in the court of public opinion	**Japhet Boutin** Claims Handling Director – Financial & Professional Lines, Zurich North America	**May 1, 2023** **3:30 – 3:50 p.m.** Thought Leadership Theater GWCC Session code: 437
Emerging Risks The Future of Risk unveiled in the World Economic Forum's 2023 Global Risks Report	**Robin A. Kemper** Senior Risk Engineer, Zurich Resilience Solutions	**May 2, 2023** **10 – 10:20 a.m.** Global Studio GWCC Session code: 440
Risk Modification Prepare to play a pivotal role in how consumers receive goods by understanding your warehouse and logistics pipeline	**Andrea Blair** Director of Business Resilience, Zurich Resilience Solutions	**May 2, 2023** **10 – 10:20 a.m.** Thought Leadership Theater GWCC Session code: 520
Emerging Risks Autonomous technologies: Benefits and risks of the coming age of self-directed machines	**Joe McLean** Technical Underwriting Manager, Zurich North America	**May 2, 2023** **10:30 – 10:50 a.m.** Innovation Hub GWCC Session code: 483

steal files, install cryptominers or prepare for a future attack. IAM can help reduce the likelihood of these attacks by providing an early warning of suspicious activity.

4. Response Partners

An important part of crisis response is proactively engaging with outside support. Outside legal experts and experienced general counsel can work with forensic responders after an attack occurs to find out what legal liabilities and risks can come from the event. Incident responders can assist an organization's security team to identify the threat actor and provide recommendations on how to stay safe in the future. Keeping incident response and legal expertise on retainer can save money when an incident occurs. To help ensure coverage for associated expenses, these experts should be approved in advance by the cyber insurance provider.

5. Tabletop Exercises

Tabletop exercises help prepare security teams to handle whatever attackers throw at them. They also prepare executive teams to manage, lead and communicate during a crisis, ultimately helping to reduce losses and mitigate reputation risk. The objective of tabletop exercises is not to lecture on the intricate tactics, techniques and procedures of threat actors, but to practice responding to an attack. Government agencies like the Cybersecurity and Infrastructure Security Agency (CISA) offer sample tabletop exercises for organizations. For those that want something more tailored to their specific circumstances, private sector service providers can also help develop relevant, realistic scenarios. If security teams and executives can demonstrate their understanding of cyber crisis response procedures as part of the cyber insurance application process, this can help secure more favorable coverage terms or rates.

6. Zero Trust

A zero trust security framework mandates that trust—in users, networks and devices—must be established via multiple mechanisms and continuously verified before access is granted to data and resources. This limits unauthorized access in the environment, allowing organizations to significantly reduce risk from compromised accounts. According to estimates from IBM, organizations that maintain a zero trust framework can save an average of $1 million in breach costs compared to those that do not. Adoption is rising, and 36% of CISOs surveyed by PwC said they had already started implementing components of a zero trust framework.

The global average cost of a data breach in 2022 was $4.35 million, and in the United States, the average was more than double that at $9.44 million.

Karen Kukoda is principal of Mandiant strategic partnerships at Google Cloud. **Monica Shokrai** is head of business risk and insurance at Google Cloud.

CYBER THREATS

Since 1954, *Risk Management* has provided readers with the latest in risk management news, insight and analysis.

Whether it is dynamic issues of cybersecurity, the emerging risk landscape and reputational risk, or the fundamentals of cyber insurance and disaster preparedness, or anything in between, **we are the authority** on information you need to meet the challenges of today's evolving business landscape.

Subscribe to *Risk Management* magazine today.

Visit **RMmagazine.com/subscribe** for more details.

RISK MANAGEMENT

How to Create Greater DEI Accountability

by Natasha Nicholson

As sociologist and researcher Dr. Evelyn R. Carter wrote in a recent article for *Harvard Business Review*, "DEI initiatives are futile without accountability." DEI involves change, which is inherently difficult, and it is even harder if there is no way of knowing whether we have made progress. That is where accountability comes in. Assessing our starting point, setting our goals and then determining how close we are to getting there can give us insight into how far we have come and provide the incentive that everyone needs to push forward. Critically, accountability shows that we take our responsibilities seriously and provides evidence that we are acting on our promises.

DEI accountability also helps reduce risk. When organizations clearly demonstrate and articulate accountability regarding DEI, they strengthen these initiatives and protect against reputation damage and associated risks. That is because they are providing proof through their actions that the organization places value on having diversity at all levels, and has enabled all employees to feel included and treated equitably.

Without accountability, it is easier to be accused of ignoring the needs of employees and the demands of customers, ultimately chipping away at the organization's reputation. This has serious implications for the organization and its operations. For example, it could contribute to an eroding culture that affects recruitment and retention or, in extreme cases, could lead to cases of misconduct and harassment.

Having an effective approach to DEI accountability has the benefit of uniting employees and managers around a common goal. It also creates transparency, which is essential to foster trust with both employees and customers. It also helps stakeholders understand what is working, what is not working and where to make course corrections, leading to better results in the future.

GETTY/KOH SZE KIAT

6 WAYS TO DEMONSTRATE ACCOUNTABILITY

While everyone is responsible for DEI, business leaders are at the forefront of organizing their teams to gather the evidence on DEI progress and turn that data into a compelling narrative that will show the organization's commitment. Every organization has a unique history and culture, so there is no single approach that will work for all. Each organization must choose a set of strategies and accountability measures that will best help to meet the challenges and reveal the opportunities that come with creating a more diverse, equitable and inclusive organization. Along with the related model (see page 18), the following six strategies can help demonstrate DEI accountability:

1. Implement a three-step DEI accountability model. The model breaks down the accountability process into three parts: 1) committing to a strategy; 2) building a program; and 3) creating an enabling environment. Each step carries with it a set of actions, accountability measures and possible assessment questions. Note that this model is an example and that your measures and assessments may be different, depending on your organization's needs.

