CASE STUDY

Inside Job

Investigating an internal data breach

CAPITOL DIGITAL & Californsics

Client
Large Corporation

Service
Incident Response

The Situation
Our client, an industry-leading manufacturer of fuel cells, was involved in a large lawsuit related to the termination of an employee. The client believed an accomplice in IT, who had previously received advanced technical training in the military, was helping the ex-employee steal data from the company.

The Challenge
Confidential information only known to certain senior executives had inexplicably appeared in communications from opposing counsel, leading the client to suspect their network had been compromised. The CEO had emailed the leaked data internally, suggesting that the company email system had been one target of the suspected breach.

The Solution
Our Incident Response team analyzed the client's file and mail servers and several months of activity logs. We discovered that an outside user had made multiple attempts to access data on each server. This user had successfully accessed one of the file servers and the mail server, using credentials that we determined had been created by the IT accomplice. These credentials were used for access after this IT employee had been terminated. Furthermore, the same IP address had accessed the CEO's email account over a period of six months.

The Outcome
After discovering the unauthorized access to the client's file server and the CEO's email account, we assisted the client in securing the vulnerabilities in their network. Due to the sensitivity of the client's products, the data and our report were delivered to Homeland Security and other law enforcement agencies for further investigation.

Key Success

Rapidly determined the method, intent, and suspected perpetrator of the network breach.

555 Capitol Mall, Suite 235 ▪ Sacramento, CA 95814 ▪ 916.449.2820 ▪ www.Capitol-Digital.com