Q2 2024 RMmagazine.com

RISK MANAGEMENT

THE IMPACT OF AI ON INSURANCE UNDERWRITING

A publication of RIMS the risk management society

RIMS Risk Maturity Model®

WHAT

The **RIMS Risk Maturity Model®** (RIMS RMM®) is a self-assessment designed to help you identify the strengths and weaknesses of your organization's risk strategy. The RIMS RMM® was built for risk professionals, by risk professionals.

The model focuses on the elements ("pillars") and characteristics ("attributes") considered most important for maturing risk management capabilities.

RIMS RISK MATURITY MODEL® Pillars

STRATEGY ALIGNMENT
Degree that decisions integrate risk, results, and threats to the strategy itself.

CULTURE AND ACCOUNTABILITY
Degree that risk considerations are pervasive from the governing body to the front line personnel.

RISK MANTAGEMENT CAPABLITIES
Degree of organizational and individual learning and development with respect to managing risk.

RISK GOVERNANCE
Degree that the enterprise risk management discipline influences and interacts within an organizational risk ecosystem.

ANALYTICS
Degree to which an organization uses technology and analytics to establish, collaborate, gain insight and maintain connections with stakeholders.

This Risk Maturity Model helps you establish a baseline of risk maturity. Once you know that, you can determine the risk maturity level most beneficial to your organization for managing change and getting your organization future ready. Your RMM report measures your organization against five pillars and 35 attributes that leading risk management professionals believe are most important for success. How does your organization compare? Find out at www.RIMS.org/RMM.

PRICING	RIMS Member: Included in membership	Non-member: US $199 the first year, US $99 after

To take the RIMS RMM® assessment, visit www.RIMS.org/RMM

RIMS® the risk management society

Volume 71, Issue 2

contents

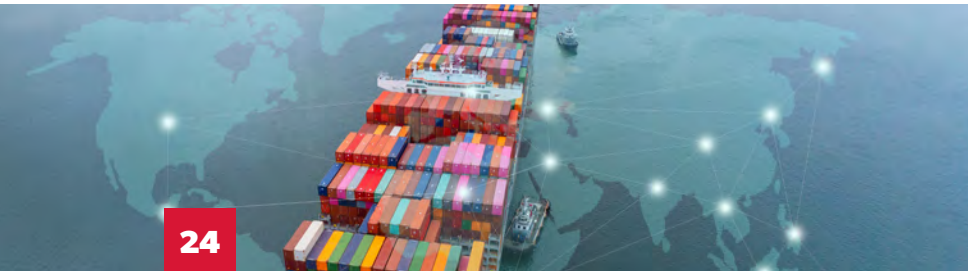
14

FEATURES

18

COVER: ADOBE STOCK/SUMMIT ART CREATIONS
THIS PAGE: TOP: ADOBE STOCK/SUMMIT ART CREATIONS; BOTTOM: SHUTTERSTOCK/MACROVECTOR

FOREFRONT



DETAILS

THIS PAGE: TOP PHOTO: SHUTTERSTOCK/ANTON VIERIETIN; BOTTOM PHOTO: SHUTTERSTOCK/APCHANEL

Risk Management Magazine (ISSN 0035-5593) is digitally published 4 times per year, with 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 71, Issue 2.

AN AWARD-WINNING PUBLICATION

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

RISK MANAGEMENT

CONTACT US

All submissions and letters should be sent to:

Morgan O'Rourke
Editor in Chief
Risk Management
morourke@RIMS.org
T: (212) 655-5922

www.RMmagazine.com

INSIDE

10 Tips for Developing an Effective ERM Program

by Michael J. Cawley

Developing an enterprise risk management (ERM) program can be a difficult task, even for experienced risk professionals. While there is no one-size-fits-all approach, the following tips—compiled from decades of challenges faced and lessons learned in risk management—can help organizations achieve their own ERM success.

1. Create a Succinct Mission Statement
When establishing a robust and meaningful ERM program, a vital first step is developing and memorializing a mission statement that explains its primary purpose. The statement should combine strategy with tactical execution by focusing on actionability instead of empty buzzwords or jargon, and be succinct to encourage understanding, consensus and transparency.

Essentially, the mission statement must tie together the "what" and "why" of ERM. For example: "Enterprise risk management is the process for identifying, assessing, mitigating and monitoring all enterprise-wide risks that might impair the company's ability to achieve its strategic business objectives."

2. Establish a Risk Management Framework
Expanding upon the ERM mission statement, risk professionals should formulate another program cornerstone: the risk management framework (RMF). This authoritative manual "sells" and guides your ERM program.

There are three distinct components to every successful RMF. In the initial section, set the context for ERM. To get there, take stock of your company's identity and explain why ERM can make a tangible difference by asking the following questions: What does your company do and what are its unique business characteristics and drivers of success? What is the connection to, and reliance upon, risk management? How does the discipline of ERM potentially impact the company's

SHUTTERSTOCK/ANTON VIERIETIN

high-level business goals, such as earnings performance, capital preservation, liquidity maintenance and reputation protection?

The second section of the RMF establishes the foundational elements of ERM by detailing the company's overall cultural model and spelling out its identity, what it recognizes and rewards, and the ethical behaviors it expects. Here, the company should also establish the risk governance structure with roles and responsibilities delineated by line of defense. At a very high level, this second section of the RMF should also speak to the concepts of risk appetite and tolerance, with the latter reflecting a specific pre-defined threshold where appetite is exceeded, triggering notification, assessment and/or corrective action.

The third section of the RMF addresses the tactical execution of ERM. This process comprises the following elements: 1) identifying risk on an iterative basis, with the net result being your universe of exposures; 2) assessing risk consistently and transparently, particularly focusing on severity and likelihood; 3) mitigating inherent risk severity and likelihood to an acceptable residual level through well-defined controls; and 4) monitoring risk on an ongoing basis, pinpointing prominent metrics, such as key risk indicators (KRIs), and disseminating reports for both internal and external use.

3. Connect Your Overall Corporate Culture to Risk Management

Risk culture represents the shared understanding and behavioral attitudes of the company's employees toward risk-taking and comprises key pillars like governance, training, risk-aligned performance and business conduct. How does your risk culture connect with a company's overall culture that dictates conducting business with integrity and ethics at all times?

Simply put, a company should strive to cultivate a high-performing environment that is inclusive and equitable at the same time. All employees should feel empowered to do their best and contribute to their fullest potential to advance and thrive in their careers. The overall culture should guide day-to-day decisions and link brand identity with behaviors that are both expected and rewarded.

4. Pinpoint Your Risk Universe

When defining a risk universe, the key point is straightforward: Do not miss a single risk. It is also important to allow flexibility such that emerging risks can be readily incorporated and to sub-categorize or break down the overall universe in a way that makes sense and is digestible.

For instance, you might consider establishing three core categories at the outset—financial, operational and strategic—as these appear consistently across all risk registers, no matter what industry the company represents. Then you can construct a customized core risk category that reflects the source of your revenue streams (e.g., retail, manufacturing, construction, insurance).

5. Institutionalize a Formal, Automated Risk Register

Full implementation and consistent use of an automated risk register tool are vital to ERM success. Mere spreadsheets will not be sufficient. The ideal risk register should focus on a small number of key risk attributes (causes, consequences, controls and key risk indicators) and select metrics (severity and likelihood, and direction and velocity) that will enable risk assessment and prioritization. It is important to appoint one risk owner per risk to establish accountability from the outset.