STEPS	ACTIONS	ACCOUNTABILITY	ASSESSMENT
COMMIT to and develop a bespoke diversity, equity and inclusion strategy	■ Create awareness and understanding ■ Build a case for change ■ Establish leadership alignment ■ Create and implement a plan	■ Outline goals, priorities, objectives and measurements ■ Define leadership accountability and aligned incentives	■ What is your level of progress to plan? ■ What are you learning along the way? ■ What adjustments do you need to make?
BUILD an inclusive program designed around employee experiences	■ Design methods to seek out and attract diverse talent ■ Create systems for removing bias from HR processes ■ Establish a measurement dashboard ■ Focus on uncovering and harnessing the value of diversity	■ Track progress on areas like recruitment, retention, advancement and pay equity ■ Gather employee feedback—formally (surveys, polls) and informally (regular in-person check-ins)	■ What progress have you made on attracting and retaining diverse talent? ■ Do employees feel included and have a sense of belonging? ■ Do they believe they are being treated equitably?
CREATE an enabling environment where all employees are part of the solution	■ Provide employees with actionable guidance ■ Equip managers with tools and strategies ■ Create connections (employee resource groups, mentorship, sponsorship)	■ Obtain feedback on learning experiences and monitor training completion rates ■ Gauge whether employees have a greater understanding and appreciation of differences	■ Are employee perspectives and behaviors changing in a positive direction? ■ Are managers implementing more inclusive management practices? ■ Are leaders being held accountable?

Source: *Kantola's Building a Diversity, Equity & Inclusion Program: Leadership Primer*

2. Compile facts and feedback. Accountability can be broken down both quantitatively and qualitatively, and both methods are equally important. Using the model above as a guide, compile the data you have gathered on the measures that are most important to your organization. If this is your first effort, then this will help you to establish a baseline and look at how far you can move the needle in the future. At the same time, establish and maintain an ongoing feedback loop with both employees and managers, gathering their input and tracking progress.

3. Assess progress and identify gaps. Use the facts and feedback gathered to evaluate the level of progress you have been able to achieve. See the questions in the model and consider others such as: Where are your areas of DEI strength and weakness? What does employee feedback tell you about your workplace culture? Is leadership fully supportive? Are they prepared to be transparent with where you stand in your DEI journey?

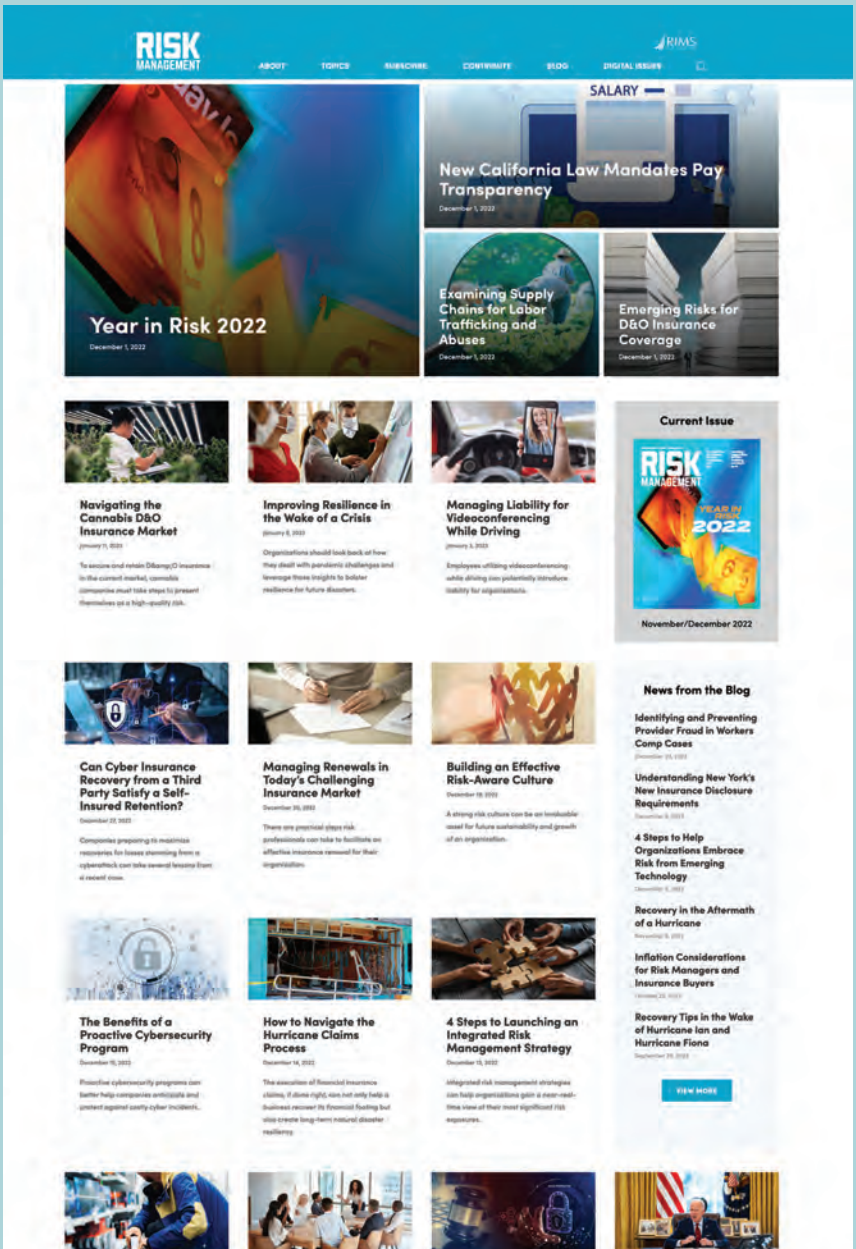
4. Implement consequential accountability measures. In a survey on leadership progression and diversity, Gartner found that "organizations that embrace consequential accountability will reach gender parity 13 years earlier and racial parity six years earlier in their leadership benches." Gartner defines consequential accountability as something that "integrates DEI measures into leaders' performance evaluation processes to ensure that there is mutual understanding of, and commitment to, DEI as a strategic priority." Consider this approach when assessing leadership alignment.

