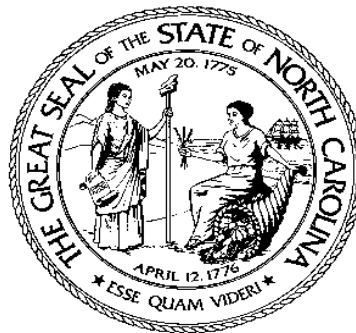


2010 NASCIO RECOGNITION AWARDS

Protecting, Securing and Making NC Voter Data Available

Risk Management Initiatives

05/27/2010



Submitted by:

North Carolina State Board of Elections

Executive Summary

In North Carolina, state and local entities are responsible for administering voter registration data. Data may initially be processed at one of several locations, including the citizen's County Board of Elections (CBE) office, a local office of the state's Division of Motor Vehicles (DMV), or even at the State Board of Elections (SBE) central office. Since CBE offices are administered by the county and are not under direct control of SBE, risk management was an integral concern. Therefore, to improve the efficiency and integrity of the state's voter registrations, the State Board of Elections and the 100 County Boards of Elections began a major initiative to consolidate their disparate systems. Deciding how to best design an infrastructure to mitigate risk was going to be a challenge.

SBE decided to design a decentralized statewide system to mitigate risk and provide high availability to CBE, SBE and the public. This system consists of 101 remote agencies, including DMV, that replicate voter registration data real-time to a county mirror database at SBE. These mirror databases then replicate the data to a statewide centralized database. This system is redundant by nature, giving the ability to have multiple points of failure while retaining the ability to perform day to day job functions.

As a result of the collaborative efforts, North Carolina was able to not only standardize voter registration, but to mitigate risk in a way that has allowed the statewide elections information management system (SEIMS) to be always available and secure enough to keep the public confidence intact. This project was completed in December 2006.

Problem Description

In 1998, the North Carolina State Board of Elections (SBE) along with all 100 County Boards of Elections (CBE) worked to create and implement a statewide elections information management system (SEIMS.) SEIMS was designed to standardize voter registration across North Carolina. The initial solution seemed simple: create a statewide voter registration application and deploy it to all 100 counties to use to manage voter registration data. As we delved further into the project, we realized that there were many technology challenges to overcome. Initially, there were three technology challenges that involved managing risk.

The first challenge was overall design, and the choices were centralized and decentralized methodologies. In early 2000 and in the past, the most common central systems were mainframe systems, but at the time of this project entities were moving away from the mainframe model to a client server model. The second choice, decentralized, was too disconnected and normally data only traveled one way, while a centralized methodology left us with a single point of failure.

The second challenge was to ensure the security of the overall system and to make sound decisions that would mitigate risk to the enterprise. After deciding on a hybrid decentralized model, SBE realized that securing the data and systems would pose a

difficult challenge, especially since all of the remote servers would reside on an infrastructure that was not controlled by SBE.

The final challenge was the ability to recover from system failures and disasters. Understanding the business, risks involved and what are acceptable downtimes are some of the factors that helped to determine backup and recovery strategies.

