Being Prepared for a Bad Day: Optimizing IT and Data Resilience

Presented by:
Louisiana Secretary of State Kyle Ardoin &
Chief Information Officer Brad Manuel

IT and Data Resilience Overview

- Natural and man-made disasters, the increase in cyber attacks, the need to build and maintain public trust, and the need for continuity of services dependent on data and technology are reasons that strong IT and data resilience is vital.
- IT resiliency is the ability to quickly recover your IT systems due to an emergency event, such as a power outage, natural or man-made disaster, hacking event or infrastructure failure.
- Data resiliency is the ability to protect and/or recover data quickly due to an emergency event, such as hardware failure or cyber attack.

Building Blocks of Resilience: Steps You Can Take

- Reduce or eliminate downtime with redundancy or fault tolerance
  -Supply automatic backup power
  -Supply redundant infrastructure (routers, switches, servers, etc.) to failover to
  -Supply a replicated database to failover to in the event the primary database becomes unavailable

Building Blocks of Resilience: Steps You Can Take

- Backup your data
  -Having regular backups allows for smooth and quick recovery in case of an emergency event with minimum loss of data depending on the backup timeline
  -Backup to multiple locations (including off-site)
  -Test and verify your backups regularly

Building Blocks of Resilience: Steps You Can Take

- Take proper security measures
  -Implement a cybersecurity training and awareness program for your staff
  -Create and regularly update strong cybersecurity policies
  -Get legislative or budgetary buy-in to assist your state's investment in cybersecurity.
  -Cybersecurity is ever evolving, so create a culture of evergreen assessment and after-action reviews

Building Blocks of Resilience: Steps You Can Take

- Have a business continuity plan (BCP)
  -Gives direction on how to continue operations while achieving the defined recovery time objectives (RTO–the maximum tolerable time that a certain system can be down without causing catastrophic damage to an organization)
  -Tabletop exercises are a great tool to test your plan and train your staff on responding to emergency events. These can range from small brainstorming sessions to formal events for all personnel, and gives everyone an understanding of what is required during an actual event
  -Use these exercises to update your BCP

Building Blocks of Resilience: Steps You Can Take

- Continuous monitoring and testing
  -Hire dedicated cybersecurity staff–while cybersecurity is everyone's job, department accountants cannot and should not be expected to perform the technical tasks
  -Have regularly scheduled testing by both your dedicated staff and a properly-credentialled, trusted third party
  -Test your network, website, web applications and people
  -Test your policies and procedures to validate their purpose and build confidence of support staff

Resiliency Action Items

- Work with your legislatures or appropriating bodies to secure the necessary resources to be resilient.
- Regularly train and test staff to ensure resiliency.
- Create and update your business continuity plan to be prepared for emergency events.
- If you take the proper precautions, you will be prepared for every “unexpected” event.

Questions

Sec. Kyle Ardoin

Brad Manuel