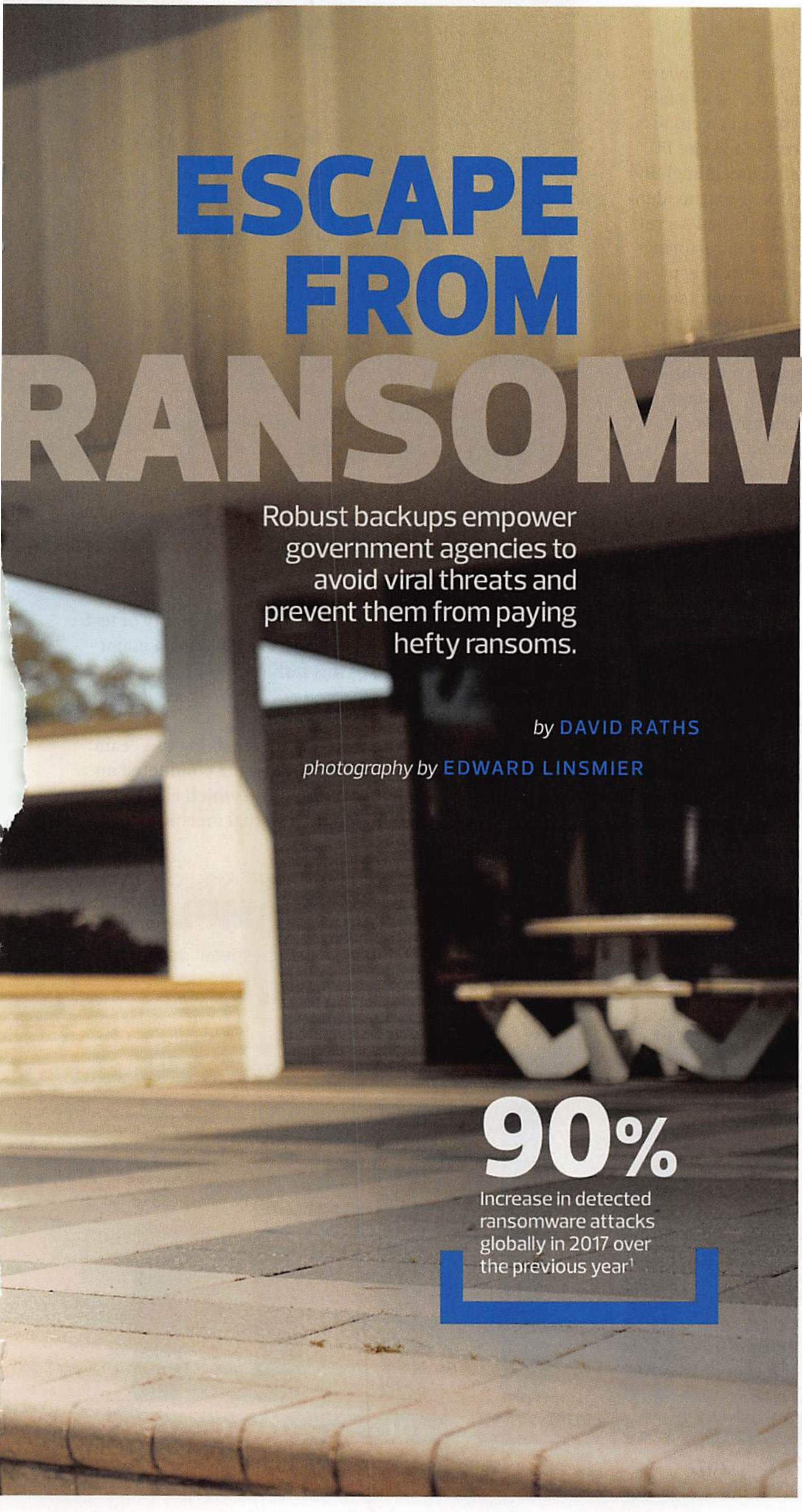


ESCAPE FROM RANSOMWARE

Robust backups empower government agencies to avoid viral threats and prevent them from paying hefty ransoms.

by DAVID RATHS

photography by EDWARD LINSMIER

Herminio Rodriguez recalls exactly where he was and what he was doing on the morning in February 2016 when the city of Sarasota, Fla., was hit by ransomware.

