CASE STUDY

Ransom is as ransom does: An unrecoverable backup nightmare

OVERVIEW

An IT administrator at a high-tech manufacturing site begins an early shift by checking unusual activity in the datacenter. Suddenly, an URGENT notification pops up on their phone. Their company is under attack, sensitive data was extracted, and they have three days to pay 1000 Bitcoin ($50 million USD) before the information goes to auction on the Dark Web, and the corrupted computers and data are permanently disabled. Yikes!

The IT team lead on duty notifies their management and everyone immediately goes to work isolating the affected network and mail servers. It takes a couple of hours to shut things down.

With time ticking, there is no easy way to tell just how many computers, servers, or files were affected by the malware and how long recovery will take. A lot of steps are involved, and the stakes are high. Every hour production is shut down, sales are lost, and that impacts their supply chain.

At least they have a good backup and recovery plan, and don't need to worry about the ransom, right? Ah... no they do not. Their home-grown partial backup system did not account for broad attacks like this one. Besides, all the redundant backup copies were kept on-premises. Some of the copies were encrypted during the attack and cannot be restored unless the decryption key is used.

Business management gulped hard and paid the ransom to expedite the data recovery process. The company was offline for more than five days. They lost 100's thousands of dollars in sales and worker productivity and got behind on order fulfillment, not to mention the ransom funds. Problems have lingered for months afterward as they work to shore up their cyber defenses, regain customer trust, smooth out issues with suppliers impacted by the attack, and cut back on improvement plans and strategic investments to cover the ransom costs (no magic money tree saved them).

COMMVAULT® CLOUD SAAS BACKUP: ALL-IN-ONE DATA PROTECTION SOLUTION

With SaaS Backup, they would have had enterprise-grade data protection in place to cover on-prem, multi-cloud, and hybrid environments—from a single pane of glass. SaaS Backup is specifically designed to deliver the speed, scale, security, and storage flexibility needed to reduce risk, minimize business disruption, and recover rapidly from attack by:

- Deploying in minutes without hardware expenses
- Protecting and managing their critical environments from a single SaaS solution
- Automating backups and reducing IT burden
- Isolating data to virtually air-gapped locations outside of source environments
- Preventing unwarranted access with zero-trust two-factor authentication, SSO with SAML, and role-based access controls
- Spotting unusual conditions, user behaviors, and file access patterns in real-time
- Easily detecting and flagging new anomalies and trends in at-risk datasets
- And guiding users to make more informed recovery decisions

GOING BEYOND "WHAT IF?"

The above disaster scenario is a fictional version of a real incident. With Commvault in place, the customer could have mitigated the risk of cyberattack and maintained business continuity—restoring data fast, back to specific points-in-time, versions, or locations. Commvault is a proven, cost-effective solution, acting like a virtual insurance policy for data protection and disaster recovery.

It's time to change the question from "What if we used Commvault?" to "How soon can we use Commvault to safeguard our business?"