Case Study:
Incident Response

Client Profile

Business: Commercial Printing

Size: 175 Employees

Industry: Manufacturing

Compliance: NIST 800-171

Key Metrics

Data speaks louder than words, so we selected a few points of interest to help tell the story:

12

Members of our IR team engaged to contain and remediate the event

$10 mil+

In estimated costs averted from ransom payouts, business downtime, and reputation damage.

CHALLENGES

A mid-sized commercial printing firm experienced a cyberattack and was surprised to learn that their cyber liability insurance provider was not open on weekends, so they were unavailable to help. With no immediate support available, they turned to us for expert guidance and assistance in managing the event.

SOLUTIONS

Our response was immediate and we were able to work closely with the client's managed detection and response (MDR) provider to isolate the compromised devices. Our IR team then began to analyze logs and investigate the event to ensure there were no other traces of hacker activity. Once we determined that the threat was fully contained, the client engaged us to provide technical remediation services to help them rebuild certain services and bring network operations back online. This incident underscored the importance of having an IR retainer in place before a crisis occurs, as the lack of one can lead to significant delays when unexpected cyber events strike.

RESULTS

1

Rapid Containment & Recovery

With immediate access to an expert team, the attack was isolated, which minimized downtime and prevented further damage. Without a retainer in place, the incident could have escalated, leading to prolonged disruption and higher costs.

2

Access to Technical Remediation Skills

Our team's technical remediation expertise enabled us to rebuild critical systems and restore the client's network operations efficiently, minimizing recovery delays and business disruption.

3

C-Level Engagement

Observing the effectiveness of an incident response retainer led C-level leadership to recognize the importance of proactive cybersecurity measures. Without a retainer in place, the consequences could have been significantly more severe.