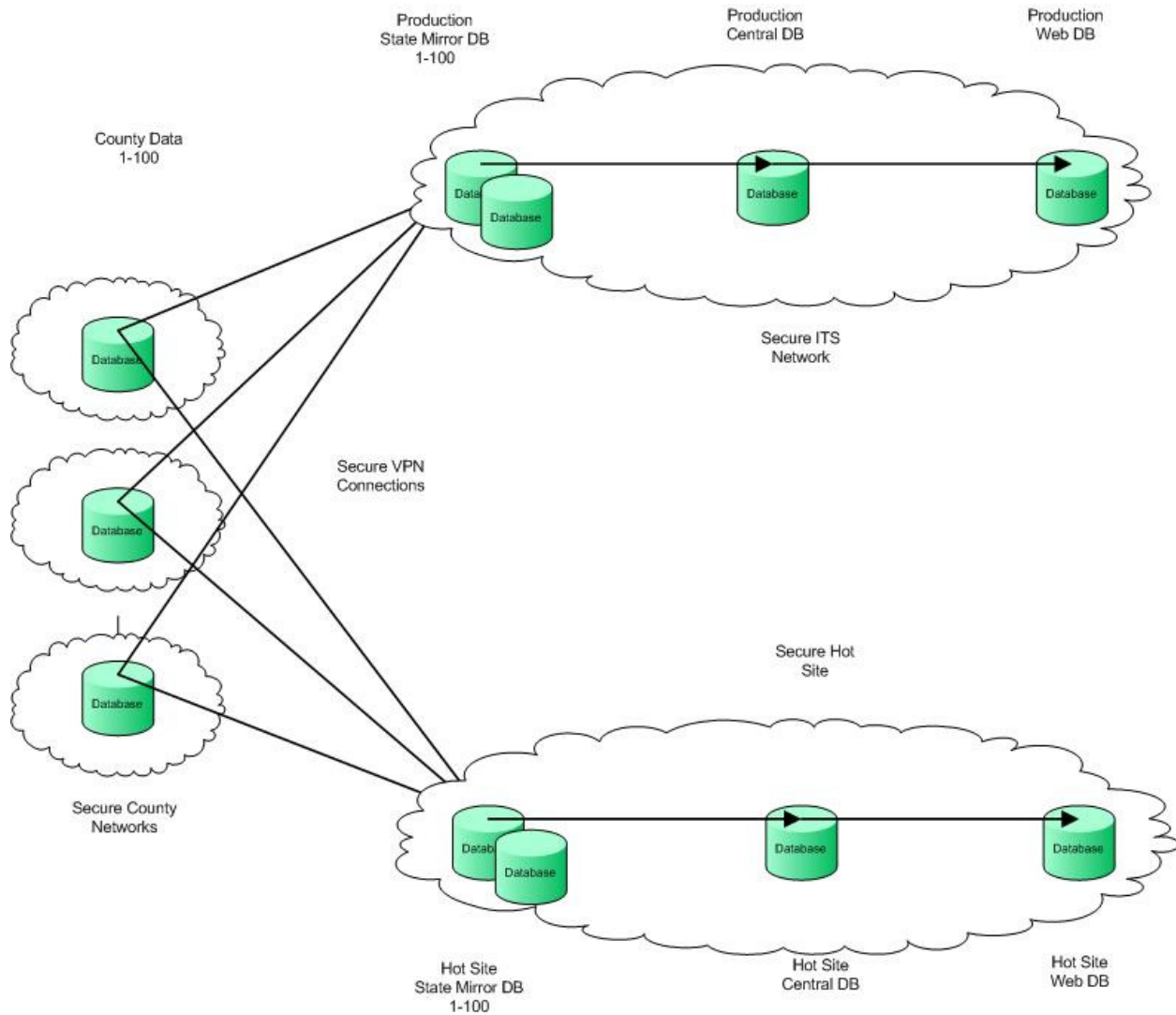
Solution

In choosing an infrastructure methodology, our design team researched many different methodologies, including centralized, decentralized and a hybrid approach. When this began in early 2000, almost 80% of the counties in North Carolina only had access to very low speed Internet access. In addition, all CBE offices are owned, staffed and paid for by county funds. Realizing that a centralized system would be extremely costly to the state, a hybrid decentralized methodology was developed.