Rodriguez, who had been the city's IT director since November 2014, was meeting with Sarasota County officials in their offices nearby City Hall. He started receiving text messages from staff. The files on the city servers had become encrypted and inaccessible. "I stepped outside and had a phone call and realized that there was something horribly wrong," he says.

Racing back to City Hall, he and his security analyst took the next 45 minutes to verify that the city was under a ransomware attack. Cybercriminals had encrypted millions of files and were demanding the equivalent of $34 million in bitcoin to decrypt them.

Largely because of the Veeam Software Backup & Replication solution that Sarasota had put in place only four months earlier, Rodriguez was confident that the city's IT infrastructure could be restored quickly, and he never considered paying a ransom. "I could not have accepted a job where I would have to pay a bad guy to get my files back," Rodriguez says. "That would mean I wasn't doing my job."

90%

Increase in detected ransomware attacks globally in 2017 over the previous year[1]

Source: [1]Malwarebytes Labs, "Cybercrime tactics and techniques: 2017 state of malware," 2018

Many state and local government agencies are less prepared than Sarasota. Ransomware attacks highlight key mistakes governments tend to make regarding disaster recovery planning: not testing the operations of their backups and not ensuring that backups are remote but accessible.

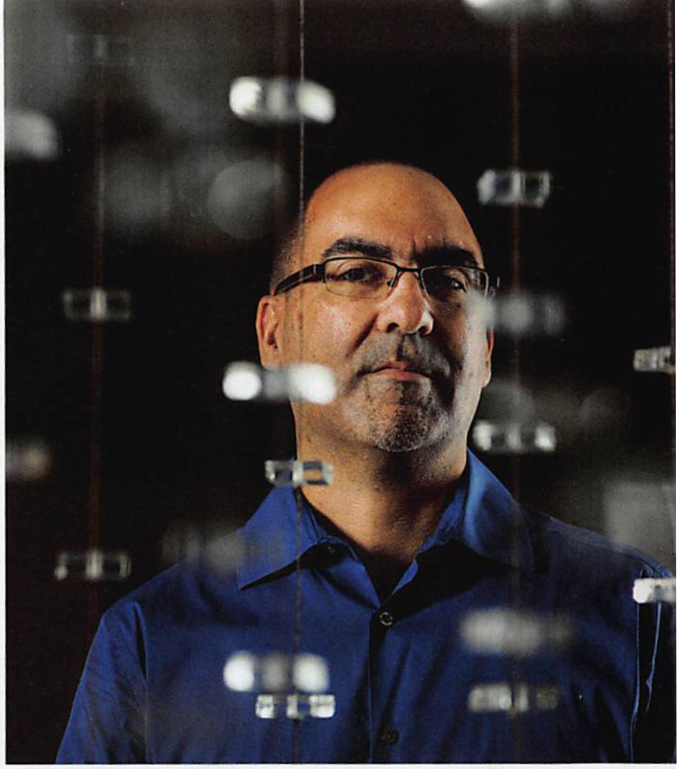
"Too many people think ransomware only happens to others — until they fall victim themselves," says Alan Shark, executive director of the Public Technology Institute. "Experts recommend comprehensive backups. While this is certainly sound advice, one must be very careful."

"Data must be backed up separately from the application software and stored offsite. It must be cataloged and go through a separate automated data scan that seeks out any malicious code and flags anomalies," he adds.

VERIFY BACKUPS

Although the city of Sarasota IT team members were confident they could restore their data, city workers meanwhile were unable to do their jobs.

"Our finance, inspections and utilities departments were all down. It was a huge wake-up call," Rodriguez says.



The ransomware had arrived as a fake invoice in an email attachment, the IT team determined. By 4 p.m., the team identified affected servers and began restoring them with Veeam. "The previous solution had an old virtual tape library, but nobody verified the solution worked," he says. "Backups were nonexistent."

