Staffing Agencies

Benefits of a Smart Cyber Insurance® Policy

The Big Picture: While Staffing Agencies may not be the first sector to come to mind when thinking of cyber attacks, they are often prime targets for hackers due to the vast amount of personal information they store about their clients. The threat of a hacker publishing client names, Social Security numbers, or passport numbers not only bears a financial burden for staffing agencies but also carries an unparalleled reputational risk.

What's New? There were roughly **623 million ransomware attacks globally in 2021**, and staffing agencies need to actively implement cybersecurity best practices to help reduce the chance of becoming victims of cyber incidents.

Your Solution: Adequate cyber liability coverage and risk management practices are now essential. Staffing agencies should have cyber liability insurance to cover the cost of a cyberattack, including first- and third-party coverages such as ransomware and social engineering.

Cyber Claims Examples

A Michigan-based staffing agency was the victim of a sophisticated ransomware attack in October 2021. The attack caused a temporary disruption to company servers and leaked over 81,000 Social Security numbers.

The world's largest global staffing agency experienced an Egregor ransomware attack in December 2020. The agency employs over 38,000 people and lost files containing accounting spread-sheets, financial reports, and legal/business documents.

One of the largest US-based IT staffing agencies was hit with a REvil ransomware attack in January 2020 that exposed commercial and personal employee data. The agency has over 10,500 employees and supplies staffing to Fortune 500 clients alongside government agencies.

Smart Cyber + Cyber Excess Policy Highlights

Reputational Damage
One of the most impactful consequences of any cyber incident is the reputational damage done to an organization. Loss of trust from key partners and clients can devastate a staffing agency and hinder its ability to forge new business relationships or place clients.

PII Protection & Coverage
Staffing agencies maintain a wealth of Personally Identifiable Information (PII) about their clients and employees, including Social Security numbers, home addresses, employment history, etc. Cyber coverage will pay for the costs of investigating a potential breach, determining if notification is required, and providing notification services to affected individuals.

vCISO Digital Experience
Policyholders receive on-demand access to actionable advice, tailored IT security recommendations, and resources to help reduce risk and provide a full scope of their business's IT security posture.

Vulnerability Alerting
Policyholders receive notifications of emerging cybersecurity risks and new vulnerabilities on their systems through Corvus email alerts to help proactively prevent future cyber attacks.

Risk Mitigation Services
Through the policy term, we offer a suite of complementary and reduced-cost services aimed at helping our policyholders prevent, prepare for, and respond to any cyber incident.

Incident Response
Corvus's dedicated breach response and cyber claims teams work with you during the entire life cycle of an insurance claim. We also provide assistance with the engagement of trusted partners, including breach counsel and forensics firms to ensure success.

Industry Benchmarks

Limit Benchmarks
While recommended limits will vary by the specifics of each risk, these benchmarks approximate the Smart Cyber Insurance® coverage purchased by organizations grouped by gross annual revenue. (Corvus offers limits of up to $5m for primary and excess Cyber policies).

* Data reflects Corvus primary policies only. Policyholders may be achieving aggregate limits greater than $5 million through excess policies.

Annual Revenue	Typical Limit Purchased
Up to $50m	$1.5m
$50m - $200m	$3.5m
$200m - $300m	$4m
$300m +	$5m

Eligibility for such programs is determined when you apply for coverage. Policy quotes, terms and conditions, and premiums are made in accordance with Corvus Insurance's underwriting guidelines. The policy, not general descriptions or material within this document, will form the contract between the insured and our insurance carrier partners. Coverage may not be available in all jurisdictions.

CORVUS

Brian Alva
Vice President of Cyber Underwriting
balva@corvusinsurance.com

At Corvus, our mission is to make the world a safer place by helping organizations mitigate or eliminate the impact of adverse events. We're the leading provider of data-driven Smart Commercial Insurance® products, with offerings in cyber and technology E&O. Our nationally distributed team includes many of the most experienced Cyber Insurance underwriters.

Contact your insurance broker for a quote today!