6. Continually Hone Your Risk Rating Scales

Establishing understandable and transparent severity and likelihood rating scales is crucial to fostering risk governance and risk culture. Keep in mind that simple descriptive identifiers (e.g., high, rare) can expose you to potential misinterpretation. Instead, be specific when defining severity and likelihood and modify the definitions as needed.

For example, severity determination can be predicated on several different indicators, such as financial impact, brand/reputation, regulatory or strategic. Use whatever indicator lends itself to the risk in question and best resonates with the risk owner.

In terms of likelihood, rating scales should not measure the chance of incurring any risk event whatsoever. Rather, it should address the possibility of a significant event as defined in the severity table that you formulate. An "almost certain" rating might anticipate a significant event once every year, while a "rare" rating might project a significant event only once every 50 years.

7. Establish Material Risk Policies

Risk policies should articulate a company's general approach to identifying and managing material risks. Policies are high-level approaches to decision-making, include significant discretion, and are often delineated in qualitative terms rather than strictly with qualitative measures.

As a rough measure, there should be policies for a dozen or so material risks in your universe. Each risk policy should generally address: 1) the definition of the risk policy in question; 2) the goal of the risk policy; 3) controls that mitigate the risk, itemized by line of defense; 4) roles and responsibilities to manage the risk; 5) risk appetite for the risk in question; and 6) specific risk tolerances and escalation provisions in the event these tolerances are exceeded.

8. Actively Promote the Embedded Risk Governance Structure

ERM should never be considered a separate service function. Rather, look at it as a discipline consciously embedded in crit-

ical decision-making processes throughout the organization. Primary ownership for the daily execution of risk management rests with the business unit, with support from risk-related functions like ERM, compliance or internal audit, as well as risk-related boards and committees.

Risk governance structure is best portrayed in the three lines of defense model, where day-to-day management, control, oversight and independent assurance of risk are assigned to the following groups:

- **First line:** business units and supporting functions
- **Second line:** all groups responsible for ongoing monitoring and challenging the design and operation of controls in the first line
- **Third line:** entities responsible for independent assurance over the management of risks, including challenging both the first and second lines

9. Set Appetite and Tolerances for All Key Risks

Risk appetite represents the general willingness to assume risk and, in turn, to expose the company and its capital to potential loss. Establishing and enforcing consistent, transparent and expected behaviors around risk appetite, conveyed through appetite statements and guidelines, is crucial to the risk management framework.

Drilling down deeper, risk tolerance reflects the specific pre-defined thresholds that exceed the appetite for a specific risk, triggering notification, assessment and/or potential corrective action by management. Key risk indicators (KRIs) are metrics that provide a way to quantify and monitor each risk. Think of them as change-related metrics that serve as an early-warning system to help companies effectively monitor, manage and mitigate risks.

10. Connect ERM with Other Risk-Related Disciplines

Once you construct and adhere to a robust risk management framework, risk-related issues can be confronted head-on. Consider the following risk-related areas:

- **Governance, risk and compliance (GRC):** This is a subcategory of your risk universe that simply slices and dices a smaller body of risks in a slightly different fashion.
- **Environmental, social and governance (ESG):** This is a mixture of operational (e.g., corporate governance) and strategic (e.g., climate risk) exposures, as well as the precepts from your overall cultural model described in the foundational section of your RMF.
- **Diversity, equity and inclusion (DEI):** DEI initiatives are undeniably risk-related in nature and, like ESG, can be viewed through the prism of both the risk register (e.g., operational risks like human resources, talent management/retention and compliance) and, even more importantly, foundational elements contained in your RMF like ethics, culture and governance.

Whether the risk-related challenges are actual risks within your risk universe or principles addressed within your risk management framework, applying the discipline of ERM will still work to address the wide range of risks facing your organization. R

Michael J. Cawley is a risk management executive with more than 35 years of experience in the strategic and tactical elements of corporate enterprise risk management. He currently serves as a subject matter expert in an advisory role on ERM best practices for GRC software provider DoubleCheck.

Preventing Social Media Copyright Claims

by Michael S. Levine, Latosha M. Ellis and Veronica P. Adams

As businesses increasingly rely on social media to promote products or services, copyright infringement claims are increasing. Therefore, it is important for organizations and those who facilitate their advertising campaigns to understand the intersection of copyright law and social media. Claims previously exclusive to publishers have now reached major companies that market their products through their own social media posts or third-party influencer posts. Reposting user-generated content without the creator's permission can expose organizations to significant legal liability and risks. Being on the wrong side of a copyright infringement lawsuit could cost thousands or even millions of dollars in legal fees and damages. Fortunately, a comprehensive risk management and insurance program can help mitigate these losses if a copyright owner accuses an organization of unauthorized use of their work.

UNDERSTANDING THE RISKS

Understanding the potential risks is crucial to recognizing the activities that can expose an organization to copyright infringement claims. For example, businesses that create and share photos and videos to promote their product or service can be liable for copyright infringement if they use content without approval from the creator.

Companies that use music on their social media pages or websites are also at risk. Copyright exposure arises if the music is not properly licensed, even if it is playing innocently in the background. For example, the U.S. District Court for the Southern District of Florida found that Bang Energy violated Universal Music Group's copyrights when it posted TikTok ads with music without the artist's permission.

It is important to note that a low follower count is not a defense. Likewise, while it is a best practice for other reasons, crediting the original creator does not confer the right to use copyrighted work or afford automatic protections. Instead, linking to the source and attributing the original creator notifies the creator of unauthorized use. There is also software that can detect inappropriate uses of copyrighted material on the internet, contributing to the notable increase in claims.

Copyright infringement claims can lead to significant defense costs, actual damages, statutory damages and attorney's fees. For example, 17 music publishers sued Twitter for over $250 million for copyright infringement (including a $150,000 statutory penalty for each of the thousands of violations). They claimed that Twitter had not paid for a license allowing its users to upload copyrighted material.

Uploading or downloading copyrighted works without permission from the creator violates the creator's exclusive rights to reproduce and distribute. Those who commit copyright infringement may face federal statutory damages of up to $30,000 per work infringed or up to $150,000 per work in cases of willful infringement. Damage amounts are especially serious because as more companies lean into trends like short-form videos with music cues on platforms like Instagram or TikTok, the number of potential infringement cases increases significantly.

COMPOSITE ILLUSTRATION/ANDREW BASS JR.; SHUTTERSTOCK/THEBILLJR, VITALII VODOLAZSKYI

Many companies use a social media strategy that leverages popular influencers to advertise on TikTok and Instagram. All three major U.S. record labels have sued companies for failure to obtain a license to use the music in more than 100 videos. In one case, a federal judge ruled for the labels, finding the social media posts to be "work." In other cases, creators have elected for quicker alternatives like sending cease and desist letters, settlement demands, or bills for the creators' licensed work. These actions underscore the importance of analyzing exposure to copyright infringement claims and developing a strategy to mitigate and decrease liability.

MITIGATING COPYRIGHT INFRINGEMENT RISKS

Although there may not be an all-encompassing solution to avoid copyright infringement claims, organizations can minimize the potential impact of such claims by relying on a comprehensive insurance program, having a clear social media governance policy and using original content.

