Insurance Buyers' News

BRJ Insurance

Joplin
1801 W 32nd Street, Building C, Suite 207
Joplin, MO 64804
Phone: 800-422-5275 • 417-887-3550
Fax: 417-887-3252

Nevada Insurance Agency
300 S Johnson Dr. Nevada, MO 64772
Phone: 800-527-0808 • 417-667-6444
Fax: 417-667-3041

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

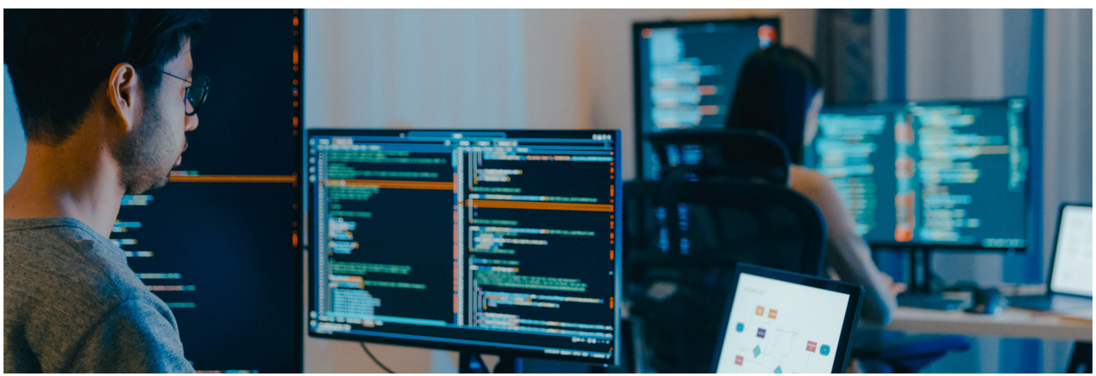
Rolla
PO Box 1258, Rolla, MO 65402-1258
Phone: 800-364-2212
573-364-8888 • Fax: 573-341-2257

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

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

Cybersecurity September / October 2025 Volume 36 • Number 5

Cybercrime in the U.S. — Escalation and Adaptation



Cybercrime in the United States has reached critical levels, with economic damages and operational disruptions intensifying year over year. According to the FBI's Internet Crime Complaint Center (IC3), more than 1 million complaints were filed in 2024, representing over $12.5 billion in reported losses—a staggering 30% jump from 2023. And as 2025 unfolds, early indicators suggest even greater vulnerability across sectors.

High-Profile Incidents

Recent attacks spotlight both the scale and creativity of cybercriminals:

continued on next page

This Just In …

The Property &Casualty Insurance is showing signs of softening, especially after several years of steep rate hikes:

- Average premium increases across all account sizes were 4.2% in Q1 2025, down from 5.4% in Q4 2024.
- Commercial property rates rose just 2.6%, one of the lowest increases in recent quarters.
- General liability rates are still climbing, but at a slower pace—averaging 3.95% in February, down from 4.19% in January.

This cooling is largely due to increased competition, new capital entering the market, and improved underwriting results, especially in personal lines.

Sector-Specific Insights

Here's how different lines are behaving:

continued on next page

- Change Healthcare (UnitedHealth, Feb 2024): A ransomware assault paralyzed nationwide billing systems, delaying reimbursements and threatening patient care logistics. The disruption exposed systemic risk in healthcare IT.
- LoanDepot Breach (Jan 2024): Hackers accessed sensitive financial data on 16.6 million borrowers. Fallout included regulatory probes and costly litigation tied to consumer privacy violations.
- Dallas County Government Attack (Apr 2024): Criminals published sensitive documents online after ransomware demands were refused, underscoring vulnerabilities in public-sector data governance.

These examples represent a broader pattern: attackers aren't just chasing money—they're disrupting infrastructure, weaponizing information, and exploiting third-party systems with surgical precision.

Cybercrime Trends to Watch

Several key trends define today's digital threat landscape:

- Ransomware tactics have evolved, with "double extortion" now standard: files are encrypted, and sensitive data is leaked or threatened to pressure payment.
- AI-powered phishing is on the rise. Attackers use generative tools to mimic real employees, personalize bait emails, and bypass spam filters.
- Third-party risks are multiplying, especially in sectors like healthcare, education, and finance. Vendors with outdated protocols create soft entry points into otherwise secure systems.
- Even small and mid-sized firms are increasingly targeted—not because they're high-value, but because they're under-defended.

