White Paper

New Tools Help State and Local Governments Battle Ransomware, Other Big Disasters

In recent years, ransomware attacks have immobilized many cities and towns across the U.S., from major metro areas, such as Atlanta, Baltimore and New Orleans, to relatively tiny towns.

Increasingly, state and local governments find themselves targeted by malicious cyberattackers who sneak into their information technology systems, encrypt critical data and other files, and then demand millions in ransom payments to restore access. When governments find themselves being ransomed, their choices are typically to pay, which will undercut their ability to deliver key services to their communities due to budget restrictions, or not pay, resulting in the immediate inability to serve their communities and the loss of key data that will inevitably plague them for years afterwards.

In 2016, Sarasota, Florida, a city of about 55,000 people along the Gulf Coast, was one of those targets. A city employee had clicked a phishing link disguised in an email and soon enough malware spread through the city's servers, locking down important files. The attackers demanded $34 million in the cryptocurrency Bitcoin to unlock them.

But Sarasota city officials didn't cut a check.

Just a few months before, the city's IT administrator implemented Veeam Backup and Replication, a software solution that helps organizations of all sizes back up critical data as per their disaster recovery plans. Working through the night, the Sarasota IT team was able to restore their systems, relying on backup copies of the city's critical data. By the next day, services had been fully restored.

"They were in a position to ignore the ransom demand and just restore that data into a known good, uninfected state. And that was a huge benefit for them," says Veeam's Senior Director of Enterprise Strategy Jeff Reichard.

Veeam is an industry leader in the field of backup and recovery software. The latest version of its Veeam Availability Suite platform — v10 — was released in February 2020 and comes enhanced with next-generation data-protection capabilities designed to help organizations recover critical workloads, whether they're in the cloud, virtual or physical and regardless of their location. Chief among its capabilities: what the company calls "100% bulletproof ransomware protection."

By design, the v10 platform is meant to be easy to use.

Because Veeam Availability Suite is a software-only solution, it can be deployed on an agency's existing infrastructure — or whatever compute and storage resources are available at the moment of crisis.

"What you hear from customers constantly is: 'It just works,'" Reichard says. "What customers really appreciate is that it's simple and that it saves them without them having to invest huge amounts of time. You can set it up and get it running quickly; and it actually does what it's supposed to in a super-reliable way."

When Veeam and Sarasota city officials first began their partnership, the city had been struggling with a clunky and unreliable legacy backup tool. Once IT staffers downloaded a free trial version of Veeam, they were backing up critical data within an hour.

"They didn't have to pay for weeks of consulting, training, or deployment services, nor bang their heads against it for a week to get it running," Reichard says.

205,000

The number of organizations that were hit by ransomware attacks in 2019 — an increase of 41% from the year before.

Source: "Ransomware Attacks Grow, Crippling Cities and Businesses," The New York Times, 2019.

Prime Targets

Disaster recovery has long been a key concern for state and local government. Major natural disasters, such as hurricanes and floods, can knock offline critical services, leaving citizens in the dark — sometimes literally — and hamstringing local authorities' ability to coordinate vital response efforts.

But the ransomware threat to state and local governments represents a unique challenge — and the threat is growing.

In 2019, over 205,000 organizations were hit by ransomware attacks — an increase of 41% from the year before, according to research published in The New York Times. Along with state and local governments, many of those targeted in recent years have been schools and health care organizations.

State and local governments have become prime targets for ransomware attacks for a few key reasons.

First, the fact that local governments are tasked with carrying out important, often urgent, functions leads some cyber hijackers to think they'll be more likely to fork over cash in a crisis. "Their services are critical — literally life and death in the case of things like emergency response, health care coordination, police and fire," Reichard says.

In addition, the budgets for state and local governments are still recovering from the fiscal belt-tightening following the 2008 financial crisis, meaning they often struggle with the financial and technical burden of robust disaster recovery planning or backups.

State and local governments can also be easy targets for cyberattackers because their IT infrastructure is often distributed. "When you've got disparate, separately managed systems that are connected, what you have is a security nightmare," Reichard says. "There's going to be a vulnerability somewhere. And once somebody gets into one of them, because they're connected, they can spread through other ones."

Finally, and unfortunately, the ongoing response to the coronavirus pandemic, which is spurring massive changes in the way local governments operate, could also up the risk. "As governments at all levels are sending employees home, the employees' home-compute infrastructure is going to be part of the attack surface for bad actors in a way that it has not been in the past," Reichard predicts.

The 3-2-1-1 Rule

Disaster recovery planning is designed to help organizations get back on their feet when the worst-case scenario hits their doorsteps.

