FEDERAL DESIGNATION OR NOT, WHAT TO KNOW IN AN ELECTIONS-AS-CRITICAL-INFRASTRUCTURE WORLD

INTRODUCTION

In January 2017, the U.S. Department of Homeland Security (DHS) designated the conduct of government elections as "critical infrastructure." The designation highlights a very important question: how do states ensure that they are deploying state-of-the-art security in their election technology and processes in a rapidly changing world? If the designation holds, it could present an opportunity for states and localities to engage infrastructure—and process—security experts to share insights and proven best practices to learn how to bring and maintain the highest standards for security to their election technology and process.

Twenty-first century advances in communication, automation, and logistics provide great benefits to our personal lives and to our businesses. They also bring a new context in which government must think about security. Long-implemented, comfortably familiar practices, when critically evaluated against modern security protocols, simply prove to be insufficient.

Going forward, with technology rapidly advancing and the attendant need for security to keep pace, what a government today perceives as strong security protocol—technological or otherwise- likely will not be the case tomorrow. The danger is in familiarity breeding mediocrity and leaving us open to undetected and increasing breaches.

THE REALITY OF RISK IN ELECTIONS

The purpose of this paper is to help states and localities assess whether their perceptions of security accurately reflect the reality of ever-changing technology, and provide best practices and tools to help detect risk and defend against and mitigate the consequences of breaches.

A 2015 CompTIA IT Security Study concluded that while malware and hacking register the highest level of security concern among end users, there are a great many threats that should raise the same level of concern. Prominent among these is human error; the use of outdated process, inexperienced or untrained people, lack of process oversight, and antiquated technology are leading culprits in security breaches.

ROOT CAUSE OF SECURITY RISK[1]

Top Human Error Sources

- 42% End user failure to follow policies and procedures
- 42% General carelessness
- 31% Failure to get up to speed on new trends
- 29% Lack of expertise with websites/applications
- 26% IT staff failure to follow policies and procedures

[1] CompTIA 2015 IT Security Study

"95 percent of all security incidents involve human error."—IBM's 2014 Cyber Security Intelligence Index

COMPONENTS OF ELECTION INFRASTRUCTURE

Components of Election infrastructure as defined by the DHS:

- Storage facilities
- Polling places
- Centralized vote tabulation locations used to support the election process before, after and during elections
- Information and communications technology
- Voter registration databases
- Voting machines
- Systems which manage the election process
- Systems which report and display results on behalf of state and local governments

PHYSICAL LOCATIONS

Storage Facilities

Traditionally, purpose-built voting equipment and ballot materials were kept in locked warehouses. Modern physical security precautions add technology to enhance security, including:

- Biometric access control
- External and internal 24/7 camera and audio surveillance security
- Internal floor-to-ceiling cage storage area with sealed cage doors, a numbered security seal, and a manual log to documents the security seal number used to enter the cage

Polling Places and Centralized Tabulation Locations

Security at polling places and tabulation locations has generally been provided by poll watchers and/or staff observing the comings and goings of voters, candidates, canvassers, and staff. Current best practices for hardening security at polling places (without disenfranchising voters) and tabulation locations include a combination of human, process and technological advances:

- Natural Surveillance— maximizing the visibility of areas that should be observed
- Access Control—Limiting and regulating entrances
- Territoriality—Clear delineation of space creates a sense of ownership for legitimate users (staff)
- Staff Awareness—Training staff to spot and report suspicious activities

INFORMATION AND COMMUNICATION TECHNOLOGY (ICT)

Voter Registration Databases

Malicious actors use a variety of methods to interfere with voter registration websites and databases that were not in existence or in wide use at the time HAVA was implemented. Phishing attempts, injection flaws, cross-site scripting (XSS) vulnerabilities, denial-of-service (DoS) attacks, server vulnerabilities, and ransomware are among the risks. Since most security breaches are human-based, targeted attacks of VRDBs can be preventable if election officials and network administrators ensure their system has multiple levels of security with no single point of failure, and implement the following common sense best practices:

- Assign strong user permissions and maintain strong password requirements
- Encrypted Data—At rest and in transit
- Backup Critical Information—Test ability to revert to backups during and after an incident
- Regular Scans of VRDB Network and Systems—Scan and probe all network segments to ascertain weak points and ensure system functions as intended
- Self-healing Databases— Allows for automated failover and recovery
- Software as a Service (SaaS) Delivery Model— Allows for ongoing security updates that eliminate key threats and reduce vulnerabilities to voter data Penetration Testing—Attempt to infiltrate the system to test the security of the system

Voting Systems and Associated Infrastructure

Researchers have demonstrated that many legacy voting systems—most of which are over a decade old—are susceptible to tampering. Familiar paper processes provide a false sense of security, as paper is prone to human errors ranging from not filling out a ballot correctly to the postal service misdelivering or losing ballots in transit. Modern technology, however, can be used to encrypt ballots and personal data with missile-launch-code levels of security.

