CORVUS

# Smart Cyber Reinsurance

## Embedded Cyber for Today's Environment

# Who is Corvus?

Through insurance products and digital tools we are reducing risk, increasing transparency, and improving resilience for policyholders and program partners. Corvus's market-leading specialty insurance products are enabled by advanced data science and include Smart Cyber Insurance®, Smart Tech E&O℠, Smart Cargo®, and a suite of products for Financial Institutions. Our digital platforms and tools enable efficient quoting and binding and proactive risk mitigation.

**Our mission:** To make the world a safer place by mitigating or eliminating adverse events. We do this by empowering carriers, brokers and policyholders to better predict and mitigate risk.

## Why Offer Corvus Smart Cyber Reinsurance?

Our White Label Reinsurance Solutions help manage the cost of your cyber program while further differentiating you with brokers and policyholders. What we provide:

- Coverage for all policyholders with no account-specific underwriting
- Experienced response team that improves quantitative and qualitative claim outcomes
- Proactive risk management tools to enhance value for and engagement with agents and policyholders
- White label alternatives that further differentiate your business
- A variety of coverage options to best suit the needs of each program
- Ongoing cyber threat monitoring throughout the policy period
- Prioritized recommendations for fixing key vulnerabilities (with Corvus experts available to assist)
- Risk management experts to enable policyholder preparation
- Security testing and awareness
- Fully bundled solution with no additional charge for Corvus services

## Table of Contents

# Corvus's Smart Cyber Reinsurance Coverage Options

## 3rd Party Coverages:

- **Network Security and Privacy Liability:** in the event the insured is sued for damages after a Security / Privacy breach, the policy will pay those damages and defense costs
- **Regulatory Investigations, Fines and Penalties:** if a government agency or regulatory authority finds that the insured is guilty of breaching a Privacy Regulation, the policy will pay for the Defense and the civil fines / monetary penalties/monetary amounts they are obligated to deposit into a fund as equitable relief due to the Security/Privacy breach. Media Liability: coverage if the insured is sued for damages by a third party due to the release/display of Media Material that results in things like defamation, slander, trade libel, infringement of trademark/copyright, etc.
- **PCI DSS Assessment Expenses:** if there is actual or alleged non-compliance with the Payment Card Industry Data Security Standards by the insured, the policy will pay the Defense costs and the costs, fines and penalties, fraud loss recoveries, etc. required by the Merchant Services Agreement.
- **Breach Management Expenses:** coverage when the insured has a legal obligation to notify individuals who are affected by a breach and they have to contractually indemnify a third party for those costs due to a breach

## Enhanced Buy-up Coverage:

- Automated quoting for buy-ups (up to $3M limits and $300M revenue for most classes of business)
- Up to $5M primary and excess limits, with broad industry appetite
- Streamlined online application process
- Selling tools to help quantify clients' cyber risk and sell coverage

## 1st Party Coverages:

- **Breach Response and Remediation Expenses:** The policy will pay the cost to the insured to hire forensic computer experts to figure out the scope of the breach, notification expenses to share with the affected individuals, legal expenses to determine legal duties and notification laws, costs to provide identity theft or credit monitoring, costs to host a breach hotline for customers, etc.
- **Social Engineering & Cyber Crime Coverage:** Coverage for theft of funds or financial fraud loss that the insured suffers as a result of a malicious actor duping them/impersonating an employee or client
- **Cyber Extortion and Ransomware Coverage:** The policy will cover the cost of the expenses incurred to avoid further disruption or failure to an insured computer systems and the ransom payment required by the malicious actor holding their data hostage
- **Digital Asset Destruction, Data Retrieval and System Restoration:** The policy will pay the expenses the insured incurs to restore, recreate or replace Digital Assets or Computer Systems that are directly impacted by a breach or administrative error
- **System Failure Coverage:** The lost revenue, extra expenses or data restoration expenses that the insured incurs as a result of an administrative error, computer crime, accidental physical damage, failure in power supply, electrostatic buildup, etc. will be paid by the policy
- **Reputational Loss Coverage:** business income loss that the insured suffers due to an Adverse Media event that occurs after a breach; covered by the policy
- **Business Interruption:** Coverage if the insured suffers a loss of revenue or extra expenses due to an interruption or outage of their system due to a breach

# Corvus Scan: How it Works

Our **non-invasive** scan examines your policyholders' externally-facing IT system looking for common risk factors like out-of-date software, risky open ports, and unpatched software. Corvus does not require access to servers, and does not require a password. We see the same information a malicious actor would when they are scanning the web for potential targets.