In addition to the Veeam solution, the city had bought a new disk target — a Dell EMC Data Domain storage appliance.

"Once we went to Veeam and Data Domain, everything changed," Rodriguez says. "We crafted this new solution and were just getting the hang of it when the ransomware hit."

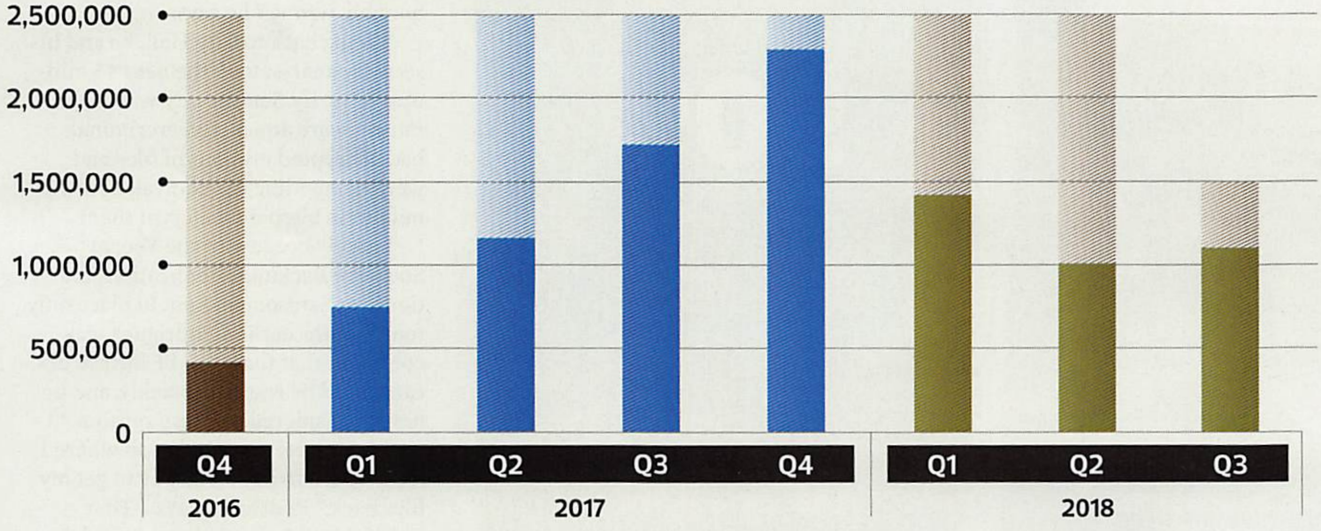
Rodriguez knew the city's backups were reliable thanks to regular testing, but he did not know how long it would take for the restoration.

"Although we had done plenty of test restores, we hadn't really done a major restore of this fashion," Rodriguez says of the emergency. "We worked all night and didn't go home."

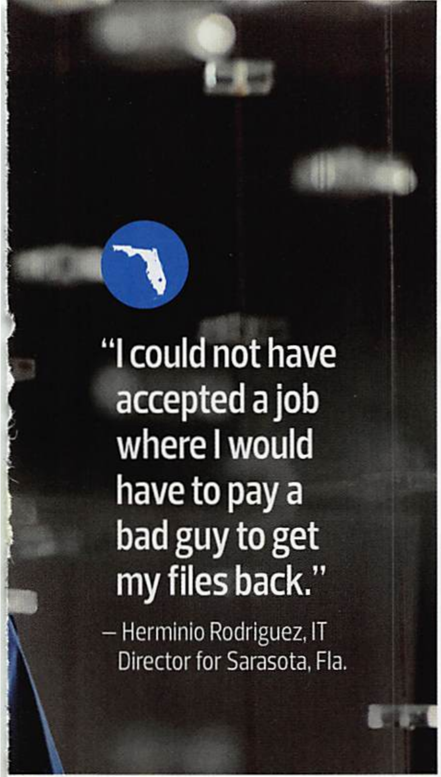
The next day, after talking to Veeam representatives, Sarasota conducted an Instant VM Recovery, which allowed them to mount a virtual machine image

A DECLINE OVERALL IN RANSOMWARE SAMPLES

The number of ransomware samples detected by McAfee globally declined over 2018. McAfee speculates the decline was due in part to ransomware actors switching to cryptomining for more money.[1]



Source: [1]McAfee, "McAfee Labs Threat Report," December 2018



"I could not have accepted a job where I would have to pay a bad guy to get my files back."