The message is clear: every business with customer or financial data is in the crosshairs.

How Businesses Can Respond

To minimize risk, organizations should:

- Prioritize regular software updates and security patching
- Require multi-factor authentication (MFA) on all systems
- Roll out cybersecurity training with realistic phishing simulations
- Invest in endpoint protection and behavior-based threat detection tools
- Formalize a crisis response strategy, including legal counsel and PR planning

Cybersecurity is no longer an IT silo—it's a board-level concern tied directly to business continuity and brand reputation.

Insurance Products to Consider

Modern cyber insurance offerings are evolving to reflect current threats:

Cyber Liability Insurance

- Covers breach response, forensics, business interruption, legal defense, fines, and ransom negotiation
- Often includes incident response coordination and media handling

Tech E&O (Errors & Omissions)

- Ideal for SaaS and IT firms
- Covers liability from failed services or negligent performance that results in client loss

Crime Insurance

- Focuses on social engineering, wire fraud, and employee theft
- Often paired with cyber coverage for comprehensive protection

This Just In

Sector	Pricing Trend (2025)	Notes
Commercial Property	Softening	More competition, reduced deductibles, and new capital inflows
General Liability	Slight increases	Social inflation still driving litigation costs
Workers' Compensation	Decreasing (avg. -2.6%)	Most profitable line; rates declining for 15+ years
Personal Auto	Stabilizing	Underwriting profits normalizing; rate increases tapering
Excess Casualty & D&O	Vulnerable to reserve pressure	Still facing adverse development and litigation exposure

Forecasts from AM Best & Others

- **AM Best reports that workers' comp remains highly profitable, but warns of rising medical costs and litigation severity, especially in California.**
- **S&P Global expects combined ratios to improve slightly in 2025 (98–100), with premium growth around 8–9%.**
- **Swiss Re forecasts stable ROE (~10%) for the P&C industry, with underwriting margins narrowing but investment income offsetting losses.**

In workers' comp, wage inflation is pushing up premiums, but claim severity—especially medical costs—is the bigger concern. Some carriers are tightening underwriting for high-risk accounts, while well-performing risks may still see flat or declining rates.

Underwriting requirements are tightening. Insurers now expect proactive risk management—strong security protocols, clean audits, and incident planning—as a baseline for coverage eligibility and pricing.

Three Key Terms Business Insurance Policyholders Should Understand

While it's a good idea to read your insurance policy, hardly anybody does. The important thing is to understand what's in it. Here are three concepts to know about how your insurance works.

What is Subrogation and How Does It Apply to Insurance?

Subrogation in the context of insurance is the right of an insurance company to "step into the shoes" of the insured after the company has paid the loss. Subrogation entitles the insurance company to assert any rights on its own behalf that the insured may have had to recover payment from the parties that caused the loss.

Subrogation shows up across various types of insurance policies:

- **Auto insurance:** If you have collision coverage, your insurer pays for repairs regardless of fault. If another party caused the damage, your insurer may pursue that party to recover what it paid.
- **Workers' compensation:** If an injured worker is compensated due to malfunctioning equipment, the insurer may subrogate to the worker's right to sue the manufacturer for reimbursement.
- **Property leases:** Mutual waivers of subrogation are common, where landlords and tenants agree not to seek recovery from each other's insurance. Most policies permit these waivers—so long as they're agreed to before the loss.

continued on next page

Proximate Cause vs. Immediate Cause

Coverage disputes often hinge on the definition of "cause." Even if a policy is labeled "all-risk," there must be a close connection between the covered cause and the resulting damage. This is known as "proximate cause."

Black's Law Dictionary defines proximate cause as "that which, in a natural and continuous sequence, unbroken by any efficient intervening cause, produces the injury, and without which the result would not have occurred."

Proximate cause is not the same as the "immediate cause," which may be the last event before the loss. For example:

- **Basic property insurance:** It may not cover water damage—but if a fire leads to firefighting efforts that cause water damage, the policy may still cover the loss, because the fire was the proximate cause.

Many cases are not this clear-cut, and courts often side with the insured when a policy's wording is ambiguous.