## The Corvus Scan provides actionable information for your policyholders.

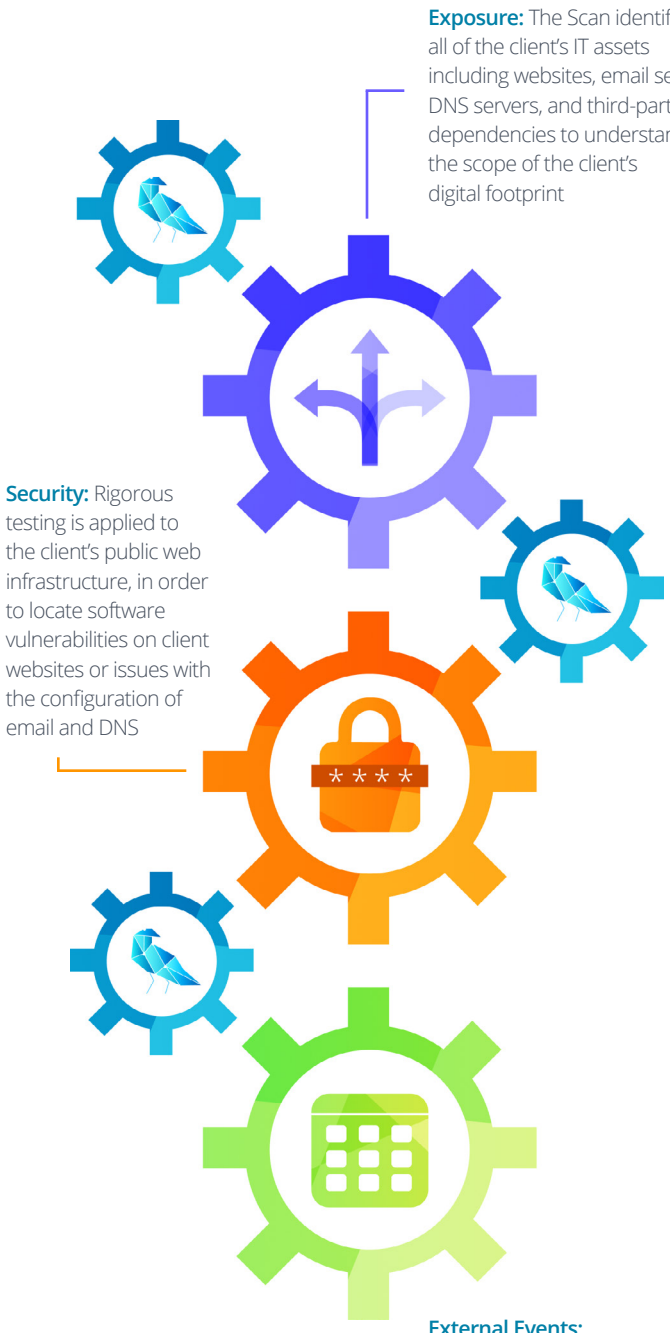
Our scan consists of three phases: discovery, testing, and recommendations. Once we've identified the scope of an organization's web-facing infrastructure, we perform tests to determine if software is patched, email is secure, and more. These measures provide insights on where security is lacking so we can offer recommendations to policyholders on how they can better protect their organization. The result? Actionable tips that can help prevent a cyber incident from occurring.

## A major value-add.

The Corvus Scan provides an in-depth report equivalent to costly offerings from third-party security companies. We understand that a review of this material with the client might be intimidating without command of the subject matter -- which is why we are here to support you. The Corvus Data Science team and our in-house cybersecurity experts are happy to provide a review of this material with your policyholders.

## Why Insurers Love Our Solution

- Fully reinsured, turn-key cyber solution that helps prevent cyber claims
- Identify critical vulnerabilities and help policyholders mitigate drivers of cyber loss
- Quarterly assessments of risk management results, combined with detailed claim experience, refine portfolio risk management strategy
- Access crucial insurance metrics, aggregate exposure data, and real-time updates about emerging threats with Corvus' data-powered Risk Aggregation Platform



# What You Need to Know About Cyber Liability

By 2025, cybercrime is estimated to cost businesses worldwide **$10.5 TRILLION** each year.

A ransomware attack occurs every **11 SECONDS**.

(Source: Cybersecurity Ventures / Cybersecurity Ventures)

## Frequently Asked Questions:

**Q:** My business is small and we don't have a lot of data; why do I need to spend money on Cyber Insurance?

**A:** Hackers don't discriminate when it comes to the size of your business. Malware takes many forms and attacks are blasted throughout large networks just to see who will take the bait. Some hacking groups even target smaller companies because they assume they do not have the same budget to spend on security protocols and training for their employees. According to Verizon's 2021 Data Breach Report, 61% of small businesses reported at least one cyber attack during the previous year.