While it is not a substitute for risk mitigation, relevant insurance coverage is available as part of a broader risk mitigation plan. The role of insurance as a component of a broader mitigation plan is twofold: First, as many would expect, insurance may help lessen or eliminate out-of-pocket loss from a copyright violation. Second, and often overlooked, insurance may help reduce or completely cover the cost of defending copyright infringement claims, even if those claims do not result in liability. Indeed, the cost of defending a lawsuit can be worth more than paying the amount of any resulting judgment or settlement.

A good social media governance policy is also part of a broader risk mitigation plan—and one that most insurers will require. When contracting third-party influencers to market products and services, it is especially important to have a policy that requires ensuring the creator has approved posts sharing music or content of others. The governance policy should account for security provisions, regulatory compliance requirements and copyright infringement prevention tactics such as specific guidelines around reposting content, using trending sounds and partnering with third-party creators.

Creating original content for social media also mitigates the risk of copyright infringement claims. While jumping on trends, such as using popular music and reposting content, are powerful plays to increase social media engagement, the dangers might outweigh the benefits. If posting original content is not ideal because of costs or other factors, it is crucial that those using third-party content and any contracted third parties understand the proper licensing and permissions that should be in place to avoid copyright violations.

INSURANCE COVERAGE FOR COPYRIGHT INFRINGEMENT CLAIMS

Adequate and appropriate insurance coverage can help safeguard organizations in copyright infringement cases. From media liability to commercial general liability (CGL) to cyber insurance, organizations can leverage insurance for defense costs, judgments or settlements related to copyright infringement claims. However, every policy includes unique language and defined policy terms. Carefully review policies and consult with insurance professionals to ensure adequate coverage for specific business risks.

Most CGL policies do not cover intellectual property risks, such as copyright infringement claims, and will typically contain an intellectual property exclusion. The policy will include coverage for advertising injury, which aims to protect businesses from claims of offenses committed in advertising, including online platforms. However, restrictive definitions and broad exclusions that might render coverage for copyright infringement illusory dilute this policy, so the relationship between a copyright claim and advertising is not automatic. Further, the common CGL policy phrase "in your advertisement" can be construed restrictively, depending on its usage.

Other exclusions beyond the intellectual property exclusion may also lead an insurer to deny coverage. For example, policies may exclude coverage for claims involving material first published or posted before the beginning of the policy period. Policies also typically exclude coverage for acts of the insured that are intended to, or could reasonably be expected to, cause injury. Thus, the company's conduct must be inadvertent, which is arguably not the case with social media posting.

Media liability insurance is a type of professional liability or errors and omissions coverage that can protect against copyright infringement lawsuits related to reproducing, distributing, performing or displaying a protected work without permission. Companies that post media content on their websites or social media should consider adding media liability insurance to their risk management program.

Cyber insurance policies may also include coverage for copyright infringement claims under a media liability insuring agreement. If included, there is generally coverage for damages and claim expenses, including legal costs and expenses resulting from the investigation and defense of the copyright infringement claim and damages that might result from a judgment or settlement. However, these damages rarely include fines, penalties or future profits.

While companies continue to embrace social media and influencer marketing techniques, they should be diligent in mitigating the risk of copyright infringement. They should also avoid assuming their current insurance program provides adequate protection, as narrow definitions, exclusions or ambiguous policy language might present complexities or prevent coverage altogether. Consult with experienced insurance coverage professionals to ensure that adequate coverage is in place for risks and potential exposure related to copyright infringement claims. R

Michael S. Levine is a partner in the Washington D.C. office of Hunton Andrews Kurth LLP and a member of the firm's insurance coverage practice. **Latosha M. Ellis** is counsel in the Washington, D.C. office of Hunton Andrews Kurth LLP, where she advises policyholders on insurance coverage issues. **Veronica P. Adams** is an associate with Hunton Andrews Kurth LLP's insurance coverage practice.

Using Parametric Insurance to Mitigate Earthquake Risk

by Megan Linkin

This year marks the 30th anniversary of the Northridge earthquake, which struck Southern California and caused $20 billion in damages. Since then, the earthquakes in California from the past decade, like the 2014 Napa earthquake, the 2019 Ridgecrest earthquake sequence or February's Malibu earthquake, have been too small or too far displaced from major metropolitan areas to cause lasting concern.

However, cities and corporations in significant seismic hazard areas should remain vigilant. According to the 2023 revision of the U.S. Geological Survey's National Seismic Hazard Model (NSHM), earthquake risk in the seismically active areas of California and Alaska has increased since the last model revision in 2018. Surprisingly, the new NSHM also shows a rising risk of damaging earthquakes on the East Coast. The updated NSHM shows higher risk than previously believed along the I-95 corridor, which includes Boston, New York, Philadelphia and Washington, D.C.—a region where hurricanes, floods and nor'easters are usually the natural hazards of concern. On April 5, 42 million people got a vivid reminder of this risk when a magnitude 4.8 earthquake shook the New York City metropolitan area and nearby parts of the East Coast.

Historically, the East Coast of the United States has not been immune to earthquakes. For example, in 2011, a magnitude 5.8 earthquake with an epicenter approximately 38 miles northwest of Richmond, Virginia, was felt from Canada to Georgia and as far west as Illinois. The earthquake damaged notable monuments in D.C., such as the Washington Monument, the Smithsonian Castle and the National Cathedral.

SHUTTERSTOCK/ANDREY VP

The East and West Coasts are home to millions of people, hubs of business and commerce, and are essential to the global supply chain due to the critical transit infrastructure in the regions. The potential physical damage from a major earthquake in almost any metropolitan area can reach into the billions of dollars, which could be further compounded by long-term economic impacts from key pieces of infrastructure or whole areas being inoperable. Such a disaster would not only have a severe impact on the region, but the country as a whole.

Therefore, businesses and governments located in earthquake-exposed areas or those with a vested financial interest in earthquake-exposed areas should leverage the expertise and product offerings from the insurance industry to harden their balance sheet against major shakes and shocks. One particular insurance offering—parametric insurance—can provide claims transparency, pay out quickly post-event and fund flexibility, allowing insureds to kickstart their recovery efforts or backfill lost revenue after a major earthquake.

Parametric insurance uses physically measured intensity—called the index or the trigger—of the underlying loss-causing event to determine the insurance proceeds that are due. Generally, the most common triggers for earthquakes are the magnitude and depth of the earthquake or the ground-shaking caused by the earthquake directly at the insured's location. Other options, like the most severe ground-shaking within a pre-agreed distance of the insured's location, are also available but less commonly explored.

All earthquake intensity metrics, such as epicenter location, magnitude, depth and ground-shaking throughout the affected area, are recorded and reported by the U.S. Geological Survey (USGS), making the USGS the independent arbiter of fact after an earthquake. The insured, insurer or any other party to the transaction does not influence what the seismographs report and what the USGS publishes, making claims adjudication quicker and more straight-forward than traditional forms of coverage. There is no need for on-site claims adjustment as the policy is triggered by objective third-party data.