5. Tell your story. Storytelling is one of the most effective ways to communicate because it can reach people at the deepest level. Once you decide what data you want to share, weave your story around it and include visuals that can help explain your progress. Be sure to provide context, such as where you started, why you wanted to take on this initiative at this time, how it fits with your mission and vision for the future. It is critical to be authentic in your storytelling—no corporate speak. Do not be afraid to share some of your challenges. Your employees and customers may be aware of some of those challenges already, so papering over them will only make it appear as though you are not taking the situation seriously.

6. Celebrate your achievements. Accountability is reinforced by celebrating wins—even incremental wins. Celebrating recognizes those who have put in the hard work to bring about change, both in themselves and in support of others. It also serves as a nudge for those who may not be bringing 100% of themselves to the effort. R

Natasha Nicholson is director of content marketing at Kantola Training Solutions.

Whatever the topic, we have you covered



From fundamental resources to news you can use, *Risk Management* has a wealth of content to help risk managers stay at the top of their game. Check out the *Risk Management* website to browse resources such as:

- **Topics Index** to help you find articles on key subjects like Cybersecurity, ESG, Disaster Preparedness, ERM, Emerging Risks and Diversity, Equity & Inclusion
- **Online Exclusive Articles**
- **Current Issue,** including our Digital Edition
- **Archive of Past Articles and Back Issues**

Visit **www.RMmagazine.com** to learn more.

RISK MANAGEMENT

CONFERENCE PREVIEW

A World of Resilience at RISKWORLD

At the height of the pandemic, all eyes were on risk management. Risk leaders around the world were called upon to help their organizations understand, respond and adapt to an array of never-before-seen risks. And the risk community rose to the challenges, demonstrating its power its power to help drive organizational resilience.

Now, the question of how to maintain resilience in the face of so much adversity and rapid change remains imperative. The road to organizational resilience continues at RISKWORLD®.

From April 30 through May 3, the global risk community and other strategic business decision-makers will convene at RISKWORLD, the world's largest gathering of risk management and insurance leaders. Held at Atlanta's Georgia World Congress Center, the event will deliver an unmatched experience for business leaders from a wide range of industries, professional responsibilities, backgrounds and experience levels.

The education sessions will explore everything from cyber concerns, data protection, supply chain and other business interruptions, to natural disasters, ESG risks, political unrest and countless other emerging risks. RISKWORLD's more than 150 education sessions and the hundreds of resources and solutions on display in the Marketplace will address the most pressing business challenges.

Risk management is a relationship business, and the advantages of networking and establishing connections at face-to-face events like RISKWORLD cannot be overstated. The event program includes countless networking opportunities, empowering and inspiring the global risk community to think big, be courageous and successfully drive resilience.

ATLANTA 2023 RISKWORLD®
APRIL 30–MAY 3

STARTING YOUR RISKWORLD VOYAGE

RISKWORLD kicks off on Sunday, April 30, with the **Opening Reception: RISK VOYAGE**. Join RIMS at the Georgia Aquarium, which features aquatic life that cannot be found in any other aquarium in the world. The risk community will have access to the aquarium's many exhibits while being treated to some of the best local cuisine and drinks catered by Wolfgang Puck.

GAINING INSIGHT AND MAKING CONNECTIONS

While expectations for risk professionals mount, it is critical to explore and identify innovative resources, tools and solutions to enhance capabilities, efficiencies and the overall effectiveness of risk programs.

In the **RISKWORLD Marketplace**, more than 300 exhibitors will demonstrate the latest products, services and resources. Additionally, the Marketplace will be home to designated centers for quick learning experiences, including:

- **DE&I Lounge**, sponsored by Marsh, provides attendees with the

SHUTTERSTOCK/TUCKERBLADE

opportunity to participate and engage in a range of discussions covering DE&I issues like allyship, talent challenges and measuring metrics.

- **Global Studio**, sponsored by TÜV SÜD Global Risk Consultants, covers international risk management practices and global business challenges.
- **Innovation Hub**, sponsored by WTW, focuses on developments in emerging risks, cyberrisks and claims.
- **Thought Leader Theater**, sponsored by Swiss Re Corporate Solutions, offers a series of succinct, interactive discussions on timely topics.
- **Wellness Zenter**, sponsored by Sedgwick, explores ideas that support health and productivity in the workplace, including corporate wellness and work/health relationships.

This year's RISKWORLD Mobile App has a new feature to help risk professionals connect with peers who share similar professional responsibilities or whose organizations are navigating similar risks. The new **RISKWORLD Connect** hub will offer a space for attendees to explore these shared challenges. To download the RISKWORLD Mobile App, registered attendees can search RIMS Events in app stores.

UNIQUE PERSPECTIVES

RISKWORLD speakers come from different backgrounds and experiences to share their unique viewpoints. In addition to the stellar lineup of thought-leading risk professionals and business strategists who will lead the education sessions, RISKWORLD 2023 will feature four powerful keynote speakers.

Johnny C. Taylor, Jr., author and president and CEO of the Society for Human Resource Management, will kick things off during the General Session on Monday, May 1. He will walk the audience through today's corporate culture challenges and opportunities, including ways to reinvent, reinvigorate, reimagine and reset our organizations and the people we lead.

At the Awards and Leadership Keynote, also on May 1, RIMS will honor risk professionals, organizations and chapters for their personal achievements and contributions to the risk management community. **Josh Linkner**, CEO and author, will entertain the crowd with a captivating presentation, demonstrating how navigating a single jazz song can provide lessons for collaboration, adaptability and decision-making.

For the first time, RISKWORLD will feature a Tuesday morning keynote presentation, sponsored by Chubb. On May 2, **Evan G. Greenberg**, chairman and CEO of Chubb Limited/Chubb Group, will share an update on the state of the industry.

The conference concludes on Wednesday, May 3, with a one-on-one conversation between world-renowned NASCAR driver **Danica Patrick** and RIMS President **Jennifer Santiago**. Patrick's determination, versatility and commanding presence have led to her success on and off the track.

DE&I AT RISKWORLD

Risk management depends on connecting the dots between business practices, breaking down silos and building inclusive cultures. Drawing risk professionals from all corners of the world, career levels and personal backgrounds, RIMS is taking the opportunity at RISKWORLD to drive greater awareness about the importance of diversity, equity and inclusion in the risk community. Marsh shares DE&I as a priority and has partnered with RIMS to create a powerful program that includes educational sessions and networking opportunities.

