CORVUS BY TRAVELERS

RISK PREVENTION CASE STUDY

Wealth Management Firm

Company Information
Wealth management firm with $500M in annual revenue

Incident Type
Security breach via compromised VPN credentials

Response time
Within 30 minutes

Actions Taken
Rapid alert of breach with expert security guidance

Results
No customer data loss, minimal interruption to operations; $250,000+ ransomware claim avoided

Additional Benefits
MFA implemented on VPN accounts to boost security

Overview

A wealth management firm generating $500M in annual revenue across multiple business units faced a significant threat when a potential ransomware situation emerged. Their ongoing collaboration with the Corvus Risk Advisory Team equipped them with the necessary tools and strategies to effectively manage the crisis.

Challenge

Corvus received an urgent alert from one of its threat intel sources. A threat actor had compromised a VPN associated with the firm and was selling access to other criminals on the dark web. The firm needed to act quickly to prevent a potential ransomware attack.

Response

The Corvus team immediately sprang into action, alerting the insured within minutes by email. A dedicated Corvus cyber expert quickly reached out by phone to both the policyholder and their broker. During the call, they assisted the firm in:

- ✓ **Revoking Access:** The compromised VPN account was disabled to prevent further unauthorized access.
- ✓ **Investigation:** The firm took the VPN offline for investigation, and discovered that the threat actor had gained access through a payroll account with a weak password after trying various combinations in a “brute-force” attack.
- ✓ **Enhancing Security:** The Corvus expert guided them in implementing Multi-Factor Authentication (MFA) on their VPN accounts to bolster security against future breaches.

Results

Once a threat actor sells access, a ransomware group is likely to strike within days. Thanks to the swift actions taken by the Corvus Risk Advisory team, the firm successfully mitigated an incident that could have escalated into a $250,000+ ransomware claim, but instead was contained to just a $3,000 expense.

The timely intervention not only prevented a potential crisis but also ensured that business operations continued with minimal downtime. No customer data was lost, so no reporting requirements were triggered that could have led to reputational harm. The incident underscored the importance of continuous risk management and the value of preparedness in the face of evolving cyber threats.