STACK Expands Cyber Insurance Services

Cybersecurity, Compliance Firm Aims to Make More Businesses Insurable, Recoverable from Cyber Incidents

DETROIT, MI, UNITED STATES, May 9, 2026 /EINPresswire.com/ -- STACK Cybersecurity, a Michigan-based cybersecurity and compliance firm, announced a strategic expansion of services focused on helping businesses become both insurable and recoverable in the face of cyber incidents.

The announcement comes as cyber insurance continues to evolve from a financial safeguard into a verification mechanism for security posture.

Cyber Insurance Has Changed. Most Businesses Haven't.

Cyber insurance is defined by federal and industry sources as a form of financial protection that helps companies offset the costs of responding to and recovering from cyber incidents, including data breaches, ransomware, and business interruption.

Policies are structured around two core functions. First-party coverage addresses direct costs, such as incident response, legal obligations, and lost income. Third-party coverage addresses liability stemming from claims brought by customers, vendors, or regulators.

That definition hasn't changed. What has changed is how coverage is granted and enforced.

"Cyber insurance used to feel like a policy you bought," said Tracey Birkenhauer, Chief Impact Officer at STACK Cybersecurity. "Now it functions more like an audit. Carriers are validating whether your controls are in place, not whether you said they were."

Shift from Coverage to Verification

As cyber risk has increased, insurers have tightened requirements and introduced more precise underwriting standards.

Government reporting shows cyber insurance remains a tool to help businesses recover from common risks like data breaches and ransomware. At the same time, insurers are limiting exposure to systemic events and narrowing coverage in high-risk scenarios.

Policies no longer assume protection. They require proof.

“Insurance is part of risk transfer,” Birkenhauer said. “But risk transfer only works when the underlying controls are real, enforced, and documented. If there is a gap between what is implemented and what was represented, that gap shows up during the claim.”

Industry and academic research consistently frames cyber insurance as a complement to technical safeguards, not a replacement for them. Companies cannot rely on mitigation measures alone, but they also cannot rely on insurance without those measures in place.

For small and midsize businesses, this creates a problem. Applications are completed under time pressure. Controls are described broadly. Enforcement is often inconsistent. The result is a mismatch between policy requirements and operational reality.

“When a business files a claim, the insurer isn't just responding to the incident,” Birkenhauer said. “They're validating the environment. They're asking whether multi-factor authentication was enforced, whether backups were tested, whether response timelines were met. That is where coverage is decided.”

STACK Cybersecurity’s Approach: Insurable and Recoverable

STACK Cybersecurity’s expanded offering focuses on closing that gap through two outcomes.

Insurable. Your controls align with insurer expectations, are deployed consistently, and can be demonstrated with evidence.

Recoverable. You can contain, respond to, and recover from an incident without relying solely on a policy outcome.

STACK’s services integrate operational security, compliance frameworks, and insurance readiness into a single model designed for manufacturers, construction firms, and regulated small businesses.

“Most businesses are trying to answer three separate questions,” Birkenhauer said. “Are we secure enough, are we compliant, and will insurance cover us if something happens? Those questions are connected. We treat them as one.”

Manufacturers face a different set of cyber insurance challenges because their risk is tied directly

to operations, not just data. Cyber insurance is intended to help offset the financial impact of incidents such as data breaches, ransomware, and business interruption. But in a manufacturing environment, interruption is often the primary exposure. A disruption to a production line, a compromised supplier connection, or a failure in industrial control systems can halt output, delay contracts, and create downstream liability across the supply chain.

Policies may cover lost income and response costs through first-party coverage and address third-party liability tied to customers or partners, but only if the manufacturer can demonstrate core controls were in place and enforced. The issue is whether security, uptime, vendor access, and compliance expectations are aligned well enough for coverage to respond when production is on the line.

STACK Cybersecurity's new service offering addresses this directly by carving out manufacturing-specific pathways to insurability and recoverability, with targeted focus on production environments, supplier access controls, and compliance frameworks that align operational security with insurance requirements.

Why This Matters Now
Cyber insurance remains an essential part of business risk management, particularly for firms managing sensitive data or operating in regulated supply chains. At the same time, coverage decisions increasingly depend on control validation, not intent.

Federal guidance reinforces the role of cyber insurance as one component of a broader risk strategy that includes identification, mitigation, and recovery. That framework leaves little room for assumptions.

"Recovery is not a moment," Birkenhauer said. "It's a process. Insurance can support that process, but it can't replace it."

Tracey Birkenhauer
STACK Cybersecurity
+1 734-744-5300
email us here
Visit us on social media:
LinkedIn
Instagram
Facebook
YouTube

---

we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.