USGS data is available days to weeks after an earthquake occurs, so determining if triggers are hit and if a payment is due can be finalized within 30 days of the event. Since coverage just requires that an earthquake occurs and meets or exceeds the intensity triggers outlined in the policy, parametric insurance proceeds are not tied to actual asset damage, so the insured can use the money they receive post-event to address losses beyond physical damage. Some potential use cases include:

- Covering assets that are underinsured or difficult to insure in the traditional market. For example, the National Cathedral's insurance policy in 2011 did not include earthquakes, requiring the Cathedral to raise millions of dollars to cover repairs.
- Offsetting lost operational revenue due to broad area disruption or loss of a critical piece of infrastructure. For example, even without physical damage to owned assets, organizations in the hospitality industry could experience major financial disruption after an earthquake if the overall area becomes less appealing to tourists and conference organizers.
- Providing cash disbursements to employees affected by the event. This can help them to recover more quickly and, in turn, bring the company back to normally-staffed operations.

As the newest NSHM suggests, the United States remains susceptible to earthquakes, even in areas long considered safe. While no business or government will ever be completely earthquake-proof, parametric insurance can help manage the potentially devastating financial and physical damage exposure. R

Megan Linkin is senior vice president of innovative risk solutions at Swiss Re Corporate Solutions.

Fighting Cyber Insurance Denials Over Human Factors

by Joshua Gold

In February, a ransomware attack against United Healthcare subsidiary Change Healthcare froze medical claims and payments throughout the United States for weeks. As with many headline-making cyber incidents, the case should serve as a wake-up call to all organizations to maximize cyber defenses and ensure that their insurance policies will respond to losses and liabilities stemming from a cyberattack. In particular, policyholders should know that the "human factor" does not preclude cyber coverage for losses suffered in a cyber incident.

For example, an early 2024 case involving a "layered" cyber insurance program sold to Southwest Airlines did not involve a hacker. Instead, it involved a computer system failure that excess cyber insurance company Liberty Insurance argued was partly due to the airline's management decisions. Specifically, after a three-day outage in 2016, Southwest submitted a cyber coverage claim for $77 million in losses from massive delays and disruptions to its operations.

The primary insurance company and three excess insurers paid the claim, but Liberty Insurance, the last layer in the tower, demurred. Southwest sought coverage for costs incurred through various programs and initiatives aimed at assisting the nearly half-million customers affected by the system failure, including:

- Promotional codes disbursed to customers with canceled flights or flights delayed more than two hours
- Travel vouchers disbursed to customers with canceled flights or flights delayed more than two hours
- Refunds made by customer service agents to customers upon request to compensate for alternate travel arrangements
- Rewards points distributed to Southwest's frequent flier program members with canceled flights or flights delayed more than two hours
- Advertising costs for a week-long extension for a sale the airline had been promoting at the time of the system failure

Liberty Insurance denied Southwest's claim, saying the airline's discretionary management decisions caused the losses. The federal trial court agreed, concluding that "Southwest's costs were not caused by the system failure but rather were the result of 'various and purely discretionary customer-related rewards programs, practices and market promotions.'" On appeal, the U.S. Circuit Court of Appeals for the Fifth Circuit reversed the trial court and remanded the case for causation analysis.

Southwest's primary and excess cyber policies promised system failure coverage for "all loss...that an insured incurs...solely as a result of a system failure." Liberty argued that "all five categories of costs that Southwest claimed were not incurred solely as a result of the system failure but rather were the result of Southwest's subsequent business decisions," adding that "Southwest acknowledge[d] that those costs were the result of business decisions." Southwest countered that such business decisions and the accompanying losses were not excluded.

The Fifth Circuit agreed with Southwest that such cost items could not be denied

COMPOSITE ILLUSTRATION/ANDREW BASS, JR.; SHUTTERSTOCK/NORMALFX, JONATHAN WEISS

coverage as a matter of law under a "but for" causation test—that is, whether the costs in question would not have occurred "but for" the system outage. The appeals court remanded the case because the trial court failed to determine whether Southwest would have incurred any of these costs had the system outage not occurred. Further, the Fifth Circuit refused to find specific insurance policy exclusions applicable to the insurance claim, ruling that Liberty's definition of a "consequential damages" exclusion was so broad that it would effectively make coverage illusory.

The Fifth Circuit's Southwest decision has certain parallels to prior coverage claims for cyber losses, including the Second Circuit's oft-cited 2018 decision in *Medidata Solutions v. Federal Insurance Company*, in which the appellate panel refused to agree with the insurer Chubb that actions by certain employees severed the causation chain under a proximate cause analysis. The court rejected Chubb's argument that oral confirmation by an employee was one of several intervening causes for cutting off computer fraud coverage to the policyholder.

Similarly, in 2021's *G&G Oil Co. of Indiana v. Continental Western Insurance Co.*, the Supreme Court of Indiana rejected an insurance company's argument that there was no coverage under a crime insurance policy for a ransomware attack where the policyholder's executive "voluntarily" made a cryptocurrency payment to the hackers. The court noted that the ransom payment was not voluntary but made under duress, and thus did not bar insurance coverage.

The Eighth Circuit's 2016 decision in *State Bank of Bellingham v. BancInsure Inc.* presents another example of a court rejecting an insurance company's argument that human decisions or human error precluded coverage for a cyber loss. The court held that the bank was entitled to insurance coverage despite the insurance company's argument that the bank's loss was caused by a virus entering the system due to a bank employee's breach of computer security protocols.

These cases highlight that cyber insurance policyholders should take any argument that employee actions, decisions or omissions somehow sever the chain of causation needed to demonstrate insurance coverage with a grain of salt. There can be coverage even when policyholders practice less-than-ideal cybersecurity hygiene or make decisions intended to mitigate losses. R

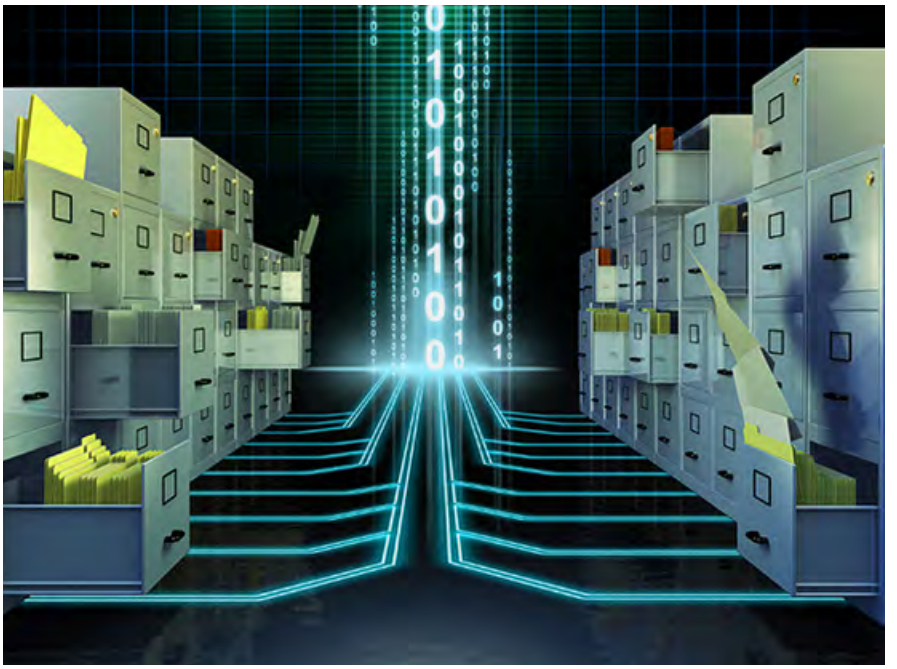
Joshua Gold is a shareholder in Anderson Kill's New York office and chair of the firm's cyber insurance recovery group.

