

Committee for Public Counsel Services

Incident Response Case Study

Situation

The **Committee for Public Counsel Services (CPCS)** is a public agency with a mission to provide legal services for clients unable to afford to retain a lawyer funded by the Commonwealth of Massachusetts. The CPCS acts in a manner similar to a private law firm, employing 450 attorneys and approximately 3000 outside contracting attorneys (who were never directly affected) whose activities are coordinated by CPCS staff. The organization has more than 20 offices across Massachusetts and approximately 700 employees in total.

Challenge

Vancord was introduced initially to CPCS during a cybersecurity emergency involving **ransomware across hundreds of workstations and servers**. CPCS responded unsuccessfully to the attack with internal resources and engaged Vancord through a referral from an existing IT provider. The situation was dire, normal business was suspended, email and communications were impacted, and its organizational reputation, and funding, were at risk.

The following immediate action steps were needed:

- Restore control of servers, which had been compromised
- Restore data which had been encrypted
- Regain access to email communications
- Assure external business parties that the threat had been eliminated
- Hardening of systems to prevent attack recurrence

Approach

Every incident response engagement requires a unique approach to contain attacks and restore systems. Vancord developed **an approach customized to the threat encountered**, using data analysis and triage to adapt on the fly to customer systems and requirements. Vancord deployed a team of three engineers on a full-time basis to investigate the threat, contain attackers to prevent further spread and damage, eradicate malware and attacker tools, and recover systems for normal business operation.

Vancord Services Provided:

Advice and consultation regarding incident strategy and interpretation, forensic analysis of systems, event data and network traffic, ongoing triage and threat hunting, log monitoring, event analysis, and alerting, reverse engineering of malware samples, creation of procedures for hardening and restoration, assistance in restoring key systems, and support in crafting public communications.

Solution

For the duration of the engagement, Vancord used Infocyte for threat **hunting** and analysis, Elastic for security event monitoring, and multiple **custom tools created by Vancord staff**. These products were efficiency aids, procured in advance by Vancord for use during incident response rather than for future customer use.

Soon after Vancord was engaged the attackers were contained and isolated. Vancord successfully stopped the attack and worked with CPCS to resume largely normal operations over the next two weeks. Employee productivity, previously halted due to the attack, resumed rapidly when email became available, when file server data was restored, and as workstations were cleaned/redeployed. Post-incident corrective actions and improvements were made as a necessary element of containment, eradication, or restoration.

Throughout the process, Vancord was able to improve CPCS systems, including stability of internal email systems and the security posture of many core servers. A chief outcome of the incident, after resolution, was the **delivery of an incident report** that documented specific findings and areas of opportunity for the improvement of internal security. CPCS gained a key partner in information security, establishing a relationship, which will continue long after the incident.

Several follow-up projects as a result of this strong partnership have included a vulnerability assessment, virtual Information Security Office, application penetration test, firewall upgrades, security operations center, and an endpoint protection initiative.

Let's Talk

Discover how Vancord can help protect your business from ransomware attacks.



Locations

500 Boston Post Rd | Milford, CT 06460 | HQ
180 Glastonbury Blvd | Suite 107 | Glastonbury, CT 06033

Get In Touch

Sales@Vancord.com | 855.512.4817
Vancord.com