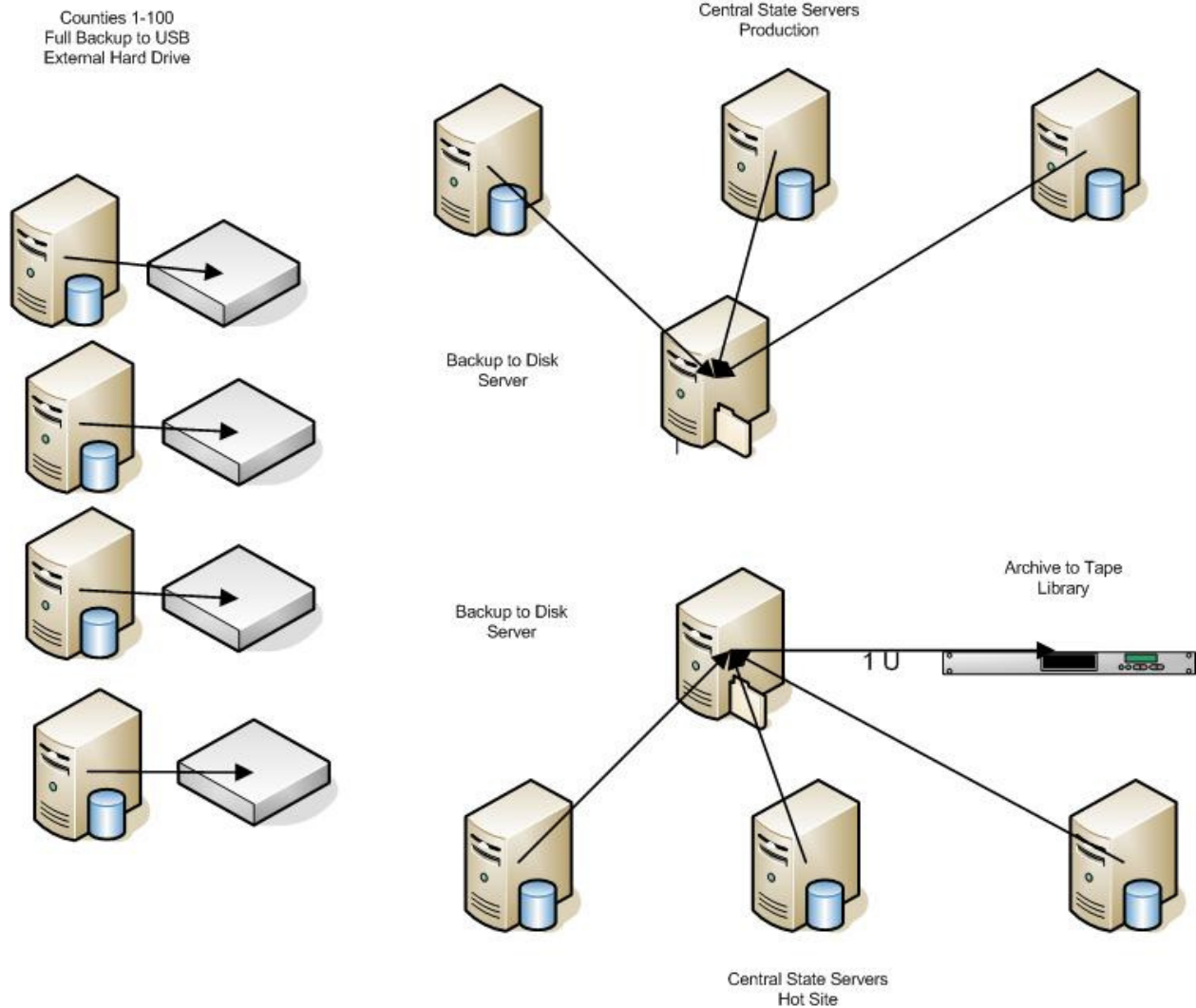
This decentralized model consists of four levels. The first level of the infrastructure includes a SEIMS server in every county along with a tape backup mechanism. The second level is a single mirror server at the state data center that all county servers can replicate data to. At the same time, the data also replicates to the SBE hot site mirror server, thus giving a second level of redundancy. The third level is the centralized database server where all county mirror databases are consolidated into one central SEIMS statewide database. The fourth level is the reporting database where the data is denormalized for web access and applications. All of the data is replicated to the state data center and the SBE hot site to all databases on a real-time basis, except for the denormalized database, which is updated nightly.

