



How to Strengthen Your Ransomware Defense

Despite years of efforts to improve defenses against ransomware, such attacks remain a constant threat.

In a worldwide survey, only 25% of respondents said they had not been hit by ransomware lately, “which leaves 75% who did suffer one or more attacks, that they’re aware of, in the last 12 months,” said Jeff Reichard, Vice President for Solution Strategy in the Office of the Chief Technology Officer at Veeam, a provider of backup, recovery and data management solutions.

It gets worse: Of those who reported attacks, more than a quarter said they were hit by ransomware multiple times, Reichard noted.

What can be done? During a [recent GovLoop virtual event](#), Reichard talked solutions and strategies with Jerry Simpson, State Deputy Chief Information Officer for Infrastructure Services at the city of Phoenix. They offered tips for state and local IT leaders to consider in the ongoing battle against ransomware and other cyberthreats.



Focus on Backups

First, it’s important to lay a solid foundation with the main tools, said Simpson, such as deploying multifactor authentication and monitoring traffic going in and out of the enterprise and across the network. But you also must prepare for the worst.

“On the back end you have the backups, you have the immutable copies, you have the copy offsite,” he said. A focus on robust backup strategies is critical, “if God forbid something does happen, and it gets through those defenses you have on the front end.”

With strong backups, data will be “protected and ready to go,” he said. It will be available for rapid systems restoration, a key to business continuity in the face of ransomware exploits.



Emphasize Training

As Phoenix built up its cyber defenses, “one of the first things we started to do is analyze the strategy. What do we currently do? What are we implementing as far as that front-end security stack of applications?” Simpson said.

From there, the city took on new capabilities. As IT started leveraging the Veeam solution set, a strategy emerged that put a heavy emphasis on training. “It wasn’t just: ‘Hey, send a couple people to class,’” he said.

“As we’ve implemented the tools, we’ve implemented the training” in depth, to ensure the city got maximum value from its cyber investment, he said.

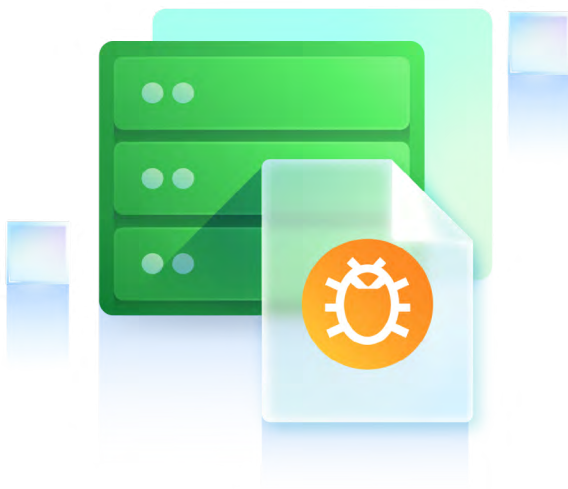


Make Communications Part of the Plan

To combat the ransomware threat, you need to create and maintain a basic cyber incident response plan, Reichard said. "That includes a communications plan. Who has the authority to declare an incident? Who has the authority to communicate with other stakeholders inside your organization, with the public, with any regulators or legal authorities that you need to deal with?"

That's just the approach that Simpson has taken. "We have incident commanders, people that come in and run the show" during cyber events, he said. "Whether it's a system outage or worse, there's always somebody on the call that's calming the people down, getting the information from the technical staff, finding out what's happening throughout the process."

The goal is to drive a methodical response. With a solid plan in place that includes a strong communications chain, "you're able to guide people through that process and recover from the incident, whatever it may be."



→ To learn more about defending against ransomware, [watch the full session on demand.](#)



Leverage Automation

Reichard pointed out that the Cybersecurity and Infrastructure Security Agency has extensive ransomware-prevention guidelines available. One common theme is security automation. "These are things that you want to have thought about before you're faced with an outage ... and a ransom demand, not after it happens," he said.

For state and local governments, "automation keeps you standardized and moving forward," Simpson said. This, in turn, helps generate buy-in from all the various stakeholders.

Incident response is complex, with lots of moving parts. Efforts can meet cultural resistance. With automation, "the groups start to say, 'Oh, we are moving to a good target ... we are starting to move forward,'" he said.



Find the Right Tools

A robust backup strategy requires modernized tools. Phoenix, for example, has 26 distinct lines of business, and "we are 100 percent now a Veeam customer throughout the city," Simpson said. "All of our federated and centralized departments are running on Veeam."

In addition to using Veeam Recovery Orchestrator to coordinate disaster recovery, "we're protecting all our systems — from financials to HR systems to our billing systems — all being backed up using Veeam," Simpson said.