Healthcare / Hospitals

Benefits of a Smart Cyber Insurance Policy

CORVUS BY TRAVELERS

1 The Big Picture

Healthcare is one of the most highly targeted industries for a number of reasons, among them the sensitivity of PHI (which provides added leverage for ransom if compromised) and the life-or-death stakes involved in the operations of some critical IT systems.

2 What's New?

+142%

According to Corvus Threat Intel, the frequency of ransomware attacks on healthcare entities increased 141.66% between Q1 2021 and Q1 2023. Ransomware rates against healthcare were 48% higher in Q2 2023 than any other quarter in the past two years.

3 The Risk Management Solution

Adequate cyber liability coverage and risk management practices are essential. Companies in the healthcare industry 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

Phishing Email Scam

An employee of a medical group opened a phishing email that infiltrated the company's centralized network, exposing a wide range of Protected Health Information (PHI), including medical record numbers, medication, dates of service and diagnoses of 1,200 patients.

A computer forensics investigator was hired, who determined that PHI had been compromised. The medical group notified the affected individuals and hired a public relations firm in anticipation of bad publicity.

Thereafter, the U.S. Department of Health and Human Services Office for Civil Rights launched an investigation and the medical group was fined as a result of a HIPAA violation for having unsecured access to the network.

Vendor Exposure

An assisted living facility outsources all its medical billing responsibilities to a third party. The medical billing vendor recently suffered a major data breach as hackers gained unauthorized access to its computer system.

After the vendor hired a computer forensics investigator it was determined that both Personally Identifiable Information (PII), including names, addresses and credit card payment information, and Protected Health Information (PHI), including medications and insurance information of 30,000 patients, had been accessed.

The assisted living facility was responsible for the data no matter where it was stored. As a result of this incident, the assisted living facility was obligated to pay for notification costs and credit monitoring services for all affected patients. It also had to pay fines, as it was in violation of HIPAA regulations, and the patients filed a class action lawsuit against the assisted living facility for allowing access to their PHI.

Lost Paper Records

It was discovered that 10,000 patient medical files from an ambulatory surgical center were left on a sidewalk as they were being moved from the center's location to a long-term storage facility. The files were left unattended and remained in plain view and accessible to the public for over 24 hours.

After a complaint was filed with the U.S. Department of Health and Human Services Office for Civil Rights, an investigation began.

As a result, the ambulatory surgical center agreed to settle potential violations of the HIPAA Privacy Rule. The ambulatory surgical center notified the affected individuals and adopted a corrective action plan to address deficiencies in its HIPAA compliance program. The ambulatory surgical center also hired a public relations firm in anticipation of negative publicity after the local news picked up the story.

Smart Cyber and Cyber Excess Policy Highlights

Coverage for Ransomware Remediation

When a business suffers a ransomware attack, cybercriminals typically encrypt/ threaten to delete company data. Cyber coverage can respond to ransom costs incurred to end the threat or unencrypt data.

Coverage for Privacy Laws & Fines/Penalties

There is a nationwide patchwork of privacy laws in effect across industries, and a healthcare professional's failure to comply can lead to significant fines or penalties from state or federal agencies. Cyber coverage can respond to the defense and payment of regulatory fines or penalties.

Risk Prevention Services

Through tailored threat alerts and partnership with in-house cyber experts, we're here to help policyholders reduce the likelihood of a cyber attack at their organization — and at no additional cost beyond their policy premium.

In-house Claims Handling

When a security breach happens, every minute matters. Our in-house incident response and claims teams are available through the entire breach response process — before, during, and after an incident.

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	$2m
$50m - $200m	$4m
$200m - $300m	$5m
$300m+	$5m

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

About Corvus

Corvus Insurance, a wholly owned subsidiary of The Travelers Companies, Inc., 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® and Smart Tech E+O®.

Brian Alva
Senior Vice President
Cyber TEO Underwriting

09/24/24