CASE STUDY

CEO's Business Email Compromise Leads to Leak of Customer Data

INDUSTRY
Real Estate

EVENT TYPE
Data Breach

REVENUE
$10-50M

EMPLOYEE COUNT
51-250

LOCATION
Texas

KEY COVERAGE
Breach Response
Business Interruption

Businesses are encouraged to have employees shut down nonessential internet-connected devices and also perform updates before leaving for extended periods of time.

A real estate company was embroiled in a cyber standoff just a few days before Christmas. A threat actor had gained access to the CEO's email account and numerous other applications. After resetting the passwords and enabling multi-factor authentication, the threat actor began sending the CEO threatening messages and demanded payment in exchange for returning the accounts. The company worked with its regular attorney to communicate with the threat actor initially before contacting Coalition a few days later.

The company was connected with breach counsel and selected Coalition Incident Response[1] (CIR) to investigate the cyber attack. CIR discovered a breach stemming from the CEO's email account that enabled the threat actor to move laterally through the real estate company's digital environment. We sourced a data mining company to determine the extent of the breach and identify which documents or systems were impacted.

Meanwhile, CIR worked to regain control of the accounts and expel the threat actor from the company's network. Because personally identifiable information had been accessed, the company needed to notify impacted individuals, so we lined up a vendor to help with notifications and credit monitoring for those affected. By working with its own attorney before contacting Coalition, the company failed to obtain the written consent required to work with outside forensics or breach coaches. However, the company reasoned that it was an extra expense incurred in order to reduce impacts to their systems and regain access to their accounts. Ultimately, we agreed to cover the attorney's fees.

Here's how other coverages came into play: Breach Response[2] covered the costs for breach counsel, CIR's forensics investigation, data mining, notifications, and credit monitoring. Business Interruption covered the cost of the initial attorney. After meeting its $1,000 self-insured retention, the real estate company's policy covered $93,000 of costs associated with its data breach.

Lesson Learned: Exercise Security Diligence When Partnering with Third-Party Vendors

Threat actors are highly aware of holidays and other events that cause businesses to lower their guards, even for just a few moments. To help protect against seasonal attacks, businesses are encouraged to have employees shut down nonessential internet-connected devices and also perform updates before leaving for extended periods of time.

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.*