Logistics, Distribution + Warehousing

Benefits of a Smart Cyber Insurance® Policy

The Big Picture: The logistics, distribution, and warehousing industries have always relied heavily on their employees and internal systems to operate and satisfy customers. Even though these industries are traditionally rooted in the physical world, the rapid introduction of digital solutions for logistics and business operations has opened the door for new and challenging cyber risks.

What's New? In 2021, **37% of all businesses and organizations suffered a ransomware attack**, totaling $20 billion worldwide. Industries such as logistics, distribution, and warehousing, have become high-risk targets: their distributed locations, employees, and assets offer openings for cybercriminals.

Your Solution: Adequate cyber liability coverage and risk management practices are now essential. Companies in the logistics, distribution, and warehousing industries 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 leading Australian logistics group was hit with two separate ransomware attacks within three months of one another in the first half of 2020. The attacks shut down their online portal and prevented customers from tracking package delivery statuses.

A Seattle-based global logistics giant suffered a ransomware attack in February 2022 that shut down its systems and halted operations. The company fears that the attack will result in an "adverse impact on our business, revenues, results of operations and reputation."

A global logistics firm operating in 173 countries experienced a RansomExx attack in December 2021 that resulted in 70 GB of stolen documents published on the web. The stolen data included confidential business agreements, intra-company emails, and more.

Smart Cyber + Cyber Excess Policy Highlights

Social Engineering & Cyber Crime
Cybercriminals often use social engineering tactics, such as phishing, to gain valuable information from their victims. The information gathered is typically used to gain access to bank accounts, resulting in stolen funds. Cyber coverage helps businesses cover the cost of a social engineering attack.

Coverage for Ransomware Remediation
When a business suffers a ransomware attack, cybercriminals typically encrypt/ threaten to delete company data. Cyber coverage helps businesses, such as those in logistics, distribution & warehousing, pay for the cost of the ransom to end the threat or unencrypt data.

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).

Annual Revenue	Typical Limit Purchased
Up to $50m	$1m
$50m - $200m	$2m
$200m - $300m	$3m
$300m +	$4m

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

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!