Developing Record Retention and Hold Order Policies

by Chris Keefer

When an organization becomes the target of a claim or lawsuit, it is required to retain all material evidence, ideally dating back to the period before the litigation when it reasonably should have known that the evidence may be relevant to anticipated litigation. Failure to retain documents and records can result in significant court sanctions, including monetary penalties and even an instruction to a jury that it can infer from the destruction of the evidence that it contained information harmful to the case.

To prevent such issues during litigation, organizations must develop and implement a record retention and litigation readiness policy. Such policies govern how long to retain various categories of documents across the enterprise and further identify appropriate protocols when the threat of investigation, claim or litigation first arises.



CRAFTING A RECORD RETENTION POLICY

A good record retention policy will begin by identifying the general purpose of effective records management, such as better organization and decision-making; maximization of available workspace; business continuity in the event of a catastrophic event; prompt response to investigations, claims and litigation; and compliance with federal, state and international legal and regulatory requirements. The policy should also contain guidelines for how long the organization needs to keep certain documents and the proper way to destroy them after this period.

The policy should list the types of documents and information included, such as all final forms of communications, data and recordings of the information listed in the attached schedule. The policy should address what documents and information will not be covered, such as unannotated duplicates, preliminary drafts of certain documents that do not reference significant decision-making, texts and materials originating outside the business, spam or junk mail, and certain private materials involving personal affairs.

The policy should also address handling hard copy and electronic records, focusing on the latter since electronic records may take many forms and be in numerous storage media. For example, the policy can broadly define electronic data as all text files, spreadsheets, emails, voicemails, recorded conversations, databases, calendar and scheduling information, data generated by calendaring, task and personal information management, computer system activity logs, electronic control modules, electronic data records, GPS tracking devices, and all file fragments and backup files containing electronic data.

This requirement applies to individual employees as well as those responsible for managing electronically stored information interfaces, such as IT staff who may have implemented certain defaults to maintain system space. Such defaults automatically destroy business emails after a specific period, usually two years. These emails may constitute records that need to be maintained outside the automated deletion course, requiring a prompt response to avoid improper destruction given a triggering event.

To avoid confusion, list the triggering events in the policy in detail, including an

SHUTTERSTOCK/ANDREA DANTI

investigation, claim or litigation. Your obligations may be triggered when you should have reasonably anticipated such an event, not necessarily when it was filed or served.

The policy should conclude with a robust schedule of all departments where subject records could be found, all categories of documents, the responsible record holder or manager, the retention period for each category of documents and the reason for such a retention period—for example, a relevant law or regulation dictating the retention period, or simply a best practice.

Due to the complexity of identifying and shepherding the development and implementation of the policy, it is wise to have a records retention attorney or specialist actively involved in the initial process and subsequent refreshers. Moreover, the internal records management team should consist of diverse stakeholders within the business, including a C-suite representative, to ensure appropriate visibility and accountability.

The policy should contain guidelines for how long the organization needs to keep documents and the proper way to destroy them after this period.

IMPLEMENTING A HOLD ORDER

Once there is a reasonable anticipation of an investigation, claim or lawsuit, the organization is required to institute a hold order pursuant to its retention policy. The hold order will suspend standard retention policy activities and direct certain respondents to retain specific categories of documents that may be in their possession. The order should define the scope of time subject to preservation, with both a beginning and anticipated end date or range of dates, and it should be clear about whether it extends to future documents, also known as an evergreen hold. In the event of an evergreen hold, the order should instruct recipients on how to create and retain documents created on an ongoing basis.

The hold order should define the issues in dispute and issues related to claims and defenses. If the hold order pertains to a filed lawsuit, mention the lawsuit by name in the order. The order should generally describe the types of documents that must be preserved without attempting to list every possible data source. The instructions should further explain the consequences of noncompliance, including civil or criminal penalties for the company and disciplinary measures for employees. Also, consider the key players to target for the hold order. Relevant IT staff should be part of the preservation process because of their e-data experience and ability to stop regularly scheduled deletion of key players' emails.

You may be required to produce your retention policy during an investigation, claim or lawsuit to demonstrate that you are not destroying relevant and material evidence. The hold order should come from the company's legal department or outside lawyer as part of a confidential and privileged attorney-client communication containing specific advice and instructions.

Once the case concludes, make sure to forward a "release of hold order" to the recipient list to let them know standard retention procedures are back in effect. R

Chris Keefer is the principal of Keefer Strategy, a preventive law practice that helps businesses proactively address enterprise-wide risks.


CPU
62 %
CPU

The Impact of AI on Insurance Underwriting

by Neil Hodge

The increasing acceptance and adoption of artificial intelligence in the insurance industry promises to have a significant impact on insurers and insureds alike. The ability to analyze large datasets quickly and effectively will allow insurers to understand risk as never before, leading to more accurate risk identification, improved underwriting and claims handling, and better premium pricing.

The technology does not come without risks, however, as important questions remain around the accuracy, fairness and security of AI-driven processes and decision-making. Therefore, insurers and risk professionals need to better understand the potential pitfalls of AI technology and take steps to ensure that the process of purchasing insurance does not introduce greater risks than what it was intended to cover.

AI Bias in the Underwriting Process

AI can bring more precision to actuarial models and underwriting, allowing insurers to provide tailored coverage to their client base and bolster risk management. The technology can also improve risk assessment and underwriting by analyzing vast amounts of information from diverse data sources, including internal data such as historical claims and customer behavior, and external data such as litigation trends, market changes, extreme weather events and social media posts. This data enables insurers to establish a more comprehensive understanding of risk factors and thus allows

ADOBE STOCK/SUMMIT ART CREATIONS

for better and more specific underwriting decisions. Additionally, insurers can use AI algorithms to create more personalized insurance policies that are based on individual behavior, preference and risk profile, resulting in a more bespoke set of coverage options that should better satisfy customers' needs.

Despite the benefits, experts warn that the insurance industry is not immune to the same problems associated with AI that have impacted every other sector—namely, the risks of bias, data misuse and data insecurity. As a result, risk professionals need to ask for more details about how AI is used when underwriting their company's policies and what checks and balances are employed to ensure the accuracy of results.

According to Wilson Chan, CEO at AI fintech firm Permutable AI, it is "absolutely critical" to address the repercussions of biased data on AI systems within the insurance industry. "Companies often face inflated premiums and coverage restrictions due to insurers training their underwriting AI on limited or biased data," he said. "The inherent nature of AI systems means that if the input data is biased, the decisions made by the AI will inevitably reflect those biases. To ensure fair treatment in insurance purchases, companies must engage insurers with crucial questions about the training data, its bias mitigation, and the transparency of AI-driven decision-making."

