rubrik

Plymouth, Inc. Recovers in 48 Hours and Zero Data Lost from Security Breach

Plymouth
ESTD 1938

INDUSTRY

Wholesale Trade

CHALLENGES

- Ransomware infiltrated the network through a temporary account

- An incomplete business continuity plan prolonged recovery

- All domain joined machines were affected

RESULTS

- Zero data lost

- $0 paid in ransom

- 100% recovery within 48 hours

Plymouth, Inc. believed it had done everything right to prevent cyberattacks by implementing controls such as endpoint protection, email security, firewalls, and monthly patching. But there was a critical gap—the organization lacked a complete recovery plan. This became painfully clear when a ransomware attack sent the IT team scrambling to restore affected systems.

"From this nightmarish experience, it was very clear that we weren't ready," said Rama Arumugam, IT Manager for Plymouth. The company had been working on a business continuity plan, but it was not complete. "We were flying blind and had to rely on our email communications and handwritten notes during this outage."

"This is where Rubrik really saved us. Thanks to Rubrik's native immutability, we kept damage to a minimum and recovered over 50 servers within 48 hours." Rama is convinced a return to normality would have been much quicker with a well-defined recovery plan.

RYUK ON THE RISE

At the onset of the attack, Rama suspected a network malfunction. "It appeared to be an internal DNS issue," Rama said. "On further investigation, we realized our network was affected by ransomware." The ransomware variant Ryuk snuck in through a temporary admin account IT had set up as part of Plymouth's relocation from Seattle to Auburn, Washington.

Ryuk started attacking Windows domain join machines, which connect remotely to the network. "They all had to be shut down immediately and rebuilt from scratch," Rama said. His team was able to prevent further infection, locked down the network, and reset every password.

"RUBRIK SAVED US TIME AND CUT DOWN OUR RTO"

Plymouth does more than sell products, they offer services to make their customers' lives easier. Whether their consumers need a variety of products frozen, moved, or stored, Plymouth supports them.

Despite the recovery plan's shortcomings, Plymouth was able to recover from the attack quickly because the IT team reacted promptly. "We run 24/7 so we were immediately notified and we got on it right away," Rama stated. "We went to our Rubrik appliance and started the process to restore."

"Rubrik's Instant Recovery feature, which leverages snapshots to execute a Live Mount and avoid data loss, was essential." He continued, "Rubrik saved us invaluable time and cut down our RTO significantly."

There were hiccups along the way. Their other Windows-based backups were unusable since they were all compromised by the ransomware. In addition, due to the nature of the incident, Rubrik wasn't linked to the company's vCenter server since all the Domain controllers along with the DNS servers were unavailable, which without it, the team had nowhere to restore to.

Fortunately, with assistance from Rubrik's support team, Plymouth found ways around the obstacles and developed a full recovery plan within 12 hours of the attack. "We recovered unscathed but the primary lesson learned is to have a robust business continuity plan and to recognize that it's never complete. It should be treated like a living document that needs to be constantly updated."

BUSINESS OUTCOMES

- **Zero data lost**: "We saw no evidence and the forensics team confirmed that no data exfiltration occurred. Rubrik ensured our backups were not compromised since the attack infected only our Windows-based systems and open file stores. I had so much confidence in our ability to recover. In terms of functionality, reliability and support, I have nothing but praise for Rubrik."

- **$0 paid in ransom**: "The attacker never actually had a chance to demand ransom because we acted so quickly."

- **100% recovery within 48 hours**: "Minimizing downtime was critical to continue to provide products to our consumers, so we moved forward the best we knew how. Rubrik's ability to instantly recover data and applications in sandbox environments enabled us to get our users online within 48 hours."

- **Best-in-class support**: "The tech support was exceptional throughout the entire process. Not only were they patient, they engaged other Rubrik engineers. They were swift in working with other vendors to come up with a solution to get the restore process moving forward. I was working around the clock for days and they were there every step of the way."

- **Rubrik's Ransomware Recovery Warranty**: "The Rubrik Ransomware Recovery Warranty offers us a new level of protection and sense of stability that goes beyond traditional means of data security found in the industry."

"The reality is, no business is immune from ransomware. For this reason, it's more important than ever to proactively prepare for a cyberattack and ensure you have the right data security solutions in place to quickly recover after an attack, while also minimizing the chance of re-infection. With Rubrik's latest product release, they continue to make critical advancements to their ransomware recovery solutions to give customers the ultimate peace of mind."

– Rama Arumugam, IT Manager, Plymouth, Inc.

Plymouth Poultry has supplied customers in the Western states with quality meat, poultry and seafood at competitive prices since 1938. Now in the third generation of ownership by the Block family, Plymouth continues to grow and strive to deliver quality.

Rubrik, the Zero Trust Data Security Company™, delivers data security and operational resilience for enterprises. Rubrik's big idea is to provide data security and data protection on a single platform, including: Zero Trust Data Protection, ransomware investigation, incident containment, sensitive data discovery, and orchestrated application recovery. This means data is ready at all times so you can recover the data you need, and avoid paying a ransom. Because when you secure your data, you secure your applications, and you secure your business. For more information please visit www.rubrik.com and follow @rubrikInc on Twitter and Rubrik, Inc. on LinkedIn. Rubrik is a registered trademark of Rubrik, Inc. Other marks may be trademarks of their respective owners.