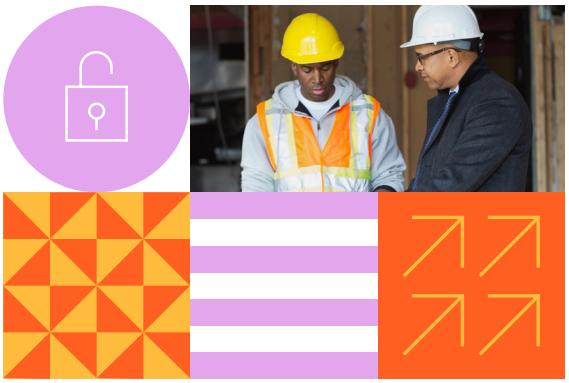
CASE STUDY

High-Profile Client Requires Strict Protocol Following Data Exfiltration



INDUSTRY
Construction

EVENT TYPE
Ransomware

REVENUE
$100M+

EMPLOYEE COUNT
1-25

LOCATION
Texas

KEY COVERAGE
Breach Response

The day started like any other for a southwestern construction company. But when the IT director discovered its systems were inaccessible and files were encrypted, the business was confronted with the unimaginable: ransomware.

Forensic investigation determined the threat actor compromised a virtual private network used to facilitate remote access. Fortunately, the business had backups of its essential data and worked through the night to successfully restore systems in enough time for employees to resume work with minimal impact. Because the backups were deemed viable and unaffected by the ransomware, we advised the construction company that there was no need to pay the ransom for a decryption key. Instead, one of our forensic vendor partners installed an Endpoint Detection and Response (EDR) solution to monitor the systems and prevent reinfection.

An investigation revealed the threat actor exfiltrated more than 60,000 documents, which needed to be manually reviewed to determine if they contained protected information. Due to one high-profile client, the U.S. Department of Defense (DOD), the company had to follow stringent protocol and file a notification directly with the DOD. The company was also required to work with highly specialized counsel to protect the confidentiality of controlled unclassified information.

After the company examined the exfiltrated data, breach counsel helped the company notify and set up credit monitoring for an estimated 850 current and previous employees who were impacted by the data breach — and one key coverage helped immensely. Breach Response[1] covered numerous costs related to incident response, breach notification, and credit monitoring, including $43,000 for data mining. Overall, the construction company paid $5,000 to cover its self-insured retention, while its policy covered the remaining $106,000.

Threat actors are increasingly opting to simultaneously exfiltrate data, transfer it to their external servers, and threaten its release if the ransom is not paid.

Lesson Learned: Create a Detailed Incident Response Plan

Ransomware attacks often involve encrypting or deleting data stored on a business network. However, threat actors are increasingly opting to simultaneously exfiltrate data, transfer it to their external servers, and threaten its release if the ransom is not paid. A well-documented incident response plan in place before an incident occurs is essential and must include specific steps for dealing with data breaches and cybersecurity controls designed to reduce the likelihood and impact of a breach.

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.*