Election-technology Security Basics

Three types of threats: An effective security system addresses all three types of risks (not just Internet hacking):

1. **Manipulation**. All computers are at risk of tampering from both insiders (people who have authorized access to the system) and from outsiders who gain access through the Internet.
   Specific to elections: Election-security experts have concluded that the most likely threat of voting-machine manipulation comes from insiders.
2. **Mistakes**. All computers can produce flawed output as a result of inadvertent human error while programming or operating.
   Specific to elections: The two largest known electronic miscounts in Wisconsin were caused by human programming error.
3. **Malfunction**. Any computer can malfunction at any time.
   Specific to elections: Wisconsin votes have been miscounted due to dust bunnies in poorly maintained voting machines. Outside Wisconsin, elections have been miscounted due to machine overheating and design flaws.

Five components of a security system:

To ensure the threats listed above do not affect the business function (for elections, that is voter-registration rolls and election results), an effective security program must have these five components:

Credit: N. Hanacek, National Institute of Statands & Technology

1. Identify the risks: Managers must identify all the risks they can.
   Vote-tabulation system example: A voting-machine company technician might install unauthorized remote-access software on the central county computer used to program the voting machines.
2. Protect the system: Managers must devise safeguards to protect against the identified risks.
   Voter-registration system example: State of Wisconsin will be requiring multi-factor authentication for administrative users of WisVote.
3. Detect any breaches or failures of the safeguards ('events'): Managers must check the system's business-day functioning to make sure the system is operating as intended.
   Vote-tabulation system example: Use the paper ballots to verify that the computers identified the right winners.
4. Respond to any events that affected the system's functioning.
   Voter-registration system example: Same-day registration at the polls enables incorrectly purged voters immediately to re-register and vote.
5. Recover the system's normal and intended operations by restoring any damaged system components; determining the causes of the event; and improving protection to avoid repetition of the event.
   Vote-tabulation system example: The Stoughton referendum miscount of 2014 should have led to improved training for municipal clerks and improved oversight of pre-election voting-machine tests.