New to RISKWORLD are **Community MeetUps**, a series of conversations designed to bring together under-represented communities in the risk and insurance industry to promote networking and collaboration. By sharing unique experiences and perspectives without judgement or expectation, these MeetUps will explore the issues that matter most to the participants and their allies. The 45-minute MeetUps will be held each day of the conference and will be facilitated by industry leaders from the African American, Asian American, Pacific Islander, Latinx and LGBTQ+ communities.

Coffee Chats will also be part of the RISKWORLD DE&I experience. These 20-minute sessions will feature thought-provoking conversations and other networking experiences that focus on hot topics in DE&I. Subjects will include ESG and talent risks, risk management's role in advancing DE&I, as well as DE&I's impact on the future of business. The Coffee Chats will be hosted by members of the RIMS DE&I Council, RIMS leadership and other prominent members of the risk community.

In the RISKWORLD Connect hub, RIMS will also host a series of networking opportunities for students from **HBCU IMPACT®**, a nonprofit that works to increase the number of Black professionals in the insurance, risk management, financial services and legal industries.

In addition, the RISKWORLD education program has a dedicated **Diversity, Equity and Inclusion track**. The track features presentations by the National African American Insurance Association and a women's leadership panel. Education sessions will also address topics such as: inclusion and belonging's effect on injury recovery, HBCU risk and insurance engagements, AI and discrimination, mentoring, and supplier diversity and accountability.

SAFETY AND SECURITY

The well-being of RISKWORLD attendees is a top priority for RIMS. Each year, RIMS contracts with outside experts to implement best practices in safety and security for large-scale events. RIMS also works closely with local police, public safety and city officials to ensure a safe and productive RISKWORLD experience.

Under the "Attend" menu option on the RISKWORLD website, visitors will find safety tips for conference attendees, safety measures taken by the Georgia World Congress Center and Atlanta's Downtown District, addresses for nearby medical facilities, and links to other important event safety information. Additionally, the Atlanta Downtown District also offers the Ambassador Force and Ambassador Escort Service, a service that provides a safe ambassador to escort visitors walking to destinations within the district.

To learn more about RISKWORLD 2023 or to register to attend, visit www.RIMS.org/RISKWORLD.

BACKUP PLANS

How to Preserve Institutional Knowledge as Employees Depart

by Trevor Treharne

The Great Resignation and Silver Tsunami have received a lot of recent attention as two workforce trends making a significant impact on organizations. With the workforce rapidly graying, some employment experts are saying we are in the midst of the "Great Retirement." According to the Pew Research Center, the rate of retirement for Baby Boomers has accelerated since COVID-19 began. Nearly 29 million people from this generation retired in 2020—three million more than in 2019—and a total of 75 million will retire by 2030.

Many employees also recognize that leaving is often the only way to get meaningful salary increases and be paid the rates they deserve. According to Pew Research Center analysis from July 2022, half of employees who switched jobs saw their pay increase nearly 10%, while the median worker who stayed put saw an inflation-adjusted loss of almost 2%. When paired with stress, burnout, organizational culture issues, understaffing, rising inflation, the looming prospect of a recession, and any number of other issues impacting work conditions, it is no wonder most people are either looking or at least open to leaving their job. Indeed, Randstad's Employer Brand Research recently found that 70% of all workers are open to new job opportunities.

SHUTTERSTOCK/TREETY

Whether they are retiring or moving on to new opportunities, departing workers take with them the subject-matter expertise and institutional knowledge they have accumulated over their professional careers. "What they leave behind is everything from relationships, knowledge of how things get done, technical expertise, alongside various aspects of product delivery, customer management or expertise around what is occurring in a market," said talent risk management and knowledge transfer specialist Steve Trautman, principal and founder of the Steve Trautman Co.

This exodus of experienced and knowledgeable talent results in "brain drain." Sometimes known as "human capital flight," brain drain comes in three major forms. It can be organizational, as talented employees retire or move to rival companies; geographical, as highly skilled individuals and graduates depart their home country or region; or industrial, as workers shift from one sector to another. All three forms pose a threat to the success and viability of an organization, especially when highly experienced or "star performer" employees leave. Losing such skilled talent can impact productivity, and resulting recruitment efforts to find their replacements can be costly.

Brain Drain in Risk Management

As a specialized sector that requires a high level of skill, ability and experience, risk management is especially vulnerable to the negative effects of brain drain. Risk management often operates in a knowledge silo, and as risk specialists leave, so does their influence and knowledge.

Risk professionals possess a significant body of knowledge and understanding. "This kind of knowledge capital, intellectual capital, and even relationship capital is not on a form, in a report or part of a checklist," said employee retention expert Chason Hecht, CEO of Retensa. "It evolved with the systems wrapped around intellectual property, customers and employees. Risk is not a one-size-fits-all world. Organizations' interests and exposure have become more complex. The understanding of how those layers fit together and how to mitigate any issues is not easily replaced."

Immediate Strategies for Combating Brain Drain

There are a number of strategies organizations can implement in the near term to retain vital knowledge and expertise and stop brain drain.

"An immediately actionable step could be to make knowledge-sharing a part of company values and policies," said Amber Clayton, senior director of knowledge center operations at the Society for Human Resource Management. "This could include direction on capturing information—such as policies, procedures, instructions, graphs, photos and videos—before, during or after a project or task is complete. Leading by example is something that can start immediately too. Host lunch-and-learn sessions to share information about specific products, services or departments."

Managing talent risk can and should be a regular team effort. "Managers and technical leaders should be scanning their teams for people with unique expertise and working to label exactly what these experts are doing that makes them unique," Trautman said. "Think about this at the task level. What do they do? What problems do they solve? What relationships do they manage? Then managers can pair those unique experts with people who have the capacity to learn and provide backup."

