

“PREVENTION OF ATTACK, NOT DETECTION AFTER THE FACT” A NOTE ON RISK ASSESSMENT AND RISK MITIGATION

by Dana DeBeauvoir, Travis County Clerk
P. O. Box 1748 Austin, Texas 78767

Introduction

We must specifically match the solution to the problem. The problem or Risk Assessment must be evaluated on the basis of likelihood of event and the extent of the damage. Risk assessment must match the proposed solution, the risk mitigation. The best, simplest protection every voter has right now is the summary screen on their DRE voting unit. We need training funds to teach people to use and understand the tools they've already been given.

Proponents of DRE voting accuracy and security often say that DRE voting is the safest, most tamper-proof method in history. These statements are not just prose. Here are two examples of the improvements DRE systems offer. First, in optical scan technology, each candidate position has a unique set of candidates or propositions for each ballot style. The tabulation code had to be re-written for each election. Thus, the importance of Logic and Accuracy testing. The opportunity for vendor interference was present for each election and was much greater than in current DRE systems. To make the point, the vendor had to program the ballot for each election.

Usually the Logic and Accuracy tests used to proof and confirm each ballot position were prepared by the Elections Administrator. However, in some counties, especially the larger counties, the complexity of creating a test deck sufficient enough to check all the permutations of voting was often beyond the capability, time constraints, and resources of the jurisdictions. While not the best control, often, larger counties relied on the vendor to provide the test deck. At the time, this was an acceptable procedure. Now we look back and see the flaw in this approach. The vendor was both programming each election as well as creating the testing materials. Let's look at some examples of risks.

Ballot stuffing

The protection against this risk involves comparing the number of signatures on the paper sign-up sheet with the number of ballot records cast on the system, including all storage medium. The protection begs procedures to look at the sign-up sheets even so far as comparing signatures, train election judges, and have multiple political parties represented in the polling place. Often, collusion is the quickest violation to be exposed.

Post-election tampering

Texas, and probably most states, requires a real time audit log at the central counting station. The log records, in real time, every event, tally, correction, and report produced. Such log serves as both a deterrent to improper actions and a record of all actions, which can be publicly reviewed. There should be segregation of duties at every level of election activity, including ballot preparation, equipment preparation and distribution, and set-up of the Central Counting Station.

Hacking

If there is no external communications pathway, then there is no risk of hacking, or gaining unauthorized entry into to the tabulation system. Texas requires the use of closed systems. Most counties do not use modem transfer or only do so from substations, not directly from the polling place. If modem transfer is used, it must be a secured landline with one-time, one-way traffic. The telephone number must be prescribed in advance. It is possible to detect attempts to enter a modem line. Also, the Counting Station should still accept surrender and delivery of the physical medium and compare the tally and number of votes cast on the medium to the modemed results.

Wireless tampering

Again, there is no risk of wireless tampering if there are no external communications pathways.

Trojan Horse/Version control

The risk is that someone could place a different version of the software into the system. Such version may be able to change votes. There are two solutions or mitigators to this risk. First, most DRE systems do not require programming for each election. The software is loaded and never addressed again until time for an approved and supervised upgrade. The Elections Administrator does not have access to the software code. The "programming" of the system for each election is only ballot definition which can be compared to compiling an excel spreadsheet.

Second, it is reasonable to conduct Cyclical Redundancy Checks (CYC), otherwise known as "hash codes". Hash code testing confirms that the certified version and only this coding are contained in the software used to conduct an election.

Inside Job/Hacking

The risk is that a disgruntled former employee of an election vendor, or a temporary or permanent employee of the Election Administrator could gain access and corrupt the system's ability to correctly tally votes. Performed for each election, CYC and L&A testing proof the ballot and increase confidence in the integrity of the system. Using proper locks and seals on the software and hardware, and a tracking system, usually bar coding, increases the probability of proving any tampering or lack thereof. Other controls include procedures that do not allow work to be preformed by a single person. With segregation of duties, all work is done in teams and supervised. Currently, an inside job is perceived as the greatest risk and is also the most difficult to accomplish. Nevertheless, this risk should be taken seriously because although the likelihood of attack is small and chance of detection is high, successful intrusion could be devastating to the true outcome of an election.

Switching or Doubling Votes

After the ballot is compiled and sealed, Logic and Accuracy testing must be done. Referred to as L&A, this testing has long been required for punch-card, optical scan, and other electronic voting systems. L&A testing proofs the ballot and proves that the system

is properly adding votes to each candidate in the same quantity as the votes were manually entered. The system result is compared to a known set of data and must match. L&A testing is the most important tool Election Administrators possess and should be taken very seriously. L&A testing increases confidence that the system properly attributes votes and that the tally will be repeated exactly the same way each time the system is voted.

Omitted or Wrong Candidate

The risk is that inadvertently or deliberately a candidate would be left off the ballot or be assigned to the wrong precinct(s). Logic and Accuracy testing confirms that each candidate appears in the proper precinct, including split precincts, and does not appear in precincts outside that candidate's jurisdiction. Again, L&A testing is the most important tool in confirming that the ballot is correct.

Summary

What risks do we really face? We need further risk assessment. We can rely on tests already performed, but the identified/likely problems and their solutions must be developed specific to each voting system. All the above examples are risks we've anticipated. What have we not predicted?

The greatest point of risk is at the point the ballots are aggregated. Tampering at the precinct level is unlikely, highly detectable, and very decentralized. Affecting a few votes in one precinct would be a violation of basic election principles and not acceptable. However, unless the race affected was extremely close, it is unlikely that tampering with one precinct would change the outcome of an election. The greater risk is at the aggregation point, the Central Counting Station. We need greater protections, including sum checks and other audit procedures at the central counting station level.

What is most important for election administrators and those interested in truly preserving voter confidence are tests, procedures, and audits that prevent any system from being delivered in the field with flawed software. The true goal should be prevention of attack, not detection after the fact. The purpose of a Voter Verifiable Paper Ballot (VVPB) is personal confirmation at the voter level. A VVPB will not mitigate any of the above risks.

Not every voter will want to confirm ballot accuracy. So, at best, VVPB is a sampling approach to detection of errors or problems after the fact. Instead, we need to concentrate on developing stronger prevention and protection methodologies.

Recommendations

- Require use of Cyclical Redundancy Checks or hash code testing and set procedures for conduct and frequency of the tests, especially at the start of the Central Counting Station.
- Require use of Manual Logic and Accuracy testing and set procedures for a sampling approach to conducting the tests.

- Require development and use of automated, high-volume Logic and Accuracy testing and set procedures for conducting the tests on the election system.
- Consider a broader approach to testing before a voting system is deployed, instead of Voter Verifiable Paper Ballot.
- If VVPB or VVAT is adopted, then use a single station approach in the precinct. This will support training of election workers and assistance to voters. It will also offer greater practicality in the field and be more cost-effective to implement.
- Demonstrate the validity of sum checks at the Central Counting Station before tally of the early voting and Election Day ballots.
- Adopt principles of segregation of duties for conduct of the election, including pre-election preparation, conduct of early voting and Election Day, tallying of results, and recounts. Adopt the principles of court evidence for managing and storing ballot documents.