The second challenge was security of the servers, database and data. Since SBE decided on a decentralized methodology, and the SEIMS servers had to reside in an environment that was not controlled by SBE, we had a significant challenge on our hands. The first issue was securing the server. SBE used all standard practices in securing access to the server and hardening it to protect against malware, viruses, and other attacks. These servers are currently Windows servers with Microsoft SQL Server databases. To further protect the servers, SBE wrote custom code that was placed in MSSQL to terminate any connections to the database if they did not derive from an approved SEIMS application. This protects the data from backend access from applications like Microsoft Access or any other foreign user trying to gain unauthorized access to the SEIMS databases.

The next security challenge was securing the transmission of data from the CBE SEIMS servers to both sets of SBE servers. Since the transmission came from 100 different county environments to which SBE had zero control, we decided on a point-to-point Virtual Private Network (VPN) methodology. The CBE SEIMS server initiates a VPN tunnel from itself to the SBE mirror server, thus leaving no gaps in between and protecting the data across the Internet. The next image shows a design of the environment.



The final challenge was backup and recovery of the SEIMS data. Our original design included tape backups at the county and state levels. IT professionals know that it is always easy to create backups, but how do you know they are actually recoverable? Tape backups are also difficult to verify and time consuming to catalog and recover from. Because of these and other tape related challenges, SBE designed and implemented a USB backup system for all CBE offices. USB 2.0, the physical size of the USB drives, and the amount of storage a USB drive can contain allowed for this implementation. With these USB drives, data can be easily stored, verified, cataloged and recovered. At the state level most of the tape devices were replaced with backup to disk devices, and one core tape backup unit was left in place for offsite storage. See the next image for an example of this design.



Data and process recovery is important to everyone in business. Every day we ask the question, what happens if our server dies? Since we have 100 county offices, a decentralized model allows for 99 counties to still operate if one county server is unavailable. In addition, since data is replicated to the state level servers, if a state server becomes unavailable, all county servers will still function and queue transactions until the state server becomes available. There is still the issue of what happens if that one county server becomes unavailable. If this happens, CBE offices will then be able to utilize a remote Citrix environment and access their state mirror database via the Internet. When the CBE server becomes available again, the data will then replicate from the mirror back down to the host, thus keeping the data in sync.

Public Value of the Project-- Significance

This decentralized solution is a win-win for everyone. The CBE office wins since they have local access and LAN data speeds from their application to their database on the

SEIMS servers. In the event of a failure to the local county server, they can utilize SEIMS via Citrix to the state mirror servers or even process locally in the event of a state server failure. All of this produces a potential for minutes of downtime. SBE wins by having real-time access to all of the data in a single database without having a single point of failure. North Carolina wins because their SEIMS voter registration system is always available to election officials, state officials and the general public.

Public Value of the Project--Benefits

In general, the SEIMS statewide decentralized infrastructure has provided North Carolina the following benefits:

1. Cost Effectiveness – Since this project began State Board of Elections has had significant cost savings in the following areas:
 - a. Eliminated tape drives and replaced with USB drives. This is a savings of approximately \$90,000 every four years.
 - b. Reduced labor costs. With our recovery models in place, hot replacement servers are ready to be drop shipped and replaced by any county worker; no IT professional is needed to install or configure them.
 - c. Reduced server costs. With our decentralized model, standard workstations with multiple hard drives have replaced bulky and expensive servers. This cost savings is approximately \$300,000 every four years.
2. Availability – Having no single point of failure and multiple redundancies ensures that North Carolina voter information is available 24/7.
3. Secure – Since implementation in 2004 there has been zero loss of data and only one reported breach of security where the county removed all of the rules on their firewall. After state reporting of the incident and an internal review, no SEIMS data was accessed or tampered with. Since the alleged hacker was from overseas, the server was picked up by the FBI and sent to Quantico for further investigation, where our initial analysis was verified.
4. Easy to manage – CBE servers can be managed and replaced by anyone, not just IT professionals. In our environment, if a server has an issue it is taken out of commission, sent to the state office and replaced with a “hot” spare. The defective server is then repaired by technicians at the state.
5. Recoverable – Many levels of the same data allow for recovery of the data from any point.