Another way to encourage retention is to foster a sense of connectedness to other team members or the organization's mission, a sense of appreciation from leadership, and engagement in the output of the work being done. "As a manager in meetings, ask 'How do you think we should do this?' It enables the cross-pollination of ideas and increases knowledge-sharing," Hecht said. "Standardize post-project 'lessons learned' meetings. Ask questions like: What worked? What did not? With unlimited time and budget, what would you do differently? Who should be acknowledged and why?"

Spot bonuses can also have an immediate impact on retention and morale. Look for opportunities to recognize employees who go above and beyond and consider rewarding that with a small cash bonus or extra paid time off. Be sure to do this as close to the effort as possible to clearly tie the bonus to the behavior.

For some employees, the decision to stay or leave can come down to engagement. "A failure to enable, support and develop your people will lead them to get bored and move on," said Andrew Methven, head of risk and compliance at Hearing Australia. "Potentially, it can be [even] worse if they get bored and stay, as this means you lose their engagement and energy to support the organization's outcomes."

Methven suggested establishing a "risk champions" network to provide additional opportunities for employee collaboration across the organization. "This is especially useful when there is not a large, formally established risk team," he said. "For example, my team has three people, but we work with clinical, cybersecurity, health and wellbeing, and a range of other teams who are risk experts in their subject areas. In terms of retaining good talent, you need to invest the time with them to understand how they want to develop and the opportunities they are seeking."

Longer-Term Approaches

To prevent the loss of knowledge with departing employees, organizations must also take a longer view and implement approaches with a view toward retention over time.

"Employers need to take proactive measures to ensure there is knowledge-sharing before someone takes a leave of absence, transfers to another position or leaves an organization," Clayton said. "Know your employees and who is at a high risk of leaving. Watch for red flags like issues with health, family or work. Assess if there are employees of retirement age who may be planning to retire soon."

It may also be helpful to conduct interviews with employees to better understand why employees want to stay with or leave an organization, and what you can do to better ensure the organization is a place people really want to work.

Of course, some turnover will always take place, and much can be done to smooth these cases for both the organization and the employees who remain. To that end, it is critical to know who does what and detail an employee's skills and knowledge through job descriptions and other documentation.

"Develop processes for capturing instructions and procedures, encourage communication between employees and departments, and acknowledge ideas and recommendations so employees are more apt to share," Clayton said. "Mentoring or job shadowing programs can help transfer knowledge by pairing someone with years of experience with someone with less experience, while job rotation or cross-training—where people learn other roles and responsibilities—are also measures that can be taken to ensure knowledge-sharing."

Nearly 29 million Baby Boomers retired in 2020—three million more than in 2019—and a total of 75 million will retire by 2030.

Compensation is an important factor in retention, especially in the current economic climate. Given the Pew findings, if the options are making even less money by staying at current salaries and eating the costs of inflation or leaving to make what you should, it is little surprise people may want to leave. Employers should seriously assess what they can do to meet more competitive rates proactively, and how they can be organizations that workers want to stay with.

Salary alone is not enough for a long-term solution to talent risk, however. After a while, Hecht said, "the perception becomes 'this is what I should have been paid all along—I earned it,' so there is no residual impact on retention."

Companies also need to consider the mindset of employees, particularly with stress levels and burnout at historic highs, and take meaningful steps to address those issues.

Flexibility is another consideration for increasing retention. For example, organizations may want to consider non-traditional or part-time work arrangements to keep knowledgeable employees on the payroll in some fashion. "Flexible work arrangements will soon become standard," he said. "The idea of a 40-hour work week is already being diminished, if not undermined by reality. Flexible work arrangements are the next frontier for organizations."

To ensure that expertise can be handed over to another employee, Trautman recommended that organizations construct a "knowledge silo" inventory. A knowledge silo is a block of work that someone has been doing that can take up to a year to learn. The objective is to determine how many knowledge silos an employee is responsible for so these can be handed over to existing or replacement employees in the event of their departure.

Organizations need to identify these silos as early as possible. "If you do an inventory of 300 employees, you are going to find 20 or 30 people who are uniquely relied upon," Trautman said. "You can then start to run some scenarios to show what work will stop if you extract that person."

By performing a talent risk assessment, organizations can build an understanding of each employee's knowledge silos. This process can also double as a staff retention approach. "Perhaps there is a person who is operating in between 15 and 20 different knowledge silos, which would be a lot," he said. "You might ask that person if they are happy working in that many silos and discover they feel buried in legacy work and have no focus on innovation. You can then actively extract people from blocks of work so that they can do something else. That can be incredibly powerful in helping somebody to choose to stay when the recruiter comes calling."

Gathering this inventory and understanding these knowledge silos requires careful examination on an individual level and cannot be effectively achieved through company-wide surveys. "You have to look at what individual people do," Trautman said. "We gather the data by interviewing frontline managers about what their people actually do every single day. For senior executives, their direct reports will know what their boss does. We look at the ecosystem around a person. We ask questions to get at what those people are doing and what is valuable about what they are doing."

Fighting brain drain is part of every organization's long-term talent risk management efforts. By engaging in more effective knowledge transfer strategies, organizations can ensure that, while individual employees may depart, their knowledge and expertise will remain. R

Trevor Treharne is a South Korea-based freelance journalist.

SHUTTERSTOCK/BAKHTIAR ZEIN

Employer Obligations in Disaster Response

As organizations navigate increasingly frequent and severe natural catastrophes, there are several employment law considerations they must take into account.

by Sally R. Culley

Every region around the world is at risk of experiencing extreme weather events, whether it is tornadoes, wildfires, winter storms, hurricanes, tropical storms, floods, earthquakes or volcanoes. Aon estimated that natural disasters caused $313 billion in global economic losses in 2022. In the United States alone, there were 18 major natural disaster events that resulted in at least $1 billion in damages last year, according to the NOAA National Centers for Environmental Information. In addition, data from the U.S. Census Bureau indicates that natural disasters forced an estimated 3.4 million people in the United States to leave their homes in 2022. While almost 40% were able to return in less than a week, nearly 16% never have.

As climate change makes extreme weather events ever more frequent and more severe, there is no reason to believe that 2023 will be any different. There is little that employers can do to prevent natural disasters from occurring. However, preparing for the impacts that a natural disaster may have on a business can help to keep employees safe and reduce the disaster's economic impact on the business.

