Case Study

Surviving a Ransomware Attack

Client:

Commercial Uniform and Services Company

The client is a leading provider of corporate uniforms and services—including mats, mops, cleaning and restroom supplies, first aid and safety products, fire extinguishers and safety courses—to over one (1) million businesses throughout the United States.

Challenge	CBTS Solutions	Results
• The client's virtual desktop environment suffered a ransomware attack leaving office employees unable to collaborate and work. • Client needed additional IT resources to get the network back online quickly.	• An assessment of the damage from the ransomware attack was completed and a strategy was formulated to get their virtual desktop back online as quickly as possible with the updates needed to prevent any future attacks. • Virtual Server Environment (VMware) – the client's entire server environment was rebuilt with state-of-the-art VMware servers. • Database Servers – the client's database servers were replaced and restored from backup files.	• The client was able to get their virtual desktop network back online within three months after the ransomware attack. • New network has been modernized with an increased level of security.

Business Challenge

As a result of a major ransomware attack, the company was advised by their third-party security and network hosting providers to shut down their virtual desktop network environment, close all inbound and outbound email traffic, and send all office employees home.

However, they soon realized getting their network back open would take weeks, if not months, with their current IT staffing level, and in the meantime their IT infrastructure was not set up to support a work-from-home environment.

The company began putting together a plan to not only get their network back online as quickly as possible, but also rebuild it to accommodate a work-from-home environment with the highest level of security.

CBTS Solution

The client engaged CBTS within 24 hours of the attack to obtain the necessary skilled IT resources to assist their IT organization with the recovery. Several teams of CBTS IT experts were deployed over three different shifts to ensure 24-hour operational support in the following areas:

Virtual Server Environment (VMware)

- CBTS network architects were deployed to help determine how to quickly get their virtual environment online.
- CBTS system engineers were deployed to rebuild the company's state-of-the-art VMware server environment.

Database Servers

- CBTS database administrators were deployed to rebuild all servers and data from backups, as well as implement testing of all applications and functionality.

Results

The client was able to get their virtual desktop network back online within three months of the ransomware attack. Their new network has been rebuilt and modernized with the security needed to address an increasing level of ransomware threats.