What to do after you discover a cyber incident

Scenario

An employee clicked on a malicious email link. The email originated from a threat actor and clicking on the link installed malware into the organization's network and encrypted data and files.

A message has now appeared on the employee's computer demanding that $100,000 be paid in Bitcoin within 48 hours to regain access to the company's data and files, otherwise, the threat actor will publish the sensitive data on the internet.

Next Steps

Report to Cowbell at (833)-633-8666 or email claims@cowbellcyber.ai

Immediately report the incident to Cowbell and your broker. You should never try to resolve the issue on your own; do not engage with the threat actor. We are available 24-7, 365 days a year. An incident response team will be immediately deployed to address the cyber incident.

Prepare for a scoping call

To the extent possible, please create a brief summary of what systems or data may be impacted. Have the organization's leadership on standby to attend a scoping call with Cowbell's incident response experts.

Our Claims Process

Report: As soon as a claim is filed, our cyber claims specialists will swiftly deploy appropriate incident response teams to immediately assist.
Review: A policy review and coverage investigation is conducted and the policyholder is informed of the resources available.
Respond: Cowbell's incident response team includes breach counsel, digital forensic and incident response investigators, professional ransom negotiators, public relations, and others. These teams have been vetted for expertise and efficiency and will address the incident to minimize the impact to your organization.