**Q:** I don't store data on my systems, it is outsourced to a cloud or other third party service provider – aren't they liable for the data? Do I still need coverage?

**A:** Yes, you still need the coverage because you are still responsible for the care of that data. Legally, regulatory bodies hold the "data owner" responsible, not the "data holder" or "data processor." If a client entrusts their data to you, it does not matter who you outsource that data to on the back-end; you are still responsible for communication with the client and making them whole if something happens to their data. It is also your responsibility to pursue the outsourced provider if it was their fault - but this is where your cyber coverage can come into play and pay these costs upfront for you and subrogate on your behalf.

**Q:** I don't hold or process credit card data; do I still need coverage?

**A:** Absolutely. Any form of financial information, not just credit card information, can be manipulated, stolen, deleted, or sold on the dark web. Companies are still legally required in many cases to report, notify and remediate when other forms of data are exposed.

## Claim Scenarios:

- **A medical office was the victim of ransomware** carried out by a hacker who entered the organization's network through a patching vulnerability. The malicious software installed by the hacker encrypted personal health information on the system, including patient medical records. The hacker demanded a ransom payment of 5 bitcoin to unlock the data. After a digital forensics investigation was conducted and the threat was deemed credible, the ransom payment was paid.
- **A partner at a law firm had her laptop stolen from her car.** The unencrypted laptop contained more than 10,000 customer records that contained sensitive data, including social security numbers, medical records, and billing information. All individuals that were impacted had to be notified and were offered two years of identity monitoring expenses. A total of $105,000 was incurred.
- **Malware was remotely placed into a real estate agency's computer system** and all customer data was removed. As a result, the company incurred over $20,000 in forensics expenses and $240,000 in legal expenses.
- **Hackers placed malicious software on a local pizza shop's computer system.** The police in Marysville, Ohio started receiving an abnormal number of complaints about stolen credit card information. Due to a lack of cybersecurity infrastructure, threat actors were able to gain access to the shop's payment information.
- **An excavation and construction company noticed** their printers acting up one day in April 2021, and soon after, they found themselves locked out of their entire network. The ransom cost $100K, but they estimate that an extra $1 million in additional work is needed to recoup their $100K loss.

# Policyholder Benefits

## How Risk + Response Services makes your clients safer.

| Annual Scan Reports | Cybersecurity Alerts |
|---|---|
| Corvus Scan Reports are delivered annually, providing IT security analysis and actionable recommendations | If a critical vulnerability is discovered, Corvus generates a notification to help mitigate the threat |
| **Breach Response** | **Claims Handling** |
| In the event of a cyber incident, policy-holders get access to a breach coach to help navigate the incident and access to trusted vendors for critical response services | We're there with the policyholder throughout a transparent claims process led by our seasoned team of cyber claims specialists |

### Optional Add-Ons

**Cybersecurity recommendations**
Dig into all the details of the latest scan report on a call with a Corvus cyber expert

**Phishing test & discounted services**
Conduct a phishing test from KnowBe4, a leading provider

**Meet the breach coach**
Discuss breach response process and preparedness with a top privacy attorney

## vCISO Services

vCISO Services offers a suite of consultative sessions with the industry's top cybersecurity firms.

vCISO Services aims to help an organization dig deeper into specific issues and find the right offering to meet their needs. The process begins with a free, no-risk consultation call to explore options and find the best solution. Any further services selected are offered at an exclusive discounted rate.

With vCISO Services, organizations can explore their options, find the best provider to meet their needs, and strengthen their systems against cyber-attacks – **all cost-effectively and with the best vendors in the market.**

CORVUS

# About Corvus

Corvus Insurance is building a safer world through insurance products and digital tools that reduce risk, increase transparency, and improve resilience for policyholders and program partners. Our market-leading specialty insurance products are enabled by advanced data science and include Smart Cyber Insurance®, Smart Tech E&O™, Smart Cargo®, and a suite of products for Financial Institutions. Our digital platforms and tools enable efficient quoting and binding and proactive risk mitigation. Corvus Insurance offers insurance products in the US, Middle East, Europe, Canada, and Australia.

Current insurance program partners include AXIS Capital, Crum & Forster, Hudson Insurance Group, certain underwriters at Lloyd's of London, R&Q's Accredited, SiriusPoint, and Skyward Specialty Insurance. Corvus Insurance and Corvus London Markets are the marketing names used to refer to Corvus Insurance Agency, LLC and Corvus Agency Limited. Both entities are subsidiaries of Corvus Insurance Holdings, Inc. Corvus Insurance was founded in 2017 and is headquartered in Boston, Massachusetts with offices across the US and in London, UK. For more information, visit corvusinsurance.com.

**Sam Kramer**

Vice President, Reinsurance
skramer@corvusinsurance.com