– Herminio Rodriguez, IT Director for Sarasota, Fla.

to a production host from a compressed and deduplicated backup file.

"By doing instant restores, we were able to get back two servers almost immediately," Rodriguez says. "We had restored a third server manually. That allowed us to bring all the data back online within 14 business hours."

CONTINUITY FOR THE CITY

When Chris McMasters became CIO of Corona, Calif., several years ago, one of the first conversations he had was with the police chief, who wanted to know how the city was going to protect itself from a ransomware attack. At the time, ransomware was shifting from targeting corporations to governments, especially police departments.

McMasters accelerated the city's shift to Microsoft Government Cloud, including using Azure Backup and Azure Site Recovery to protect mission-critical applications and data. "That was definitely one of the reasons we went with Azure – for the continuity we could have to restore very quickly and not have to pay ransom," McMasters says. "That is also how we set priorities. We pushed mission-critical apps to the cloud first."

Corona is a city of approximately 167,000 in Riverside County. When McMasters arrived, he saw that the backup was only a mile away, while most of the applications were hosted on-premises. "That alarmed me," he says. "What happens if we have an earthquake? The San Andreas Fault is not that far from here. Having the backup just on the other side of the freeway wouldn't help us much."

His effort to find a new backup solution dovetailed with other changes he wanted to make with Microsoft at the outset. "We went to Office 365 and OneDrive and pushed our critical infrastructure – Active Directory and Domain Name System environments – into the cloud first," McMasters says.

In his first year in Corona, his team moved at least 80 percent of servers into the cloud. "The principal reason for that decision was continuity for the city," he says. The main data center is 300 miles away in Arizona, with a site recovery system set up in Texas.

REMOTE RECOVERY

In 2017, Arizona Strategic Enterprise Technology, the state's shared technology services organization, began moving its on-premises mainframe services to hosted services provided by IBM's Z cloud. In addition to the increased speed and computing power and reduction in capital expenditures, the move has enhanced the state's disaster recovery capability, says Suzan Tasvibi-Tanha, assistant director and chief of managed services in the Arizona Department of Administration.

"In the past, we would copy our mainframe logical partitions to another duplicate mainframe from the Department of Economic Security, but to fully recover in the case of an event, it would take us a good 10 days. With IBM, we have brought that down to 72 hours," she says.

IBM's Z cloud has a main data processing center in Colorado and a disaster recovery site in Raleigh, N.C. "Our data gets transmitted to both places and our disaster recovery logical partitions are ready and configured. In case of a disaster, we could switch communication to Raleigh from Colorado," Tasvibi-Tanha says. "We did not have those capabilities in the past." ■

ASSESSING YOUR RISK

Deborah Snyder, CISO for the state of New York, suggests several tactics to protect against the threat of ransomware.

- **Assess business risk.** "Take the time to actually assess your business risk and the impact a cyberattack would have on your organization. Know where your sensitive data is – not just the obvious data and your trusted system of record, but unstructured data as well," Snyder says. Identifying the location of data is the first step to protect it from ransomware.
- **Put in data loss prevention technology.** "Make sure you have encryption everywhere that you have sensitive information," Snyder says. "Pay attention to employee training. You have to persuade users to do the right thing. They continue to be the most challenging element of our structure to harden." Bad actors often target human behavior with phishing attacks and other means to gain access to launch ransomware.
- **Pay attention to insider threats.** "In this day and age, when heuristics and analytics are available to implement, identifying undesirable and suspicious end-user behavior is easier than it ever was, and there is no excuse for not doing it," Snyder says.

→ Read how Colorado mounted an effective ransomware defense with backups at **statetechmag.com/ColoradoRansomware**.