Insurers must be certain that AI systems are trained on representative, unbiased data, and that they regularly review and update AI systems to eliminate biases. They also need to provide transparency about the functionality of the AI systems they are using and what processes AI is being used in. "By adhering to these measures, both companies and insurers can contribute to the fair and responsible use of AI systems in the insurance industry," he said. "This commitment to transparency, unbiased data and ongoing vigilance is fundamental to fostering a trustworthy and equitable insurance landscape."

To illustrate the risk of biased decision-making, Chan offered an example using flood risk insurance. "In this instance, AI models trained on historical data might unfairly impact companies in areas prone to increased flood risk, overlooking current climate patterns," he said. "This could result in companies facing higher premiums or coverage limitations, irrespective of the mitigation measures they have implemented, such as building floodwalls or elevating properties above sea level."

Other common types of business insurance may also be prone to AI bias. Business continuity insurance faces challenges when AI models—limited by data constraints—inaccurately assess a company's risks based on industry or location. For example, a manufacturing company in a rural setting might encounter higher premiums due to insufficient data that fails to consider its robust supply chain relationships, remote operability or contingency plans for power outages. Similarly, AI bias can impact directors and officers (D&O) insurance because AI models trained on industry-specific lawsuit data could inflate prices and restrict coverage for companies operating in sectors prone to litigation and insurance claims, overlooking these specific companies' clean legal records and key governance practices.

The historical data used to train AI systems can also be problematic, said Peter Wood, an entrepreneur and chief technology officer at tech recruitment firm Spectrum Search. Historical biases rooted in the data used in AI algorithms can adversely impact companies and lead to "skewed" risk assessments, especially in niche or emerging sectors where historical data may not accurately reflect current realities. "As AI systems learn from past data, they might assign undue risk to certain companies based on outdated or irrelevant criteria, leading to higher premiums and restrictive coverages," he explained.

Risk professionals need to ask for more details about how AI is used when underwriting policies and what checks and balances are employed to ensure the accuracy of results.

To counter AI bias concerns, Ryan Purdy, senior director and consulting actuary at tech and professional services firm Davies Group, said insurers need to understand the nature of any external data sources they intend to use for underwriting, including who provides the information in its root state, how it is updated and how often. "Data ages and can become less important to the assessment of risk or product suitability for a customer over time," he said.

Addressing AI Underwriting Concerns

Companies need to adopt proactive approaches when dealing with AI-driven insurance under-

writing. The key is to engage in transparent dialogue with insurers. "Companies should inquire about the nature of data sets used for training the AI models," Wood said. "It is essential to understand whether these datasets encompass a wide range of industries, including the latest trends and developments."

He added, "Companies should ask insurers about the mechanisms in place to identify and mitigate biases. This includes questioning whether the AI systems are regularly audited for fairness and accuracy. Additionally, they should inquire about the possibility of manual reviews

or overrides in cases where AI-driven decisions seem unjustly skewed."

Due to the potential for flawed outcomes, companies need to ask more questions about how risks evaluated through AI technologies are assessed and priced. While regulators may be keenly watching insurers for possible abuses regarding the treatment of consumers, "there are fewer safeguards for corporate insureds that are viewed as 'sophisticated purchasers,'" said Tom Davey, co-founder and director of litigation at finance and insurance consultancy Factor Risk Management. As such, there is a greater need for companies to raise questions and concerns themselves.

According to Jeremy Stevens, EMEA business unit director at insurance services provider Charles Taylor Group, companies need to ensure that their insurers can guarantee transparency in their AI decision-making processes. To do so, he said, "companies can ask for explanations on how these models arrive at decisions affecting premium pricing, underwriting and claims handling." Insurers, in turn, "should provide detailed documentation or reports that outline the factors and data inputs considered by AI models as these will help companies understand the rationale behind decisions," he said.

Companies should make sure that their insurers maintain comprehensive audit trails that trace the decision-making process of AI models to ensure full accountability. "Insurers must comply with industry standards and regulations that govern AI in insurance," Stevens said. "Companies can request information on how the insurer adheres to ethical AI practices and regulatory guidelines, so insurers must ensure their audit functions do not lag behind regulations."

Companies should also ask whether the insurer is continuously evaluating and monitoring the AI algorithm's performance, how the insurer arrives at specific decisions, and whether it regularly checks for biases, errors or changes in the data that might affect underwriting decisions. Other steps include checking that the insurer's AI-based underwriting system complies with various data laws such as the European Union's AI Act, the EU's General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA) and the U.S. Health Insurance Portability and Accountability Act (HIPAA), as well as various ethical standards. To better address these issues, companies can establish a collaborative relationship with their insurer. "Provide feedback on decisions and discuss how they align with your company's risk assessment," Stevens said.

It is also important to understand what kind of tech support insurers are getting if they use third-party AI tools. "How often their data is captured is important, but insurers should also work to understand how long it might be until the next update of the technology is available," Purdy said. "Are these future changes in data collection, data structures or technology versions going to force additional changes from the insurer side to keep making effective use of these technologies? Working to line up these providers' development timelines to the insurer's own timelines can alleviate substantial headaches in the future."

Data security is another area of concern. Experts warn that companies could be in danger of making key risk information publicly available if insurers use or share their data on AI systems—which often retain rights to the intellectual property of any inputted data—when training AI technologies to improve their underwriting. Companies need to actively protect their risk data by maintaining confidentiality, sharing it selectively, and enforcing contractual clauses for data protection, Wood said. They also need to vigilantly monitor the use of their data and check on what cybersecurity measures the insurer has in place to protect data from breaches or misuse.

"Companies should demand clarity on how their data will be used and ensure that their information is anonymized before being incorporated into larger datasets," Wood said. "This includes negotiating agreements that restrict the use of their data solely for underwriting purposes and not for training AI models. Insurers, for their part, must adhere to stringent data protection regulations and employ advanced encryption and access control mechanisms to prevent unauthorized data usage, too."

He added, "Furthermore, there should be transparency about data handling practices. Regular audits and compliance checks can help maintain trust and ensure that both parties adhere to the agreed-upon terms regarding data usage and privacy." R

Neil Hodge is a U.K.-based freelance journalist.

SHUTTERSTOCK/FAMILY STOCK

10 GEOPOLITICAL RISKS YOU NEED TO PREPARE FOR THIS YEAR

by Christopher Mason and Dr. Ian Oxnevad

Geopolitics drive a significant amount of risk and create liabilities in sectors and locations that may seem far removed from world events. For example, consider how conflict in Ukraine has impacted economies and sanctions regimes across the United States and European Union. Because of these risks, risk practitioners must consider how global events can quickly challenge risk management strategies. As U.S. Deputy Attorney General Lisa O. Monaco recently said, "companies are on the front lines of today's geopolitical and national security challenges."

SHUTTERSTOCK/MACROVECTOR

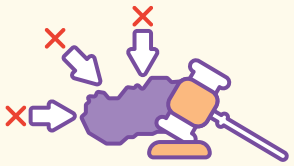
The world is undoubtedly at a governance crossroads. This year, at least 64 countries will hold elections and millions of members of Gen Z will reach the eligible voting age, increasing the probability of significant shifts in the established world order, including longstanding regulatory norms. Elections and political polarization also lead to an increase in misinformation and disinformation campaigns that can sway voters, public discourse and even business reputations. In addition, politicized regulation, fiscal spending decisions and global conflict can significantly impact national economies and companies.

