Wisconsin elections depend on two ***entirely*** separate IT systems

If you hear someone talking about 'election security', pay attention to which system they are describing. Security measures that protect one system do not protect the other.

	VOTER-REGISTRATION SYSTEM	VOTE-TABULATION SYSTEM
Name of system	WisVote	Several systems are used in Wisconsin. One, the DS200, counts 60-70% of Wisconsin's votes.
What does it do?	Records voter registrations; keeps them up to date; prints the poll books you get your name checked off on when you vote, among other election-administration tasks	Reads our ballots, counts our votes, determines who wins our elections.
Most knowledgeable source for reporters	WEC is your primary source. They know this system inside-out.	Vendors (ES&S, Dominion, Command Central, and Clear Ballot) are your primary source regarding tabulation-system security. Local election officials know only their own local security practices, which are not the most critical.
Developer	State of Wisconsin; a collaboration between WEC and Division of Enterprise Technology	Any of several private companies; not always the current vendor
Owner	State of Wisconsin	Software is owned by vendors; Hardware is mostly owned by local governments
System updates managed by	State of Wisconsin	Four vendors handle all updates and maintenance; and in all but a few counties, the pre-election programming
Security managed by	State of Wisconsin	**Software security**: Primarily the vendors' responsibility, but local officials have control right before each election and on Election Day. **Hardware security**: Vendors for their computers; county officials for central computers; municipal clerks for voting machines.
General security program	Has all five standard components actively in place: 1) Risk identification; 2) Safeguards; 3) Monitoring to detect events; 4) Response plan; 5) Recovery plan	We have only vendors' assurances about their security practices. Local officials' protective practices are limited to air-gapping, locks, and seals; they rely on minimal, informal detection practices; and they have no specific plans for response or recovery.
Who would know if it was hacked?	The State of Wisconsin, specifically the DET and WEC, continuously monitor all cyber activity, with the assistance of the federal DHS. Voters notice if their registration disappears, but they can re-register at the polls.	We don't know whether the voting machine companies would know if they hacked. Local officials cannot assess their software; hacks wouldn't show up in the pre-election test. Voters have no ability to detect miscounts. WE CANNOT KNOW UNLESS CLERKS AUDIT!
Has it ever been hacked, in Wisconsin?	WEC knows that hackers are always trying and that none have succeeded. Federal DHS has determined that some attempts came from Russia.	No one knows, because no one examines the software (a copy is in every machine), and no one performs routine results audits. There have been electronic miscounts, but none that appear, on their face, to be deliberate.