DEVELOPING AN EMERGENCY ACTION PLAN

The Occupational Safety and Health Administration (OSHA) requires employers to provide safe and healthy working conditions, which includes protecting employees from unreasonable danger in the workplace due to natural disasters or other emergencies. OSHA defines a workplace emergency as a natural or man-made "situation that threatens workers, customers or the public; disrupts or shuts down operations; or causes physical or environmental damage."

Before a disaster strikes, employers should identify reasonably foreseeable emergencies so that they can prepare an emergency action plan. Plans can include information like procedures to be followed in case of an evacuation due to fire or flooding, creation of a safe room to use in the event of a tornado or severe storm, and work-from-home rules in the event that extreme weather makes travel unsafe. For help in developing an emergency action plan and guidance on what it should include, employers should review the OSHA and U.S. Department of Labor resource *How to Plan for Workplace Emergencies and Evacuations* (see sidebar on page 28).

Once an emergency action plan is in place and has been communicated to employees, it is important that the employer provide robust training to all employees on what it contains. In a crisis, it is far more likely that employees will remember and follow the plan if they have been properly trained and have gone through emergency drills.

COMMUNICATING WITH EMPLOYEES

Communication before, during and after a severe weather event or other emergency is critical, and plans for such communication should be included in the emergency action plan. Employees should know and understand how to communicate with their employer and how to obtain necessary information in

SHUTTERSTOCK/STOKKETE

The Essential Elements of an Emergency Action Plan

To help organizations prepare for emergencies and disasters, the publication *How to Plan for Workplace Emergencies and Evacuations* from the Occupational Safety and Health Administration (OSHA) and the U.S. Department of Labor provides guidance for developing emergency action plans. The booklet can be found at www.OSHA.gov under "OSHA Publications."

When developing an emergency action plan, it is important to first conduct a hazard assessment to determine what could cause an emergency in your workplace. The plan should be tailored to the worksite, and if you have more than one worksite, each site should have its own emergency action plan.

It may also be helpful to identify an emergency coordinator who can assess the situation, lead response and evacuation efforts, and communicate with outside emergency services.

At a minimum, an emergency action plan must include:

- A preferred method for reporting emergencies and alerting employees to evacuate or take action
- An evacuation policy and procedure
- Emergency exit procedures and route assignments, such as floor plans, workplace maps, and safe or refuge areas
- Names, titles, departments and telephone numbers of individuals both within and outside your company to contact for additional information or explanation of duties and responsibilities under the emergency plan
- Procedures for employees who remain to perform or shut down critical operations, operate fire extinguishers, or perform other essential services that cannot be stopped for every emergency alarm before evacuating
- Rescue and medical duties for any workers designated to perform them

Although not specifically required by OSHA, it may also be beneficial to include:

- A designated assembly location and procedures to account for all employees after an evacuation
- The site of an alternative communications center to be used in the event of a fire, explosion or other emergency
- A secure on- or off-site location to store original or duplicate copies of accounting records, legal documents, employee emergency contact lists and other essential records

the event of an emergency, It is difficult to think clearly in the midst of chaos, so it is important for employees to know in advance what they are expected to do.

Employers should maintain current contact information for all employees and have a process in place to ensure it is routinely updated. Some organizations implement a communication tree, where a few employees are designated to each call a list of people, each of whom calls another list of people, and so on until everyone has been contacted. Other employers use technology to send out a recorded message or group text, while some establish a call-in number for employees to save and use during emergencies. Whatever procedure the employer chooses, someone should be specifically charged with ensuring that it is followed during an emergency and that all employees are contacted.

EMPLOYEE COMPENSATION REQUIREMENTS

The Fair Labor Standards Act (FLSA) outlines a number of regulations with regard to employee compensation, and employers should be familiar with them. There may be specific regulations that apply only to specific businesses or types of employees, but as a general matter, how employees are paid during a disaster will depend on if they are classified as exempt or non-exempt.

Employers are required to pay non-exempt employees only for hours actually worked, even if the reason for not working is a natural disaster or other emergency and not the employees' fault. For example, if an employer closes the workplace and sends employees home in preparation for a potential natural disaster, there is no obligation to pay non-exempt employees for any time that they are not actually working after the closure.

However, there are potential exceptions for waiting time or on-call time. Examples of such exemptions include if the power is out at the workplace but employees are required to stick around in case it comes back on, or for non-exempt employees who receive fixed salaries for fluctuating workweeks. Also, if maintenance workers or nurses are required to stay on the premises, they must be compensated, even if they do not perform any work.

As for exempt employees, if there is any work performed during the week, employers are required to pay them their full weekly salary. Accordingly, if a workplace is closed due to a natural disaster or other emergency for less than a full workweek, the employer must pay the exempt employees' full salaries for the week. If a closure lasts an entire week and exempt employees do not perform any work at all during that time, the employer is not required to pay any compensation.

Employers can require employees to use paid time off or other leave when they are unable or choose not to work because of a natural disaster or other emergency, but this policy should be clearly communicated to employees in advance. Ideally, this should be included in an employee handbook that is distributed to all.

It is also important for employers to protect their payroll and timekeeping records. In the event of catastrophic damage

to the physical workplace, records may be lost, making it difficult or impossible for employers to process payroll. It is a good idea to maintain off-site electronic backups as they can be easily accessed if original records are no longer available.