It is essential for companies to get more proactive about managing their geopolitical risk exposure. Here is a breakdown of the key geopolitical risks to consider for the rest of 2024 and ways for companies to remain resilient:

1 Global Conflict

International conflict will continue and expand in 2024, increasing the downstream impact on companies operating globally. Conflicts in Ukraine and Gaza have recently hurt portfolio investments in sectors ranging from tourism to energy, while also spurring growth in others. Companies must understand how major geopolitical shifts impact revenue to protect themselves from conflict-related risks and disruptions up and down the supply chain. Key questions focus on how conflicts affect shareholder value, customer access, operating costs, market share and security expenses. Global conflict will also factor into insurance decisions and costs as certain insurers have suffered from recent events and others are weighing future risks. Assessing your geopolitical risk exposure will allow more informed decision-making when negotiating your insurance coverage.

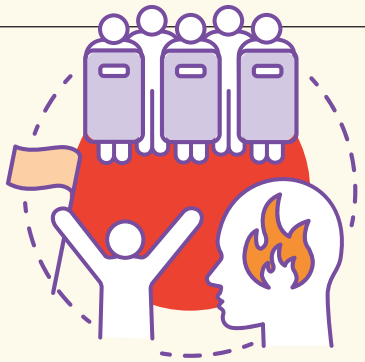
2 Economic Sanctions



Recently, economic sanctions have significantly impacted the global economy. Sanctions issued by the U.S., UK and EU against Russia have grown in scope and complexity. Other countries, including China, have also issued sanctions against U.S. companies, which increases the burden on risk teams to ensure strict compliance. Notably, the U.S. Department of Justice has prioritized sanctions enforcement and will pursue sanctions evaders in 2024, increasing the magnitude of potential financial and reputation risks from violations.

Understanding your exposure to potential sanctions in emerging and established markets now requires more extensive due diligence and boots-on-the-ground knowledge than in the past. Simply reviewing lists of sanctioned entities may not uncover indirect sanctions exposure within your company's supply chain.

3 Social Unrest



Social unrest has defined our current era in ways that few other trends can match. Political demonstrations and activism can pose risk to assets and security in diverse sectors and countries. Climate activism, protests over conflict in the Middle East conflict, government reforms, migration, and sectors ranging from agriculture to the automotive industry have blurred the lines between political action and social movements.

However, open-source intelligence monitoring can provide suitable advanced warnings of unrest and may facilitate advanced planning for alternative supply chains, insurance packages and inventory. In addition, keeping a pulse on local public sentiment toward your company may help you to anticipate any social unrest issues that could directly impact ongoing operations.

ICONS/SHUTTERSTOCK

4 Misinformation and Disinformation

Respondents to the World Economic Forum's *Global Risks Report 2024* cited misinformation and disinformation risk as their top concern. Additionally, what was once the domain of politics and propaganda is now a risk to the private sector. In addition to threats to elections, companies worldwide also face new risks in the form of social engineering attacks, reputation threats and fraud risks from misinformation and disinformation. This year, disinformation in the form of deepfake attacks impersonating executive management cost one Hong Kong firm millions of dollars. Companies now even face professional disinformation agents that can target any company and tarnish its reputation.

Tackling disinformation threats requires establishing a team within your company to respond in the event of an incident. The team may include legal counsel, risk officers, public relations leaders and cybersecurity professionals who can establish and execute crisis response plans.

5 AI Implementation and Regulation

The competition over AI and the risks firms face when considering implementation of such technology are heating up. Government leadership in the U.S. and Europe have recently recognized the emerging risks posed by AI and announced new guidelines. However, the early announcements demonstrate that government officials currently need to improve their ability to regulate rapidly evolving technology, increasing the burden on the private sector to avoid violations of current and emerging regulatory requirements.

Aside from monitoring emerging regulations, companies will need to develop policies regarding the internal use of AI-based technology and how to mitigate risks posed by outside or foreign actors that may be utilizing the technology for illicit purposes.

6 Cybersecurity and Critical Infrastructure Risks

The new front lines in global conflict are frequently established through cyberattacks, and the risk of such attacks is heightened in areas near international conflicts. For example, Russia has ramped up attacks against companies located in Baltic states supporting Ukraine and NATO. Warfare today is also starting to include cyberattacks on critical infrastructure. In the Ukraine war, for example, Russia has waged cyberattacks against civilian power grids.

The Biden administration has also cautioned about emerging critical infrastructure security risks in the United States. Water utilities have repeatedly been targeted by nation-state hackers, for example. FBI Director Christopher Wray also recently warned of the threat to U.S. infrastructure due to Chinese hacking networks and the advanced placement of malware. Wray noted that Beijing has been placing "offensive weapons within our critical infrastructure poised to attack whenever Beijing decides the time is right."

Today, terrorists and hostile governments no longer confine themselves to government targets, often targeting the private sector as well. The U.S. Cybersecurity & Infrastructure Security Agency provides an in-depth breakdown of key risk sectors. Companies involved in the management of utilities, financial services, transportation, shipping and public venues are all at higher risk of attack.

To combat cybersecurity and critical infrastructure risks, firms must first examine their proximity to global conflict zones, even indirectly through suppliers or service providers. Then, companies must establish a cybersecurity plan for emerging international threats. The latter may require consulting with overseas partners to employ the most effective cybersecurity measures available to thwart potential or known attack patterns.

7 National Elections

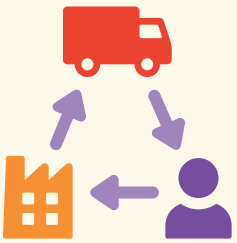
Elections can rapidly shift the regulatory and economic landscape. If a company is not prepared, the impact on its bottom line can be immediate. Heightened political activity and polarization can also translate into greater risk of civil unrest. Mitigating election-related risk requires scenario planning to ensure that existing compliance programs and operating plans will hold up in the event of different election outcomes.

8 Know Your Customer (KYC) Risks

To avoid bad actors, it is essential to know who you are doing business with. Depending on the scope and scale of a business, there may be hidden risk exposure to money laundering and sanctions evasion. As specific industries are more prone to these risks, businesses in such verticals are at greater risk of compliance failures regarding anti-money laundering (AML) regulation and KYC requirements. For example, the U.S. government has recognized the increased risks associated with real estate investment in the country. The Department of Treasury recently proposed a rule focused on curbing money laundering through real estate, particularly for all-cash deals.

All companies should assess their current KYC programs to best avoid exposure to money laundering or terrorist financing links, starting with understanding who their customers and clients are. It is also essential to periodically review a risk-ranking methodology in the context of shifting geopolitical conditions. Relying on available watch lists alone may not truly depict the current risk landscape as watch lists are backward-looking. Organizations shoud ensure that their risk management program incorporates a forward-looking mechanism to account for emerging risks.

9 Supply Chain Integrity



Supply chain disruption is still top-of-mind for many companies, especially those that have felt the impact of COVID-era breakdowns. Global tensions, including ongoing and emerging conflicts, directly impact supply chain integrity. From investors to customers, many stakeholders now prioritize avoiding supply chain-related environmental and social harm. Ensuring a healthy supply chain requires a deep understanding of the third parties involved, digging below the immediate tier-one suppliers and conducting due diligence on tier-two and tier-three entities.

