Portfolio Media. Inc. | 111 West 19th Street, 5th floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Voting Machine Critics Tout Low-Tech Fix For Hacking Fears

By **Shayna Posses**

Law360 (November 6, 2018, 11:37 PM EST) -- Russia's meddling in the 2016 presidential election pushed U.S. voting security into the spotlight, leaving officials scrambling to shore up the infrastructure before midterms. But efforts have been uneven, with a number of states shirking the surprisingly low-tech fix touted by election-integrity experts: paper ballots.

On **Tuesday**, 14 states had voters in some jurisdictions casting ballots with no paper records, with five — Georgia, Delaware, South Carolina, New Jersey and Louisiana — running paperless elections across the board on vulnerable direct-recording electronic machines, according to nonprofit Verified Voting.

These machines, which store votes electronically, have a host of documented problems, ranging from security flaws that make them vulnerable to infiltration to software glitches and hardware issues that can lead to misrecorded votes. With no paper trail, it's hard to detect when something goes wrong and even harder to recover, according to Chris Deluzio, counsel for the Brennan Center for Justice's Democracy Program.

"Without a paper record, it's pretty much impossible to recover lost votes or confirm a tally if the software is corrupted or the data in the machines is lost or otherwise infiltrated by a malware or something else," he said. "That's a pretty sobering fact, that without the ability to audit the paper ballots after the fact, there's really no way to confirm that the tabulations were correct."

Meanwhile, the fear of a hacking attack remains very real, with 67 percent of Americans believing it's very or somewhat likely that Russia or other foreign governments will try to influence the midterms, according to the Pew Research Center.

And that's not unwarranted, according to a Monday report by the Boston Globe revealing that internal government intelligence documents showed more than 160 incidents of suspected hacking into the U.S. election infrastructure since August.

The Drive for Computers

Electronic voting machines came into vogue in the aftermath of Florida's hanging chad debacle, which threw the 2000 presidential race into disarray and triggered a rush to ditch punch card ballots.

Congress' solution was the Help America Vote Act. The 2002 measure poured upwards of $3 billion into replacing punch card and lever machines with updated options, the thought being that "computers that counted our vote would be better," Verified Voting President Marian K. Schneider explained.

The "newest, shiniest voting system on the market" was the direct-recording electronic, or DRE, machine, Wiley Rein LLP partner Lee E. Goodman said, and — according to Verified Voting — by 2006, more than half of all states used them in at least some counties.

But computer scientists had their doubts. They were "the first to understand that without any kind of a paper record of a voter's choices, the voting systems would not be able to be verified," Schneider

said.

That was a major problem because research showed again and again that the machines contained serious vulnerabilities.

The Risks

J. Alex Halderman, a University of Michigan computer science professor and election-security expert, has taken one machine — a Diebold AccuVote DRE, the type used in Georgia — on tour this year to demonstrate just how hackable they are.

Though supporters claim the machines are secure because they aren't connected to the internet, that's simply not true, Halderman said, explaining that they have to be programed with the ballot before the election, which is done on a centralized computer.

"Research shows that if an attacker can infiltrate the election management system for a jurisdiction, then they can very likely spread vote-stealing, malicious software to every voting machine in the jurisdiction," Halderman said. The software can then alter how votes were cast while covering its tracks to avoid detection.

His findings made an impression on at least one observer: U.S. District Judge Amy Totenberg, who is overseeing litigation seeking to force Georgia to switch from the AccuVote system to paper ballots.

Though the judge declined to make the state change course ahead of the midterms, **holding in mid-September** that there just wasn't enough time before voting started, she made it clear that election officials aren't off the hook. Her ruling chastised Georgia Secretary of State Brian Kemp and other officials for burying their "heads in the sand" about the critical cybersecurity issues plaguing their "dated, vulnerable" DRE system, rather than heeding the warnings proffered by Halderman and his fellow experts.

Spokespeople for Kemp, who has faced criticism for staying on as Georgia's top elections official while running as the Republican gubernatorial candidate, didn't return multiple requests from Law360 for comment on the security of the state's voting system — though he did announce Sunday that his office was investigating the Democratic Party for "failed efforts" to hack into the online voter registration system, which the party has vehemently denied.

