Insurance Buyers' News

BPJ Insurance®

Springfield
PO Box 4207, Springfield, MO 65808
Phone: 800-422-5275
417-887-3550 • Fax: 417-887-3252

West Plains
PO Box 964, West Plains, MO 65775
Phone: 800-400-3896
417-256-6162 • Fax: 417-256-6165

Rolla
PO Box 1258, Rolla, MO 65402-1258
Phone: 800-364-2212
573-364-8888 • Fax: 573-341-2257

River City Insurance
PO Box 127, New Madrid, MO 63869
Phone: 800-899-7392
578-748-5215 • Fax: 573-748-5392

Climate Change September / October 2024 Volume 35 • Number 5

Climate Change Impacts Commercial Insurance Rates and Regulations

Recent headlines have highlighted the impact of climate change on homeowners insurance but commercial insurance lines are also experiencing its effects.

Homeowners

Homeowners across the U.S. have experienced substantial increases in insurance premiums. For instance, home insurance premiums rose by 21% between May 2022 and 2023. In high-risk states like Florida, premiums have jumped as much as 35%, making insurance less affordable for many homeowners.

In addition, some major insurers, including State Farm and Allstate, have stopped issuing new homeowners' policies in California due to the elevated wildfire risks. Other companies are following suit in various high-risk areas, leaving many properties without adequate insurance coverage.

Commercial Insurance

But climate change has also significantly impacted commercial insurance in the United States, leading to increased costs and changes in the way insurers manage risk.

1. **Rising Insurance Costs:** Due to the increased frequency and severity of extreme weather events, insurance costs for commercial real estate have escalated dramatically. For example, in states with high exposure to natural hazards, insurance costs have risen by 31% year over year and 108% over the past five years. This trend is

continued on next page

This Just In …

Customers of CrowdStrike, Inc. a cybersecurity technology company based in Sunnyvale, Calif., experienced a major outage on July 19, 2024, caused not by a cyberattack, but by a faulty sensor configuration update. The update triggered a logic error that resulted in system crashes and blue screens of death (BSOD) on affected Windows systems. The problematic update was part of regular updates deployed by CrowdStrike to its Falcon platform to address new cyber threats, specifically targeting malicious named pipes used in cyberattacks.

This update led to widespread system crashes affecting approximately 8.5 million Microsoft Windows devices globally. The impact was extensive, disrupting various sectors, including healthcare, retail, financial services, and air transport, with over 7,000 flights canceled or delayed.

CrowdStrike has since issued a fix and provided detailed remediation steps. The company says it has also initiated a thorough root cause analysis to prevent such issues in the future and communicated with customers to address the disruption and provide support.

The event is estimated to have cost the top 500 U.S. companies approximately $5.4

continued on next page

This Just In

billion in losses, though only between $540 million and $1.08 billion of these losses were insured. Experts note that the non-malicious nature of the incident meant that the insured losses were lower compared to a potential malicious event.

CrowdStrike is facing lawsuits from shareholders and some businesses. The shareholders' lawsuit, led by the Plymouth County Retirement Association, alleges that CrowdStrike made materially false and misleading statements about the reliability and testing of its software, which contributed to a 32% drop in the company's share price and a loss of approximately $25 billion in market value.

Additionally, Delta Air Lines is seeking damages for the financial impact of the outage, which resulted in an estimated $500 million loss due to canceled flights and other disruptions.

These lawsuits highlight the critical importance of reliable software and transparent communication about potential risks. CrowdStrike has stated that it believes the cases lack merit and plans to vigorously defend itself.

expected to continue, with a projected cost premium increase of 24% above the national average by 2030 for high-risk states.

2. **Insurers Exiting High-Risk Markets:** The added risk from extreme weather events has caused some insurers to reduce coverage or completely withdraw from certain states. This has left many commercial properties struggling to find affordable insurance options, increasing their vulnerability to climate-related losses.
3. **Increased Premiums and Financial Strain:** Insurers are raising premiums to build reserves leading to a difficult balance where premiums might become unaffordable for many businesses.

NAIC

Insurers are adopting various strategies to mitigate climate risk, including enhanced risk assessments, the use of predictive analytics, and the development of new insurance models tailored to specific climate risks. Regulators are also becoming more involved, with increased focus on insurers' preparedness and stress testing to ensure financial stability in the face of escalating climate risks

Thus, the National Association of Insurance Commissioners (NAIC) has implemented several measures to help insurance companies manage the impact of climate change. Currently, 14 states and the District of Columbia require insurers to report their climate-related risks to the NAIC Task Force on Climate-Related Financial Disclosures (TCFD), covering about 80% of the U.S. market.

