

CASE STUDY

Coalition negotiates 75% reduction in ransom cost after files and backups are encrypted



INDUSTRY

Healthcare

EMPLOYEES

100

COVERAGES

- Extortion
- Breach response
- Digital asset restoration

If this ever happens to your business — don't answer the phone. Don't pick up calls from unknown numbers. It simply starts the clock. After you've engaged, there is no turning back.

After more than 30 years in business, a medical practice management company started their day like any other before their IT team realized they couldn't get into their system. IT logged in, and all files were encrypted with the dreaded .crypted file extension. Unfortunately, their backup data was also compromised, a concerning development given the large amount of Protected Health Information (PHI) and billing information they store. The policyholder had been hit with HelloKitty malware, a dangerous new ransomware variant known to exfiltrate its victims' data before encrypting it.

The policyholder contacted Coalition immediately, we assessed their environment and prepared to start communications with the threat actor. It was important to get in touch with the attacker because the victim's phone had been ringing off the hook — at least seven times within the first 24 hours. We asked the policyholder to stop communicating with the threat actors and helped assess their backups.

With their backups fully encrypted, and absent any other options to restore their operations, the company made the difficult decision to pay the ransom in order to restore their operations. Fortunately, CIR was able to negotiate the ransom demand down by nearly 75% from \$750,000 to \$200,000 and proceeded to help the company restore all of their data. The costs to respond to the incident, to recover lost data, and to pay the extortion, together with the lost income resulting from the incident, were covered by the company's cyber insurance policy with Coalition.

Coalition brings together active monitoring, incident response, and comprehensive insurance to solve cyber risk. To learn more, visit coalitioninc.com.