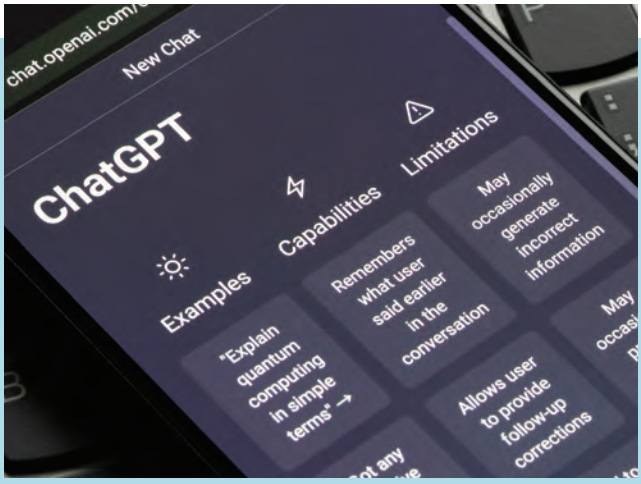
POLICIES FOR LEAVE, ACCOMMODATION AND CONTINUED EMPLOYMENT

Following a natural disaster, employers can expect to receive increased requests for leave and accommodation. Employers should follow their policies for paid time off usage following an extreme event. In addition, the Family and Medical Leave Act (FMLA) requires employers with at least 50 employees to give unpaid leave to employees who cannot perform their jobs because they suffered a serious health condition such as physical or mental illness, injury or impairment, or must care for a spouse, child or parent with a serious health condition. This requirement may also be applicable following a natural disaster. Beyond the FMLA, there may also be state and local laws that require employers to provide leave. Additionally, mental or physical injuries resulting from a natural disaster can lead to increased requests for accommodation under the Americans with Disabilities Act.

If an employer instructs an at-will employee to come to work and the employee refuses to appear, unless they are otherwise legally entitled to leave or an accommodation, they can be subject to disciplinary action, including termination of employment. However, some local and state laws provide protection for employees who are under a mandatory evacuation order. Also, OSHA gives employees the right to refuse to work if they have a reasonable, good-faith belief that the working conditions are unsafe. Additionally, although state laws vary, employers should keep in mind that they (as opposed to a workers compensation insurer) may be responsible for injury to or death of an employee while he or she is working, if the injury or death was caused by intentional or grossly negligent conduct of the employer.

The bottom line for employers is to plan ahead and not wait until disaster strikes. A well-written emergency action plan and clear employment policies can protect employees and the employer, minimize confusion during and after an emergency, and help ensure that operations are restored as quickly as possible following any emergency-related shutdowns. R

Sally R. Culley is a partner at law firm RumbergerKirk, where she practices in the areas of employment and commercial litigation.



CHATGPT POSES CYBERSECURITY THREATS

Since its release in November 2022, the artificial intelligence chatbot ChatGPT has generated widespread attention for its ability to produce conversational responses. While the technology demonstrates AI's promise, there are many risks to consider. In a survey by BlackBerry, 74% of IT professionals said they were concerned about the potential cybersecurity threats posed by ChatGPT. This concern is well-founded, as other researchers report hackers have been successfully using ChatGPT in cyberattacks since at least December. Respondents cited their top concerns about how hackers might take advantage of ChatGPT, including using it to craft more believable and legitimate sounding phishing emails (53%), enabling less experienced hackers to improve their technical knowledge and develop more specialized skills (49%), and using it to spread misinformation (49%). "It has been well documented that people with malicious intent are testing the waters," said Shishir Singh, chief technology officer for cybersecurity at BlackBerry. "Over the course of this year, we expect to see hackers get a much better handle on how to use ChatGPT successfully for nefarious purposes; whether as a tool to write better mutable malware or as an enabler to bolster their skillset. Both cyber pros and hackers will continue to look into how they can utilize it best. Time will tell who is more effective."

–Morgan O'Rourke

BUSINESS EMAIL COMPROMISE SCAMS TO WATCH FOR

According to a survey by Osterman Research and email security firm Ironscales, 93% of organizations had experienced at least one form of business email compromise (BEC) attack in the previous 12 months. Approximately half of all employees face BEC attempts at least monthly, with C-suite and finance department employees targeted most frequently. Fake invoices were the most common variant of BEC attack, impacting over 20% of organizations. Other top variations included data theft (19.7%), in which an attacker requests access to data they are not authorized to view, resulting in a data breach or data exposure, and account takeover (18%), where the goal is to gain access to an employee or executive email account. The report also highlighted emerging BEC variations that companies should watch for. In gift card scams, a cybercriminal impersonates a manager or executive and requests the purchase of gift cards. In payroll diversion scams, the attacker attempts to submit new payment details to divert an employee's paychecks to another bank account.

–Hilary Tuttle

CIVIL UNREST RISK ON THE RISE

Protests and civil unrest are increasingly impacting businesses around the world, according to a report from Allianz Global Corporate & Specialty (AGCS). Since 2017, there have been more than 400 significant anti-government protests worldwide, with almost a quarter lasting more than three months. The costs can be substantial—between 2018 and 2023, six major civil unrest incidents resulted in more than $12 billion in economic and insured losses. This increase in strikes, riots and civil commotion has been fueled by five key risk drivers: 1) the ongoing cost-of-living crisis; 2) distrust of governments and institutions; 3) increasing political polarization; 4) a rise in activism; and 5) climate and environmental concerns. "Operational and security management within organizations should view the current climate as a catalyst for evaluating best practices and policies around preparing locations and employees for potential civil unrest and building resilience," said Srdjan Todorovic, head of political violence and hostile environment solutions at AGCS.

–Morgan O'Rourke

SHUTTERSTOCK/TADA IMAGES, 1000 WORDS

RIMS Virtual Workshops

Advance your risk management knowledge at an interactive instructor-led RIMS virtual workshop. Explore powerful content while you learn the ins and outs of trending topics. You'll return to work with the confidence to apply your new skills to your day-to-day functions.

Applying and Integrating ERM
Analyze the benefits and challenges of ERM, create an ERM agenda, and review real-world case studies.

Captives as an Alternate Risk Financing Technique
Identify opportunities and risks associated with captive formation and analyze various alternative risk financing solutions that support corporate goals.

Claims Management
Gain practical techniques to improve your claims management process and boost the bottom line for your business.

Fundamentals of Insurance
Learn insurance basics, from terms and concepts to policy components and types.

Fundamentals of Risk Management
Learn risk management basics and how you can create, protect, and realize enterprise value.

Leveraging Data and Analytics for Continuous Risk Management
Learn how you can apply leading practices to take ownership of risk data, effectively explore and promote its uses, and leverage it for improved awareness and risk management.

