CASE STUDY

Asset management firm pays ransom to protect partner's client data

INDUSTRY

Financial Services

EMPLOYEES

<50

COVERAGES

- Cyber Extortion
- Breach Response

An asset management firm was hit by ransomware and followed all the appropriate steps to remediate the incident. They immediately contacted Coalition[1], and we arranged breach counsel and a forensics investigation[2] with one of our panel vendors to handle the restoration. Although the threat actor was demanding $1.5M, the firm had viable data backups and wanted to avoid paying the ransom.

After restoring their data from backups, the firm quickly resumed operations. However, they received an email from a bank they partner with to secure loans. The bank had seen the firm's name on the dark web, knew the firm had been compromised, and was concerned about its own client data leaking.

Typically, Coalition does not recommend paying a ransom to a threat actor once a business has resumed operations, but we recognized the potential negative business impact if the data was published on the dark web. With that in mind, we entered into negotiations with the threat actor and agreed upon $200,000 — an 87% reduction from the initial demand. Once we received confirmation the threat actor deleted the exfiltrated data, the firm's Cyber Extortion coverage kicked in to cover the ransom payment.

Coalition brings together active monitoring, incident response, and comprehensive cyber insurance designed to help mitigate your organization's cyber risk. To learn more, visit coalitioninc.com.

[1] The claim scenarios described here are intended to show the types of situations that may result in claims. These scenarios should not be compared to any other claim. Whether or to what extent a particular loss is covered depends on the facts and circumstances of the loss, the terms and conditions of the policy as issued and applicable law.

[2] Breach response included the engagement of an incident response firm; the insured selected one of our preferred panel vendors.