Key Exclusions in Business Owner Property Policies

Even robust policies include exclusions that limit coverage. These exclusions can have critical consequences depending on the type of loss:

- **Flood and earthquake:** Typically excluded unless a separate rider or policy is purchased. Many businesses falsely assume they're protected until disaster strikes.
- **War, nuclear hazard, and government action:** Standard exclusions in nearly all property policies.
- **Wear and tear, rust, deterioration:** Ordinary aging of property isn't covered.
- **Dishonest or criminal acts:** Losses caused by fraud or illegal conduct by the insured (or their employees) are excluded.
- **Mechanical breakdown:** Many BOP policies exclude this unless added via endorsement.
- **Mold, fungi, bacteria:** Covered only under very specific conditions, often with strict limits.
- **Business interruption exclusions:** Coverage only applies if the cause of interruption is a covered peril—so exclusions can quickly derail a claim.

Reading exclusions carefully can be the difference between a covered claim and a surprise denial.

The State of D&O Insurance in 2025

Directors and Officers (D&O) liability insurance continues to evolve in 2025, shaped by litigation trends, regulatory shifts, and emerging technologies. After several years of softening premiums, the market is showing signs of stabilization. While pricing remains competitive, underwriters are increasingly cautious, especially in sectors facing heightened litigation or regulatory scrutiny.

One of the most notable recent rulings came from the Delaware Supreme Court in *Origis USA LLC v. Great American Insurance Company*, which clarified how prior acts exclusions and no-action clauses interact in layered D&O programs. The court upheld exclusions in newer policies but remanded a portion of the case to explore whether advancement provisions override no-action clauses. This decision underscores the importance of precise contract language and has prompted insurers to revisit how defense cost obligations are structured.

Underwriters in 2025 are focused on several key concerns:

- **AI-related exposures**, including misrepresentation of capabilities ("AI washing") and lack of oversight in third-party vendor use.
- **Cybersecurity failures**, especially those tied to board-level decisions.
- **Derivative lawsuits**, which continue to rise, often targeting governance lapses.
- **Bankruptcy-related claims**, as economic pressures mount across industries.

In response, insurers are adding or tightening provisions. Enhanced coverage for entity investigation costs is becoming more common, while sublimits for ESG-related claims and AI disclosures are being introduced. Some carriers are also revisiting bump-up exclusions, as seen in the Towers Watson case, where a $90 million settlement was denied coverage due to merger-related valuation disputes.

Coverage is far from standardized. While most policies include the

continued on next page

familiar ABC structure (Sides A, B, and C), the breadth of exclusions, defense obligations, and sublimits vary widely. This variability makes brokers indispensable—not just for negotiating pricing, but for tailoring coverage to a company's risk profile, governance practices, and industry exposures.

As the market matures, companies are urged to reassess their D&O programs, especially those that scaled back coverage during the hard market. With litigation complexity rising, the right policy could mean the difference between resilience and reputational damage.

Emerging D&O Risks That Demand Board-Level Attention

As D&O insurance evolves, so do the exposures that trigger coverage. Here's a closer look at four increasingly relevant risks that directors and officers must navigate with precision:

AI Washing and Oversight Failures

AI washing refers to the practice of overstating or misrepresenting a company's use of artificial intelligence to attract investors or inflate valuations. Companies may claim their products are "AI-powered" when they rely on basic automation or manual processes. The SEC has begun cracking down on misleading AI disclosures, and shareholder lawsuits have followed when performance fails to match the hype. D&O insurers now scrutinize AI governance, requiring boards to demonstrate oversight of third-party vendors, data privacy, and disclosure accuracy.

Derivative Lawsuits: Governance Under Fire

Derivative suits are brought by shareholders on behalf of the corporation, typically alleging that directors or officers breached fiduciary duties. These claims often target failures in oversight, self-dealing, or mismanagement. Because settlements are paid to the corporation—not the shareholders—Side A D&O coverage becomes critical, as companies cannot indemnify executives for these payouts. The rise in large-dollar settlements, especially in M&A and fraud cases, has made robust Side A protection a boardroom priority.

Bankruptcy-Related Claims: Coverage Gaps Loom

When a company enters bankruptcy, directors and officers lose access to corporate indemnification. This exposes them to personal liability for pre-bankruptcy decisions, including alleged mismanagement or breach of duty. Coverage disputes often arise over whether D&O proceeds are part of the debtor's estate, and courts may restrict access to policy funds. Policies with clear "order of payments" and bankruptcy carve-outs are essential to ensure executives aren't left defenseless when insolvency strikes.

These risks aren't theoretical—they're active fault lines in today's D&O landscape. Boards must treat them as strategic priorities, not just insurance footnotes.