cogent infotech

Case Study

Ransomware Readiness Program: Immutable Backups + Recovery Drills for Public Sector

The Client

A large public sector agency responsible for critical citizen services needed a proactive strategy to strengthen resilience against rising ransomware threats targeting government infrastructure. Its existing backup environment lacked immutability safeguards, and disaster recovery processes had not been consistently tested under real-world conditions, increasing the risk of prolonged service disruption during an attack.

The Challenge

- Backup systems were vulnerable to tampering, encryption, or deletion during ransomware incidents
- Lack of immutable architecture across a hybrid environment spanning on-premise and cloud systems
- Limited visibility into recovery time objectives (RTO) and recovery point objectives (RPO)
- Disaster recovery testing was infrequent and not aligned to realistic attack scenarios
- Recovery procedures were not fully integrated into broader cybersecurity incident response workflows
- Prolonged citizen service outage risk and growing pressure to strengthen public sector cyber resilience

About Cogent Infotech

Founded in 2003, Cogent Infotech is a trusted, award-winning firm with **23+ years** of experience**, 150+** government contracts, **10,000+** projects, and a **96% employee retention rate**. Recognized as an SBA Small Business and MBE-certified, we deliver excellence through diverse talent, AI-driven recruitment, and cooperative contracts like **NASPO Value Point and TIPS-USA.**

John Makely
Sr. Sales Manager
Business Development

John.makely@cogentinfo.com

323-573-2680

Solution and Process

- **Immutable Backup Architecture**
  Deployed immutable, air-gapped backup storage and segmented backup environments from production systems to prevent tampering or encryption by malicious actors
- **Zero-Trust Access Controls**
  Implemented role-based access controls, multi-factor authentication, and strict administrative privilege management to secure backup environments
- **Automated Monitoring and Integrity Checks**
  Configured continuous validation of backup health and retention policies and deployed anomaly detection using SIEM, SOC monitoring tools, and Microsoft Sentinel
- **Structured Recovery Drills**
  Conducted quarterly ransomware simulation exercises to validate restoration timelines and operational readiness against defined RTO and RPO targets
- **Hybrid Recovery Integration and Executive Dashboarding**
  Integrated recovery workflows into the agency's incident response playbook and created a Power BI dashboard to provide visibility into backup status, recovery performance, and resilience posture across on-premise and cloud systems

Outcome

- Achieved **100% immutable backup coverage** across critical systems
- Reduced ransomware recovery time by **60%**
- Validated recovery readiness through quarterly simulation drills
- Strengthened alignment with public sector cybersecurity frameworks
- Minimized the risk of prolonged citizen service disruption and improved executive confidence in cyber resilience

Risk Analysis

- Backup compromise risk if ransomware reaches storage environments
- Recovery failure risk if restoration processes are not regularly validated
- Access control risk from privileged compromise in backup administration
- Hybrid environment risk across on-premise, cloud, and critical database workloads
- Public service outage and compliance risk from extended recovery timelines

Best Practices

- ✓ Deployed immutable, air-gapped backups fully separated from production systems
- ✓ Applied zero-trust access controls with RBAC, MFA, and least-privilege governance
- ✓ Used continuous backup validation and anomaly monitoring to detect issues early
- ✓ Conducted quarterly recovery drills aligned to RTO and RPO targets
- ✓ Integrated recovery workflows with the broader cybersecurity incident response program

TECHNOLOGIES

- Immutable / Air-Gapped Backup Storage
- SIEM & SOC Monitoring Tools
- Microsoft Sentinel
- Azure / AWS-Compatible Recovery Architecture
- Power BI
- RBAC and MFA Controls

John Makely
Sr. Sales Manager
Business Development

John.makely@cogentinfo.com

323-573-2680