It is fair to say that as climate change causes more losses for insurance companies, we can expect increased scrutiny on insurance transactions from legislators and insurance regulators.

Lawmakers, too, are increasingly recognizing the financial implications of climate change on the insurance industry. This is likely to drive legislative efforts aimed at enhancing consumer protection, promoting resilience, and ensuring that insurance markets remain stable and competitive in the face of climate risks

According to a recent report from Deloitte, "It's likely that regulators will at some point start requiring more of insurers in the way of disclosure and its components and assumptions—including stress tests of a wide range of plausible climate-change scenarios and a determination of how climate data is used in risk modeling for pricing and underwriting decisions."

DEI Suit Brought Against Wells Fargo Bank

Do D&O Policies Cover Hiring Practices?

The short answer is that a Directors & Officers policy exists to protect the insureds against *any* type of action brought by shareholders, including allegations of not honoring diversity, equity, and inclusion (DEI)commitments. A case in point is the recent lawsuit against Wells Fargo Bank brought by its shareholders, specifically led by SEB Investment Management AB, among others.

The lawsuit alleges that Wells Fargo misled shareholders by promoting a commitment to diversity in its hiring practices while conducting sham interviews with non-white and female candidates it had no intention of hiring. The legal action claims that Wells Fargo's practices deceived investors about the company's true commitment to DEI initiatives.

Wells Fargo first attempted to get the shareholder case against it dismissed. While U.S. District Judge Trina Thompson of the U.S. District Court for the Northern District of California previously dismissed a version of the lawsuit in August 2023, she later found sufficient evidence of potential fraudulent intent in the revised lawsuit and ruled that Wells Fargo must face the claims. Judge Thompson's decision was based on direct and indirect evidence that the bank intended to deceive shareholders about its commitment to hiring diversity.

Shareholders cited interviews with former employees, an internal whistleblower email, and the sudden retirement of a senior wealth manager who allegedly pressured the whistleblower into conducting fake interviews.

In a statement, Wells Fargo said it would continue defending against the lawsuit. It noted that the Department of Justice and Securities and Exchange Commission closed investigations into its hiring practices without taking action.

"Wells Fargo is deeply dedicated to diversity, equity and inclusion and does not tolerate discrimination in any part of our business," it added.

Wells Fargo's share price fell 10.2% over two days in June 2022, wiping out more than $17 billion of market value, after the *New York Times* reported the Justice Department probe.

In any case, Wells Fargo, like many large

continued on next page

corporations, likely holds several types of insurance that could potentially provide protection against a lawsuit alleging fraudulent practices related to its hiring policies. Key types of insurance that could be relevant include:

1. **Directors and Officers (D&O) Liability Insurance:** to protect the personal assets of corporate directors and officers, and the company itself, against claims of wrongful acts, including allegations of fraud or misrepresentation. D&O insurance can cover legal fees, settlements, and other costs associated with defending against lawsuits brought by shareholders or regulators.
2. **Employment Practices Liability Insurance (EPLI):** EPLI covers claims made by employees alleging discrimination, wrongful termination, harassment, and other employment-related issues. While this typically focuses on claims made by employees rather than shareholders, some policies might cover related regulatory investigations or lawsuits stemming from employment practices.
3. **Errors and Omissions (E&O) Insurance:** Also known as Professional Liability Insurance, E&O coverage protects companies and their employees against claims of negligent acts, errors, or omissions in the performance of professional services. In some cases, this might extend to cover claims related to misrepresentations in hiring practices, especially if these practices are tied to the company's professional services.
4. **General Liability Insurance:** While general liability insurance typically covers bodily injury and property damage claims, some policies might include coverage for personal and advertising injury, which could potentially extend to certain types of misrepresentation claims.

In the specific context of the Wells Fargo lawsuit, D&O liability insurance would be the most directly relevant, as the lawsuit involves allegations of fraudulent statements made to shareholders, implicating the actions of the company's directors and officers.

Does Your Business Need Flood Insurance?

A standard commercial policy typically does not cover damage due to flooding, including hurricane storm surge flooding.

Natural disasters can be devastating to businesses. While damage caused by some natural events—such as lightning or wind—is usually covered by commercial property insurance, you need a special policy to protect against flood damage. This Q&A from the Insurance Information Institute will help you understand this type of coverage and determine whether your business needs it.