Managing Data for ERM
Learn how risk management professionals can better define analytics requirements, identify data needed, evaluate data sources, identify data issues, combine and enhance data, and visualize data.

Managing Worker Compensation, Employer's Liability and Employment Practices in the US
Understand processes and techniques that can reduce the risk associated with workers.

Optimizing Risk Management with Artificial Intelligence
Learn how to use artificial intelligence (AI) to identify fraud, track and manage your organization's reputation, predict financial concerns, and mitigate a variety of risks.

RIMS-CRMP Exam Prep
Prepare for the RIMS-Certified Risk Management Professional (RIMS-CRMP) certification exam.

RIMS-CRMP-FED Exam Prep
Prepare for the RIMS-Certified Risk Management Professional for Federal Government (RIMS-CRMP-FED) credential exam.

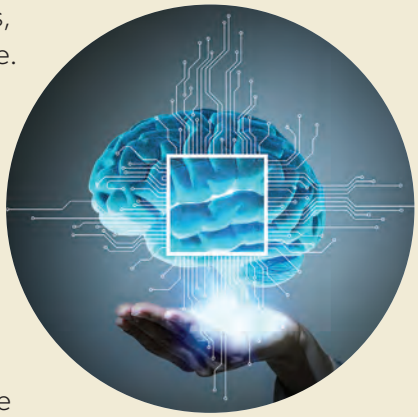
Risk Appetite Management
Learn how to develop a risk appetite framework that clarifies your company's position on risk taking.

go.RIMS.org/VirtualWorkshops2023

RIMS® *the risk management society*

AI and Privacy Risk Concerns

According to a survey by the International Association of Privacy Professionals (IAPP), organizations should consider the following privacy risk implications as the use of artificial intelligence grows:



1. Bias in AI results in harm to individuals, and potential fines for noncompliance.
2. Lack of appropriate governance results in unnecessary administrative overhead and overlooked risks.
3. A changing regulatory environment leads to less legal clarity about AI systems.
4. The lack of available skills within the organization creates a gap in available resources prepared to tackle new challenges.
5. An increased focus on algorithmic outputs necessitates clearer guidance for the explainability of those outputs.
6. The use of AI systems intensifies traditional regulatory scrutiny over privacy practices, leading to greater organizational reputation risk and compliance-based risks.
7. Organizations fear the unintended consequences of using AI systems without technical and legal clarity on requirements.
8. The use of third parties as vendors or contractors can increase organizational liability, difficulty with third-party vendor assessments, and uncertainty about controller and processor responsibilities.
9. Training AI systems requires using data. Without incorporating privacy best practices, data sets may include the nonconsensual use of personal data or secondary uses of data.
10. The existence of AI systems on a connected network increases the security risks surrounding the network, including insider threats, model exploitation and data breaches.

Source: *IAPP, Privacy and AI Governance Report*

TOP 10 TECH RISKS

In Marsh's *Global Technology Industry Risk Study 2023*, risk management leaders at technology companies identified their top risk concerns:

Data security and privacy	**71%**
Business interruption (digital)	**57%**
Technology errors and omissions	**51%**
Reputational risk	**49%**
IT resiliency	**48%**
Regulatory compliance	**44%**
Intellectual property risk	**41%**
Supply chain disruption	**34%**
Directors and officers liability	**34%**
Employee safety	**32%**

Source: *Marsh, Global Technology Industry Risk Study 2023*

$3.64 BILLION

Amount spent by large U.S.-based companies on defense against class action lawsuits in 2022, up 8% from 2021. The increase was attributed to larger claims and a greater number of companies facing class actions. While labor and employment litigation accounted for greatest percentage of class action spending in 2022, companies believe consumer fraud class actions related to social media use and ESG practices pose the biggest threat moving forward.

Source: *Carlton Fields, The 2023 Carlton Fields Class Action Survey*

SHUTTERSTOCK

THE SPECIALIZED INSURANCE YOU DIDN'T DARE DREAM ABOUT. BUT WE DELIVERED IT ANYWAY.

To offer truly specialized industry insurance, innovation is the name of the game. It's how we're taking specialization to a whole new level. With extensive experience in underwriting, risk engineering services and claims, we go beyond the expected. And we deliver the innovative, customizable solutions and service mid- to large-size businesses demand across a range of industries.

Visit us at RIMS, booth #1711.

TheHartford.com/specialization

THE HARTFORD

100 YEARS OF EXCELLENCE

MANY SPECIALTIES ONE FOCUS ONE CENTURY

A century of delivering dedicated and reliable insurance solutions has taught us that business is always changing. That's why Old Republic General Insurance Group is always evolving – expanding our specialties, deepening our partnerships, and sharpening our focus on what matters most: You.

With gratitude, here's to another 100 years of insurance expertise wherever your business happens.

orgig.com







OLD REPUBLIC INSURANCE GROUP

Our companies deliver specialized expertise.

- BITCO INSURANCE COMPANIES[1]
- GREAT WEST CASUALTY COMPANY
- OLD REPUBLIC AEROSPACE[2]
- OLD REPUBLIC EXCESS & SURPLUS
- OLD REPUBLIC GENERAL INSURANCE CORPORATION
- OLD REPUBLIC HOME PROTECTION
- OLD REPUBLIC INLAND MARINE[3]
- OLD REPUBLIC INSURANCE COMPANY
- OLD REPUBLIC INSURED AUTOMOTIVE SERVICES[2]
- OLD REPUBLIC PROFESSIONAL[2]
- OLD REPUBLIC RESIDUAL MARKET SERVICES[3]
- OLD REPUBLIC RISK MANAGEMENT[2]
- OLD REPUBLIC SPECIALTY INSURANCE UNDERWRITERS[3]
- OLD REPUBLIC SURETY
- PMA COMPANIES[3]

Insurance contracts are underwritten and issued by:
1. BITCO General Insurance Corporation, BITCO National Insurance Company, Old Republic General Insurance Corporation; 2. Old Republic Insurance Company; 3. Pennsylvania Manufacturers' Association Insurance Company, Manufacturers Alliance Insurance Company, Pennsylvania Manufacturers Indemnity Company.