COMPUTER RESOURCES OF AMERICA

Protect Your Data Against Ransomware Attacks

CRA™
Transform IT
Computer Resources of America

Protect Your Data Against Ransomware Attacks

Computer Resources of America Case Study

Client Details

Company X is a non-profit located in New York, NY with over 230 employees. *Company X* provides important health and employment services to disadvantaged low income New Yorkers and medical case management services for substance abusers throughout New York city.

Business Situation

Company X relied on a physical tape backup system and an off-site archive. The system was inefficient and could not be easily replaced because it was a significant capital expenditure. After a ransomware attack, the time to recover data from off-site backups was considerable and resulted in weeks of downed operations with critical applications unavailable.

Solution

CRA implemented a backup schema utilizing a 3-point backup mechanism with on-site appliances and cloud backups as a multi-layered solution. The new solution also provided baked in mechanisms for business continuity.

Business Need

- Quality of service issues with on-premise tape based-backup.
- Numerous user complaints for file restores because of an obsolete and inefficient system with much time needed to access off-site backups.
- Prohibitive hardware/software costs to upgrade with skewed costs/benefits.
- Cumbersome procedures to test accuracy and validity of backup data sets.
- No business continuity and resiliency plan that fitted into the Company's long-term IT roadmap.

The Solution

CRA implemented a multipoint solution that utilized:

- Best practice guidelines and alignment with security controls.
- A Linux-based appliance to house all backups with a significantly higher tolerance for malware/ransomware attacks.
- A private cloud that extended the backup schema and allowed for a seamless "instant on" for restores.
- A formalized process for testing backups as part of an annual business continuity exercise to ensure that systems performed as expected.
- Baked in business continuity. Virtualized workloads that were on premises could now be easily spun up in a private cloud and provide application access should the need arise and the office became inaccessible.

Protect Your Data Against Ransomware Attacks

CRA listened to the client's pain-points and conducted extensive requirements gathering to determine what solutions offered the best cost/benefit approach for the Company. CRA leveraged its expertise and was able to map business needs to cutting edge cost-effective solutions. This included business continuity and for events such as DR planning and adverse events such as the current COVID-19 pandemic.

CRA identified and implemented a customized multi-point backup solution to address Company's concerns and needs and solidified a strategy for IT transformation.

The business continuity elements of the solution involved backing up virtualized workloads both to the appliance and then to the cloud. CRA was able to move critical third-party applications from physical servers to virtual servers thus reducing cost and overhead and simplifying the physical infrastructure footprint. A critical element of the business continuity plan was the ability to spin up the virtual servers in the cloud and enable secure access to mission-critical applications from anywhere.

The CRA Difference

The Company now enjoys a faster, more reliable backup system. Their data is protected much more securely and aligns with best practice guidelines. The new solution provides the virtually limitless storage capacity of the Cloud and secure access to critical applications for business resiliency. In addition, the new system lowers operational risk because incorporates significant elements to guard and protect against cyber-attacks.