# Michigan County's Ransomware Recovery Plan Minimizes Impact of Network Attacks

Jessica Renee Napier | March 29, 2017

As hackers, virus writers and cybercriminals become more creative about how to disguise and plant malware, it is becoming increasingly crucial for government and industry to adopt precautions against ransomware attacks. In 2016, the Federal Bureau of Investigation recorded $2.9 million in losses as a result of cyberscamming.

And while the monetary loses are quantifiable, there also are the losses of time, data and inconvenience — all of which are more challenging to measure.

Take Michigan's Livingston County, one of many counties experiencing ransomware attacks that, on occasion, left its employees unable to tend to daily business. The local government organization receives more than 25,000 port scans per week of criminals doing reconnaissance work on the network and several thousand malware attacks per day.

The majority of ransomware attacks enter via email, luring employees to click on a link or execute a file. One of the county’s major ransomware attacks was the result of malvertising on a trusted local news website. One employee unknowingly executed the ransomware attack onto the county’s system. The result: PCs and mapped network drives were encrypted and rendered unusable, and the organization lost access to a legacy assessing and property tax system.

“It is really a productivity killer for a target area that was affected,” said county CIO Richard Malewicz.

Thanks to Livingston County's ransomware recovery plan and backup and recovery solution, however, the experience wasn't too dire; the county was able to revert back to the pre-ransomware event data and resume business as usual without any significant downtime or business impact from the attack.

At the beginning of 2016, the county began working with Unitrends, a technology solution provider for backup and disaster recovery solutions. Paul Brady, CEO of Unitrends, said that the county’s officials desired a solution that incorporated protection and recovery.

“That part was simple,” Brandy said, “but the threats they and other organizations faced were more complex than what the capabilities of your standard backup and recovery solution could handle. They needed a hardened solution that could prove reliability if a threat was encountered in the environment.”

Unitrends delivered a hardened system for storing backups within all components of the environment — backup hardware, software, replication and cloud storage —– covered under a single support call to Unitrends.

“Unitrends lives in a world where IT pros would rather not have to think much about us,” Brady said. “And we try to help them achieve that.”

Malewicz said that the Unitrends Ransomware Detection feature allows the county to predictively analyze and detect abnormal data change explosions within the backed-up data that are indicative of ransomware infections. This solution also allows the county to test its backup data, ensuring that in the event it does experience another attack or loses its data, the county officials have the reassurance of knowing that the data in the past is reliable.

“That has been an issue with other providers,” Malewicz said. “When you go back and think you have a data backup — only to find out it's corrupted in some way, making it unusable. It’s a huge time saver and gives us peace of mind.”

Malewicz, who said not all backup solutions are created equal, made the following recommendations for other county officials in the research phase. Make sure to invest in a solution from a proven and industry respected vendor that:

- tests and validates the integrity of the data each time is backed up;
- predictively analyzes and detects abnormal data change explosions within the backed-up data;
- uses a Linux system; and
- uses a deduplication hash cryptographic secure hash algorithm from the SHA-2 family.

“We measure success by the peace of mind to mitigate ransomware attacks,” Malewicz said, “and know that all of our data backup has good integrity should an event occur.”

http://www.govtech.com/security/Michigan-Countys-Ransomware-Recovery-Plan-Minimizes-Impact-of-Network-Attacks.html