Information technology at NALC

Paul Barner

Innovations in computer technology in the mid-1970s spurred the computer age and led to the advent of the personal computer (PC). This created new opportunities for businesses and individuals alike by providing more compact and affordable computer options.

However, as with any new technology, there are both pros and cons. While users can benefit tremendously from efficiencies introduced by computers, one must always remain mindful of the exposure risks associated with storing and transferring data. Therefore, to maintain relevance, thought must be given to more than just the obvious. The security of network systems must be a top consideration for any Information Technology (IT) database. And hand in hand with security goes reliability.

Behind the scenes of IT at NALC

Like many organizations, NALC has its own in-house IT Department. The mission of NALC's IT department is to maintain the union's membership and organizational databases while creating new and innovative programs in a secure, reliable and efficient environment. The department accomplishes its mission through the collaborative efforts of the network operations and software development teams. The world of IT is constantly evolving and an IT department must be able to keep up with this ever-changing environment.

There are many considerations that must be taken into account to maintain a reliable, safe and efficient computer infrastructure. A quick behind-the-scenes look into the NALC IT structure will better illustrate the complexity of network security.

Besides the obvious security protocols of user logins and passwords, devices known as firewalls are used to block entry into the network from unknown or unauthorized sources. Along with firewalls, software programs that are designed to detect potentially harmful or malicious email "quarantine" such threats, thus preventing viruses and hackers from entering the network.

Systems redundancy: A good thing

To ensure secure network reliability, NALC has created a robust IT infrastructure with systems redundancy playing a large role. One example of systems redundancy involves the availability and use of multiple internet pathways or routes to access data. This reduces the risk of losing access to the network because of internet outage or disruption in internet service involving a single pathway. However, systems redundancy doesn't stop with communications. NALC's IT infrastructure involves the use of redundant power supplies as well as air-conditioning systems that maintain its computer servers and hardware at a constant temperature. Back-up systems also are used to maintain continuity of data.

Disaster recovery

Another element of the NALC IT infrastructure involves disaster recovery. A large part of the disaster recovery program involves secure data replication. A secondary computer server and network infrastructure that mirrors the primary infrastructure but is housed in a different location is used for this replication. While the primary infrastructure is in use, all data is being simultaneously replicated or copied to the secondary. Should a disaster occur disabling the primary infrastructure, NALC can switch over to the secondary without loss of security or data.

As one can see, the process of securely maintaining the IT infrastructure that serves as the repository of NALC members' data is very complex. There is a continuous emphasis on balancing and maintaining security, reliability and efficiency by employing a combination of best practices and latest technologies.

The need to be ever vigilant

Still today, the 2016 U.S. presidential election is mired in controversy as the world was witness to sophisticated cyber intrusion. The question of overall impact never will be fully answered. What has been made clear, though, is the level of sophistication that exists and the need to continually assess computer networking systems for vulnerabilities and employ best practices to limit exposure to breaches.

This serves to illustrate the need to be ever vigilant in how we secure the information entrusted to us. We must all be continually mindful of the possible ramifications if we let down our guard.