Many companies are now reconsidering their supply chain networks and seeking new locations and partners with decreased risk exposure. In the coming years, organizations' long-term resilience may depend directly on supply chain reliability.

10 Inflation and Price Stability

Inflation and price stability can significantly impact both domestic and international revenue streams. Avoiding loss requires understanding the macroeconomic and microeconomic conditions impacting a given market. In Argentina, for example, the national currency recently became virtually worthless overnight, with inflation ultimately topping 200%. While this case is extreme, even minor fluctuations can impact the value and sustainability of overseas contracts. It is increasingly critical to consider inflation risk as part of contract and insurance negotiations.

How Risk Teams Can Prepare for and Mitigate Geopolitical Risk

While the risks above may seem daunting, there are steps risk professionals can take to minimize their firm's exposure and ensure business resiliency in 2024 and beyond.

- **Understand your firm's current risk profile and exposure to the global risk landscape.** Geopolitical risk can impact operations, supply chain integrity, cybersecurity protections and insurance premiums.
- **Consider integrating geopolitical risk-monitoring into existing risk management and reporting structures.** This can differ significantly by industry and company size. Stress-testing risk management programs against alternative geopolitical scenarios is also important.
- **Consider developing and delivering training on geopolitical risk.** The program's goal should be to educate risk management teams on what to look for on the global risk horizon. Identifying emerging risks can strengthen a company's ability to respond.
- **Ensure that any key investment decisions factor in geopolitical risk analysis.** This step requires integrating global risk assessments into due diligence processes. For example, due diligence around mergers and acquisitions should incorporate insight on how world events can impact well-established operating plans and projected valuations. Ultimately, an acquisition's value can rapidly erode based on changing geopolitical factors that may throw business operations off course.

Companies that integrate geopolitical risk analysis into their risk management programs can not only enhance their ability to spot and mitigate emerging risks, but also bolster their strategic planning capabilities and ensure long-term resilience. R

Christopher Mason is a CAMS-certified attorney and the vice president of global compliance and investigations at Infortal Worldwide. **Dr. Ian Oxnevad** is a political scientist, political economist and the director of geopolitical risk at Infortal Worldwide, where he leads the firm's geopolitical risk intelligence and analysis efforts.

GEOPOLITICAL CONFLICT INCREASING THREATS TO GLOBAL SHIPPING

While large vessel losses hit a record low in 2023, geopolitical risks are rapidly increasing the threats to global shipping, according to Allianz's *Safety and Shipping Review 2024*. Attacks on ships in the Red Sea by Houthi militants have led to significant changes in global shipping routes, with traffic through the Suez Canal (the primary passage between Europe and Asia) down more than 40% at the beginning of 2024. Alternate routes require circumnavigating Africa, meaning increased delays and costs for companies with global supply chains, as 90% of international trade is transported by sea. Rerouting along the Cape of Good Hope adds over 3,000 nautical miles and at least 10 days of sailing time for any vessel, while also increasing exposure to storms and rough seas that are harder on smaller ships that usually stick to coastal waters. As ships attempt to speed up to regain time, rerouting also has a significant environmental toll, with Red Sea diversions driving a 14% increase in emissions from the EU shipping industry alone last year. With more shipping traffic around the Horn of Africa, Somali piracy has also reemerged as a threat. In December, pirates staged the first successful hijacking of a vessel off the coast of Somalia since 2017 and attacks have continued throughout 2024.

— Hilary Tuttle

COMPANIES UNDERINSURED FOR CYBERATTACKS

In a study by cybersecurity software provider CYE, 80% of insured companies that suffered a data breach reported they did not have adequate coverage to offset the losses incurred. In fact, the average coverage gap was 350%, meaning that more than 75% of the costs from an incident were uninsured, amounting to an average uncovered loss of $27.5 million and an estimated 2.9% of company revenue. In some cases, the maximum coverage gap reached as high as 3,000%. Relatively "low-tech" sectors like accommodation and food services, construction, and transportation and warehousing were more adequately covered, while the finance and insurance, information, and manufacturing sectors saw the largest coverage gaps, often exceeding 100%. This disparity is likely due to heavier reliance on digital assets and systems in the latter sectors, which increase their vulnerability to attack. In addition, since data breaches in these high-risk industries can have such an immense impact, adequate insurance coverage can be difficult to obtain.

— Morgan O'Rourke

LESS THAN HALF OF COMPANIES HAVE NET-ZERO GOALS

As regulatory and consumer pressure grows for companies to increase their sustainability efforts, many are taking steps to cut their greenhouse gas emissions. However, according to S&P data, only 45% of U.S. organizations have made any net-zero commitments. The utilities, communications and consumer discretionary sectors have the highest percentage of companies with net-zero commitments, while consumer staples, real estate and materials have the lowest. To spur climate action, 15% of S&P 500 companies now link CEO compensation incentives to emissions reduction goals (up from 9% in 2021), while 27% have established incentives for other executives (up from 19%). "As investors obtain more climate-related information and more transparency into corporate emissions, companies could face more market pressure to build transition plans that include decarbonization or a net-zero goal," the report said. "Net-zero target-setting could evolve to become the norm."

— Jennifer Post

SHUTTERSTOCK/APCHANEL, N UNIVERSE

Spencer

2024 FUNDING THEIR FUTURE

Gala

THURSDAY, SEPTEMBER 12, 2024

6:00PM ET

CIPRIANI 42ND STREET

110 EAST 42ND STREET, NEW YORK, NY 10017

HONORING

LILIAN VANVIELDT-GRAY

Executive Vice President and Chief Diversity, Equity & Inclusion Officer

Alliant Insurance Services

For sponsorship and tickets, contact
fundingtheirfuture@spencered.org

Weird Workplace Injuries

According to a Pie Insurance survey, 30% of small business owners wished they had prioritized worker safety at the start of their venture. It is no wonder since 50% have had at least one injury claim in the past five years, some of which can be quite unique:

- A bird flew into a worker's face while they were on the roof of a house, breaking the worker's nose.
- A cork hit an employee in the eye after a customer opened a champagne bottle.
- An employee broke their foot after frantically running away from a spider.
- An employee accidently set himself on fire after attempting to burn trash using gasoline instead of diesel.
- An employee walked into a glass door they thought was open, injuring their nose.
- An employee slipped after being chased by a chicken.
- An employee broke his finger when he stepped from a truck and caught his wedding ring on the door handle.
- An employee was bitten on the finger by a baby skunk at a worksite.
- A cook got second-degree burns after dipping their hand into a vat of hot caramel.

Source: *Pie Insurance, The Wild West of Workplace Hazards*

AI RISK BY INDUSTRY

Swiss Re ranked the overall AI risk faced by 10 industries in terms of the probability of an AI-related incident taking place and the potential loss severity of such incidents. The following are the most at-risk industries today:

1. IT services
2. Energy & utilities
3. Health & pharma
4. Other (retail, hospitality, real estate, legal)
5. Mobility & transportation
6. Financial & insurance services
7. Government & education
8. Manufacturing
9. Media & communications
10. Agriculture, food & beverages

By 2034, the health & pharma and mobility & transportation sectors are expected to be hit the hardest by adverse AI effects.

Source: *Swiss Re Institute, Tech-tonic Shifts: How AI Could Change Industry Risk Landscapes*

SHUTTERSTOCK

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