A rule of thumb when it comes to planning your backup process is to remember the 3-2-1-1 rule. It's a concept Veeam has pioneered and long evangelized to its customers.

What it means: Organizations should always have at least three copies of their data, including a primary copy and at least two backup copies.

The backup copies should be on two different types of media, such as disk array, tape storage or the cloud. And of those copies, one should always be off-site.

Veeam is actually going further — adding another step to the process that serves as the final 1 in the 3-2-1-1 rule: One of those backup copies should be air-gapped — either stored offline or made immutable, meaning read-only. That provides an extra layer of protection if an organization's entire site goes down.

> “Customers can detect ransomware activity as it starts and take the appropriate action: Get servers offline and begin remediation, instead of waiting until a lot of systems have been encrypted, and the recovery effort gets exponentially harder.”
>
> **— Jeff Reichard Senior Director, Enterprise Strategy, Veeam**

Key Disaster Recovery Tools

Veeam’s platform is designed to help state and local governments more easily implement the 3-2-1-1 rule.

One of the new features in the latest version of the platform is an immutable backup capability, meaning it cannot be changed, no matter what.

The v10 platform allows customers to protect backup data to an immutable disk target that can’t be tampered with even by a user with administrative credentials. That’s key because admin credentials are often breached by online attackers.

“If I have the ability to write data to a disk target that a bad actor with administrative credentials can’t go and erase or encrypt, then I’m protected — even if my entire site gets compromised and everything on my site falls victim to ransomware,” Reichard says. “That is a big innovation in v10 and frankly something that everyone in the backup industry should be doing, but they aren’t. Veeam does.”

Another key capability of the platform, Veeam Availability Orchestrator, allows organizations to test their disaster recovery plans by practicing a failover — the process of having backup systems take over in the event of major system failure.

The orchestration capabilities by Veeam allow organizations to “painlessly test” their recovery plan without actually having to take production servers down, “to see whether your disaster recovery plan that’s been orchestrated is going to work,” Reichard says.

Battling Ransomware

When it comes to guarding against ransomware, Veeam’s platform offers monitoring capabilities that flag suspicious activity on servers and other parts of an organization’s infrastructure that could be evidence of attackers ransacking, deleting and encrypting files.

“Customers can detect ransomware activity as it starts and take the appropriate action: Get servers offline and begin remediation, instead of waiting until many systems have been encrypted, and the recovery effort gets exponentially harder,” Reichard says.

Unfortunately, hackers are getting smarter and their intrusions sneakier. It’s been estimated hackers who successfully penetrate an organization’s networks lurk in those systems for an average of 140 days before being detected.

In that case, simply restoring backups probably isn’t the answer because the backups themselves could contain tainted data.

The Veeam platform also comes with a capability called Secure Restore that lets organizations spin up backup copies of their workloads in a safe, offline environment to run malware scans on them before restoring the backups to a production environment.

“It’s not going to help me to restore my backup from three weeks ago,” Reichard says, “without being able to be sure, before I put it back live on my network, that there isn’t any malware in it. Secure Restore lets you do that exactly.”

Cyber Insurance: Far from a Cure-All

Reichard says some organizations have started to put far too much faith in after-the-fact cybersecurity measures, such as cyber insurance, as an answer to the ransomware epidemic.

If they get hit by greedy hackers, they'll take the loss and file a claim, the thinking goes.

That's a big mistake, Reichard says.

For one thing, no after-the-fact payment can make up for the fact your organization wasn't available to protect your constituents when they needed you most — an absence that, in the case of state and local governments, could put lives at risk.

And for another, there's no guarantee you'll actually receive a payout. Some major ransomware attacks, like NotPetya in 2017, have been described by governments as acts of war. Because policies often exclude war-related damages, many organizations impacted by NotPetya have still not received payment on their cyber insurance claims.

Other companies that have sought insurance claims have found them blocked because they were deemed to be partially at fault for failing to practice strong security measures.

And even if you do get paid, and your insurance reimburses some or all the damage that happens to you, it doesn't take care of what you actually lose, Reichard says, which could be the lives of your citizens at worst, and your data and the public's trust at best.

When it comes to the ransomware epidemic facing state and local governments, "The best option is to prevent the attack," Reichard says. But given the increasing sophistication of cybercriminals and the interconnected world we live in, that's not always a reality.

"If you can't prevent it, which is increasingly the case, you really need to be able to recover from it," he adds.

Learn more about how Veeam can help your state and local government agency stay secure in the cloud.

> "What customers really appreciate is that it's simple and that it saves them without them having to invest huge amounts of time."
>
> **— Jeff Reichard**
> **Senior Director**
> **Enterprise Strategy, Veeam**