CORVUS

Our Underwriters' Most Highly Desirable Industries - 2023

What we're writing:

Using company-specific data collected from the Corvus Scan combined with up-to-the-moment threat intelligence, Corvus analyzes gaps in cyber hygiene and provides risk mitigation support throughout the policy period. This strategy places us in the perfect position to keep policyholders safe and brokers informed.

While Corvus is able to consider a wide variety of industries for eligibility for a Smart Cyber Insurance policy, there are a few select risk classes that we are looking most forward to writing in the coming year. See below for our curated list of trades and businesses.

Smart Cyber Appetite

Primary: Risks earning up to $2B in gross annual revenue

Excess: Risks earning up to $2B in gross annual revenue

Capacity

- Limits up to $5M

Classes

- Manufacturing
- Banking/Finance
- Medical Services
- Auto Dealers
- Consulting
- Construction Services
- Employment Services

Do you have these types of clients who are looking for cyber insurance?

Contact your Territory Manager or reach out to flock@corvusinsurance.com

Manufacturing

As the shift towards automation continues across manufacturing, these companies offer threat actors a high-value target during time-sensitive production runs.

Why Corvus underwriters like this industry:
With minimal personally identifiable information and a limited third-party exposure, we can offer broad policy language and competitive terms.

Banking & Finance

Financial and corporate confidential data carries a particularly high value to cybercriminals due to the confidential information connected to customer accounts.

Why Corvus underwriters like this industry:
The combined forces of strict regulations and tight security controls reduce the chances of successful business email compromises and breaches (a leading driver of claims).

Medical Services

Medical services are one of the most often targeted industries because of the sensitivity of PHI, regulatory exposure and the high stakes of critical IT systems for operations.

Why Corvus underwriters like this industry:
Due to the nature of the industry, organizations must meet strict compliance guidelines and possess leading security controls.

Auto Dealers

In 2022, 15% of auto dealers reported experiencing a cyberattack, with 85% of incidents occurring due to phishing.

Why Corvus underwriters like this industry:
Regulations limit an organization's risk profile and there is little personal identifiable information in comparison to the industry's scale.

Consulting

Businesses in the consulting field regularly work with clients that have high revenues, valuable digital assets, and larger customer bases, so they may be seen as a prime candidate for cyber attacks.

Why Corvus underwriters like this industry: Services are performed at the client level — with little third party data — vastly reducing privacy exposure.

Construction Services

The adoption of web-connected tools has rapidly grown across the construction industry, but so has the risk of cyber incidents. With large receivables and payables, construction firms are often the target of funds transfer fraud.

What Corvus underwriters like: With less complex networks and limited web footprint, Business Interruption and PCI losses have a reduced impact due to how they transact business.

Employment Services

Employment services (including PEOs, agencies and recruiters) are seen as prime targets for hackers due to the sheer amount of client-based personal information kept on record.

Why Corvus underwriters like this industry: Since payments are typically only received when employees are placed — limiting wire transfers — crime exposures are typically low.

CORVUS

Do you have these types of clients who are looking for cyber insurance?
Contact your Territory Manager or reach out to flock@corvusinsurance.com

corvusinsurance.com | 9/23