CASE STUDY

Technology Company Unable to Operate for Weeks Following Ransomware Attack

INDUSTRY
Technology

EVENT TYPE
Ransomware

REVENUE
$50-100M

EMPLOYEE COUNT
1,000+

LOCATION
New York

KEY COVERAGE
Cyber Extortion
Business Interruption
Breach Response
Crisis Management

Having prior knowledge of all mission-critical data, networks, and assets is essential to responding to a cyber event and resuming operations.

A transcription service company experienced a ransomware attack that rendered their business inoperable. The company wasted no time and immediately contacted Coalition to file a claim, selecting Coalition Incident Response(CIR) to respond to the incident.

Due to the nature of its business and clientele, the company was eager to engage with the threat actor and pursue the most expedient recovery option available, in hopes of minimizing downtime. With support from CIR, our claims team cautioned the company against immediately opting to pay a ransom. Instead, we sought to explore all recovery options, including any available data backups.

Having been impacted by the ransomware, the backups were deemed unusable. However, the company was able to create a workaround to recover its data — the problem was that the recovery process would take at least one week. Upon careful consideration, all parties agreed to engage in negotiations with the threat actor.

The threat actor initially demanded $2.5 million, but CIR successfully negotiated it down to $1 million. After a thorough investigation, CIR was unable to identify a phishing email or any unauthorized entry, though sensitive data was compromised as a result of the incident.

Here's how the company's coverage responded: Cyber Extortion covered the cost of the ransom payment. Business Interruption covered lost revenue while the business was inoperable. Breach Response covered the cost of legal fees, CIR fees, and data mining. Crisis Management coverage covered the costs of a public relations firm to communicate with third-party vendors and customers. After the technology company paid its $100,000 retention, its policy covered more than $1 million in costs related to this claim.

Lesson Learned: Identify Essential Data and Systems Prior to a Cyber Event

Maintaining viable data backups is a proven strategy for recovering from a ransomware event, but backups can still be damaged during an attack. This is why Coalition encourages all businesses to prepare an incident response plan that documents how to respond during an incident. Having prior knowledge of all mission-critical data, networks, and assets is essential to responding to a cyber event and resuming operations.

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] *Coalition Incident Response services provided through Coalition's affiliate are offered to policyholders as an option via our incident response firm panel.*

[2] *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.*