Municipalities + Government Organizations

Benefits of a Smart Cyber Insurance® Policy

The Big Picture: Local governments have become disproportionate targets of cyberattacks due to decentralized and antiquated IT systems. With the rise of ransomware, traditional fears of data loss and theft from breaches have given way to an ever-changing array of threats capable of crippling government functions while causing significant monetary loss.

What's New? Between 2017-2020, **246 ransomware attacks struck U.S. government organizations**, impacting over 173 million people and costing an estimated $52.88 billion. The level of risk for local government organizations is rapidly evolving, requiring agility and vigilance to get ahead of modern cyber threats.

Your Solution: Adequate cyber liability coverage and risk management practices are now essential. Government organizations 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

The Washington, D.C. police department suffered a Babuk Group ransomware attack in May 2021, resulting in over 250 gigabytes of stolen data. The police department offered the hackers $100,000, but the group demanded a $4 million ransom instead.

Baltimore County Public Schools fell victim to a brutal ransomware attack in the fall of 2020. The school district was unprepared for a security event of this caliber and, as a result, was forced to cancel classes for two days, costing several million in recovery costs.

Webster Township in Washtenaw County experienced a ransomware attack in April 2021 that wreaked havoc on their online footprint. The attack forced the county's cyber team to create a new website, new emails, and new anti-virus/ransomware software to remediate the attack.

Smart Cyber + Cyber Excess Policy Highlights

PII/PCI Protection & Coverage
Local governments maintain a wealth of Personally Identifiable Information ("PII") and Payment Card Industry ("PCI") information about their citizens, including social security numbers, home addresses, utility payment records, credit card information, 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.

Coverage for Third-Party Risk
Government organizations increasingly transfer or entrust data to third-party vendors such as cloud storage companies to cut costs. Cyber coverage protects government organizations during a breach regardless of who caused it or where the data resided at the time of the compromise.

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	$1.5m
$50m - $200m	$3.5m
$200m - $300m	$4m
$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!