Q: Does my commercial property insurance include flood coverage?

A: No. Damage from flooding, including flooding caused by hurricane-generated storm surge, is typically not covered under a standard commercial policy, including a Commercial Package Policy (CPP) or a Business Owners Policy (BOP). Flood insurance is available from the federal government's National Flood Insurance Program (NFIP).

Q: What does flood insurance cover?

A: Flood insurance covers damage to your building and contents caused by flood. This includes losses resulting from overflowing rivers or streams, heavy or prolonged rain, storm surge, snowmelt, blocked storm drainage systems, broken dams or levees, and similar causes. To be considered a flood, waters must cover at least two acres or affect two properties. Generally, if water comes from above, such as from rain or melting snow overflowing gutters and leaking onto your inventory, you'll be covered by your standard

continued on next page

commercial property insurance.

Q: What isn't covered by flood insurance? A: Property outside your building, such as landscaping and septic systems, is generally not covered. Additionally, flood insurance will not cover damage to your business vehicles; however, this can be included in the optional "comprehensive" portion of your business vehicle insurance. Financial losses caused by business interruption or loss of use of insured property are also not covered.

Q: Do I have to purchase flood insurance? A: If your commercial property is in a high-risk flood area and you have a mortgage from a federally regulated or insured lender, you are required to purchase a flood insurance policy.

Q: How do I determine my risk for flood damage?

A: Location is the most important factor in assessing your risk for flood damage. Is your business located in or near a flood zone? (Flood map search tools can be found online.) Where in the building is your business's equipment and inventory located? Anything housed on a lower floor will be at greater risk.

Q: How long does it take to get flood coverage?

A: Typically, there's a 30-day waiting period from the date of purchase before your policy goes into effect.

Q: Does my flood policy cover mold?

A: Damage from mold and/or mildew resulting from the after-effects of a flood is covered, but each case is evaluated individually. Mold/mildew conditions that existed prior to a flooding event are not covered. After a flood, the policyholder is responsible for taking reasonable and appropriate mitigation actions to eliminate mold and mildew.

Q: How much flood coverage can I get?

A: Commercial flood insurance provides up to $500,000 of coverage for your building and up to $500,000 for its contents.

Q: What if I need more coverage?

A: You can purchase what's called excess insurance coverage to rebuild properties valued above National Flood Insurance Program (NFIP) limits. Excess coverage includes protection against business interruption. Contact your broker for more information.

Q: Where can I purchase flood insurance? A: Flood insurance is available from the NFIP and some private insurers. However, NFIP coverage can only be purchased through an insurance professional; you cannot buy it directly from the federal government. Please call us, and we will be pleased to help you.

6 Cybersecurity Coverages To Help Mitigate a "CrowdStrike" Outage

The CrowdStrike outage, significant though it was, could have been much more severe if it had been the result of malicious intent. The event underscores how critical it is for companies to carry comprehensive cybersecurity insurance that includes these key components:

1. **Business Interruption Coverage:** for lost income and operational expenses incurred due to a cyber incident. It's crucial for policies to include both direct business interruption and contingent business interruption, which covers losses resulting from disruptions to third-party services or suppliers.
2. **Incident Response Coverage:** to cover the costs associated with responding to a cyber incident, including forensic investigations, legal fees, public relations efforts, and notification costs for affected individuals.
3. **Data Restoration and Systems Recovery:** to pay for the costs associated with restoring and recovering data and systems impacted by the cyber event. Given the nature of the CrowdStrike incident, where systems were rendered inoperable, this type of coverage would be vital.
4. **Cyber Liability Coverage:** to protect against third-party claims arising from a cyber incident, including lawsuits and regulatory fines. This is essential for covering the legal liabilities and costs associated with data breaches or other cyber incidents.
5. **Coverage for Non-Malicious Events:** As the CrowdStrike incident was caused by a non-malicious software update, it's crucial for policies to cover a wide range of incidents, including those that are not the result of deliberate attacks. Ensuring the policy language is broad enough to encompass such events can provide necessary protection.
6. **Third-Party Coverage:** Given that many companies rely on external vendors and service providers, it's important to have coverage that addresses incidents stemming from third-party failures. This includes coverage for financial losses due to disruptions caused by third-party service providers.

When companies include these comprehensive elements in their cybersecurity insurance policies, they can be better equipped to manage and mitigate the financial impacts of incidents like the CrowdStrike outage.

Insurance Buyers' News