UOCAVA and Remote Online Voting Systems and Associated Infrastructure

Traditional paper mail-in methods make it challenging for remote and disabled citizens to exercise their constitutionally mandated right to vote. Modern technology allows voters to securely transmit an encrypted ballot between the voter's web browser and the election server using Transport Layer Security (TLS) transmission that employs Advanced Encryption Standard (AES) 256-bit encryption, with 2048-bit keys. TLS is the same protocol used by banks and e-commerce companies to keep personal information safe and secure during transactions, and similarly keeps all voter communications absolutely private. The TLS protocol enables voters to securely communicate in a way that is designed to detect and prevent eavesdropping, tampering, and communications forgery.

Direct Recording Electronic (DRE) and Optical Scan (OpScan) Voting Systems and Associated Infrastructure

With voting technology, recertification of systems using the highest level of encryption and latest operating systems is critical. Paper systems alone cannot demonstrate whether breaches have occurred or not. A multi-channel voting system provides both the familiarity of paper and the security of digital auditability.

- Hardware Diagnostic Test—ensuring all equipment is working as intended

- Recertification to latest NIST encryption standards
- Upgrade to latest secure operating system
- Require real-time digital audit records
- Logic and Accuracy (L&A) Testing—simulating a mock election before each election
- Risk-Limiting Audit Test—Currently, some voting systems have a process by which all of the audit can be conducted electronically, eliminating doubt in the electorate's mind.
- Tamper-evident security labels with processes to ensure verifiable chain-of-custody when accessing ballot scanners (OpScan)

Information Technology Infrastructure and Systems Used to Manage Elections

Today, election functions such as voter management, ballot layout and design, electronic poll book configuration, and reporting can reside in a single user friendly interface with a progress tracking dashboard and workflow automation for core tasks to ensure a successful and accurate election. Interoperability of modules and a centralized dashboard makes in-house election administration a more viable option, reducing the risk of external malicious actors. The use of technology can mitigate the risks that come from error-prone human and paper processes.

Human Factor

IBM reports that most security breaches are caused by human or process errors. Some of the most common human errors include:

- Lost laptops or mobile devices
- Disclosure of regulated (sensitive) information via incorrect email address
- Opening infected attachments or clicking on unsafe URLs[2]
- System misconfiguration

Modern technology allows for a corrective process of encrypting and digitally storing a backup of the paper ballot image allowing for a more efficient, thorough, and transparent audit as it provides for the ability to conduct real-time 100% risk-limiting audit of every vote, and the elimination of the potential for human error.

Another common human error includes the use of default usernames/passwords, or easy-to-guess passwords. This can easily be mitigated by using two-factor authentication- with primary authentication relying on something that you know (a password), the secondary factor that uses something you have (a mobile app and smartphone) protects users from unauthorized remote access.

Human error as it relates to access can be strictly controlled through the assignment of individual users or user groups, and controlled roles and permissions-based credentialing. The basic design for assigning functionality to specific roles is congruent with the principle of least privilege and increases levels of access and privilege as the roles progress.

---

[2] Human Error Accounts For Over 95 Percent-of Security Incidents, duo.com blog, Duo Security, Inc.

Paper Processes

Jurisdictions continue to endure unnecessary errors because they rely on human-centric, paper-based processes. Not only do these antiquated processes make jurisdictions less efficient but, worse, they become vulnerable to malicious actors. Additionally, when problems occur, the risks may ripple, leading to poor decisions, election violations, and damaged reputations that are difficult to repair.

For instance, risk-limiting audits manually examine a random sample of ballots in a way that has a chance of detecting and correcting incorrect results. Researchers have developed statistically based audit techniques that cut down on the number of ballots to be manually audited, nevertheless, this human-centric process is time-consuming, inefficient, and costly. Additionally, if the reported winner actually lost, a full manual count is needed.

CONCLUSION

The national and economic security of the United States depends on the reliable functioning of critical infrastructure. Similar to financial and reputational risk, failure to adopt a strong security protocol can drive up costs, and harm a jurisdiction's ability to maintain the voters' trust in the democratic process.

The conversation around elections as a critical infrastructure— whether the designation sticks or not— is an opportunity for states, the federal government, and industry vendors to share information and to assess the reality of their current security risks, and, where necessary, implement meaningful reforms to minimize and mitigate those risks.