> *Having the Carbonite solution led to a huge savings, and we were so happy that we had such good backup.*
>
> **Lisa Travis, Director of IT, Town of Colonie**

Fast Facts

Name
Town of Colonie

Employees
600+

Residents
85,000+

Industry
Municipal Government

Technology Environment
25 servers; three main locations in town with 15 remote locations

Carbonite Solutions
Deployed: Carbonite® Server with appliances

Carbonite® Server provides data recovery in ransomware attack

Town of Colonie avoids more than $400,000 in ransom due to appliances and backup

Background

The stories of ransomware attacks have unfortunately become more common, especially among municipalities. But, when the Town of Colonie, in the greater Albany, NY region, became the latest to fall prey to a ransomware attempt, the outcome was different than many others thanks to protection from Carbonite.

Solution

The day – January 15, 2020 – is one that will always be remembered by the six employees in the IT department of the town of Colonie. At around 3 p.m. a few employees received emails that appeared to be from other employees but were in fact a phishing attempt. The IT Department deleted the emails, and reformatted the users' hard drives. At around 6 p.m., security alerts began notifying the team that something was amiss. Troubleshooting efforts led them to analyze one of their servers that couldn't be accessed.

After a check of other servers found the same issues, they realized they had been the victim of a ransomware attack with the attackers demanding more than $400,000 to decrypt the files and applications.

The team immediately checked the three Carbonite® Server appliances stored at offsite locations and found they had not been affected. They immediately disconnected them from the network to eliminate any further potential infection. Following a two-day forensic investigation by the New York State Homeland Security and FBI, they began the process of recovery.

"We've never had anything like this happen. Since we've had the Carbonite solution, we've done some smaller restores but nothing of this caliber. We've not had to put it to the test until this," said Lisa Travis, Director of IT.

It took several weeks to restore the data and reconfigure each application server for the town but only one data file was lost. Critical to their effort was the engagement they received from the Carbonite support and engineering teams as well as the ability to restore the data in a separate environment outside of the compromised network. Most important to the recovery was the original setup recommendations made by Carbonite engineers, which ended up being the key to their appliances not being compromised.

"I'm so appreciative of the instruction I received from the Carbonite engineers three years ago when we first installed the appliances," said Jimmy Onibokun, Network Administrator. "My first instinct was to join the appliance to our domain network, which would have exposed us in this incident, but we were discouraged from doing so. This, along with having more hardened appliances and different credentials, all of which were recommendations from the Carbonite team, gave us the outcome we needed."

"The Carbonite support people and engineers were excellent, very helpful, knowledgeable and available whenever we needed," said Travis. "All the different dependencies are what saved us – we were configured correctly, we were working with qualified engineers, and we had the right components in place. All those components are critical and important when you're in an emergency."

In retrospect, the team knows they need to invest in a bare metal solution, which they're working to acquire now. They have also improved their endpoint antivirus. But having Carbonite® Server helped them avoid a much bigger disaster than what could have occurred, allowing them to continue to pay their employees and, most important, support the critical public safety systems.

"Recovering from this was a lot of work. It cost the town money in staff overtime but nowhere near the $400,000 it would have cost us. Having the Carbonite solution led to a huge savings, and we were so happy that we had such good backup."

Lisa Travis, Director of IT, Town of Colonie

About Carbonite and Webroot

Carbonite and Webroot, OpenText companies, harness the cloud and artificial intelligence to provide comprehensive cyber resilience solutions for businesses, individuals, and managed service providers. Cyber resilience means being able to stay up and running, even in the face of cyberattacks and data loss. That's why we've combined forces to provide endpoint protection, network protection, security awareness training, and data backup and disaster recovery solutions, as well as threat intelligence services used by market leading technology providers worldwide. Leveraging the power of machine learning to protect millions of businesses and individuals, we secure the connected world. Carbonite and Webroot operate globally across North America, Europe, Australia, and Asia. Discover cyber resilience at carbonite.com and webroot.com.