CRESTVIEW PUBLIC ADJUSTERS

CASE STUDY:
TELECOMMUNICATIONS COMPANY GETS HACKED

CRESTVIEW PUBLIC ADJUSTERS

CLAIM

A telecommunications firm encountered a malware attack that impacted both their software and hardware systems. Within the company's network, a malicious code was deployed.

HURDLES

One of the challenges they faced involved determining the extent of financial losses incurred by the client in future government contracts. This setback nearly pushed them to the brink of going out of business and jeopardized their prospects for securing future contracts due to the impact of the malicious malware. Fortunately, they had the safeguard of cyber insurance coverage. Another obstacle was ascertaining which aspects of their coverage were applicable to the incurred losses. As they had reached out about a year and a half into the claims process, they found themselves in a situation where they had been offered no compensation and were uncertain about the subsequent actions and available options.

STRATEGY

Crestview's cyber operations team and forensic accountant swiftly initiated their involvement in the case. They began by collaborating with the insurance provider and various vendors. Our approach centered on a comprehensive review of the financial records and insurance policy, with the objective of pinpointing the root cause of the loss, determining the specific provisions of the policy that were relevant to this particular loss, and identifying the extent of coverage. After dedicating a substantial amount of time to this analysis, we presented our conclusions and findings to the insurance company.

OUTCOME

We achieved a successful recovery of funds for both data recovery and reputation harm, categories for which the insurance initially provided no compensation. We managed to secure a substantial $50,000 recovery, marking a significant 200% improvement from the initial offer of $0.