Still, Halderman said, while DRE systems like Georgia's get a lot of the heat, every model of American voting machine to get rigorously tested over the last decade and a half has contained vulnerabilities that could allow for vote manipulation — including the optical-scanning machines used to tabulate votes cast on paper ballots.

That's why the method for which election-integrity experts advocate is voter-marked paper ballots coupled with post-election audits, Schneider said.

The Solution

Paper may not be the flashiest choice, but it's the best tool out there for conducting reliable and verifiable elections, experts say.

"The only way that we know with current technology to have very strong assurance that an attack on the voting machines can be detected is if we have some kind of physical fail-safe, a form of record that just can't be changed in a cyberattack that we can go back to," Halderman said.

That can take the form of a paper ballot or what's called a voter-verified paper audit trail, which is a receipt printed out by an electronic voting machine to allow voters to verify their selections before casting their ballots and to provide a record for officials to audit.

The preferred choice is a paper ballot marked by hand or with an assistive ballot-marking device, according to Verified Voting, which points to several problems with the paper trail system, including that many voters don't bother checking the printout and that the unwieldy receipt rolls can be hard to audit. Still, Schneider noted, paper ballots aren't enough on their own.

On top of the fact that scanners can be hacked, paper is also susceptible to good old-fashioned cheating, Halderman said. Thus, the other piece of the puzzle is conducting post-election audits that compare the results tabulated by the scanners with the paper records.

Douglas W. Jones, a computer science professor at the University of Iowa and election-security researcher, agreed, explaining that audits are the key to finding discrepancies, whether they're the result of an attack, a machine malfunction or simple human error.

"If you don't do quality control, you won't find the errors, and if you don't find the errors, you can't fix them," he said.

Thirty-three states and Washington, D.C., require post-election audits, according to the National Conference of State Legislatures. But only a few like Colorado and Rhode Island require what Deluzio calls the "gold standard" of audits, the risk-limiting audit.

Deluzio said there's been some "good momentum" around adopting risk-limiting audits, which offer strong statistical proof that an election outcome is right by taking a random sample of the ballots and comparing them with the computer-tabulated results, with the size of the sample fluctuating based on the margin of victory. However, he said, there's a long way to go.

The Wake-Up Call

The push for paper isn't new.

People initially thought those suggesting the move "sounded like Luddites," but states have gradually been going in that direction in the face of growing concerns about electronic voting machines and the proliferation of large-scale data breaches, Halderman said. California, for example, has required elections to have a paper trail since the mid-2000s.

Then came the revelation that **Russia attacked election systems** in 21 states as part of a campaign to influence the 2016 presidential election. The knowledge that the American electoral system is being actively targeted by nation-state hackers drew far more attention to the cause, said Morrison & Foerster LLP partner David D. Cross, who represents some of the plaintiffs challenging Georgia's DRE system.

"It went from being at the time of, for example, the California transition, a fear, a possibility, that by 2016, was clear was a reality," he said.

In the aftermath, everyone from President Donald Trump to U.S. Homeland Security Secretary Kirstjen Nielsen to the National Academies of Science, Engineering and Medicine has called for paper voting records.

And some states have heeded the advice. Virginia made the decision to switch to paper ballots a month before state elections last year, and other states like Pennsylvania — where, according to the Brennan Center, more than 80 percent of voters use DRE machines — have committed to transitioning away from paperless voting in the coming years.

There have also been security strides beyond the physical voting process, experts say, including increased information sharing between federal and state governments stemming from **the January 2017 designation** of the U.S. election systems as critical infrastructure, as well as improvements to many states' voter-registration systems, which were prime targets of Russia's meddling efforts.

As a result, Jason Abel, who leads Steptoe & Johnson LLP's political law and campaign finance practice, thinks the U.S. election infrastructure is better off security-wise going into the midterms than it was last time around.

"But in the 2016 election, we were in an extraordinarily bad place," the attorney said. "So while we are in a better place now, we're not where we need to be."

The Future

Moving from denial about election security concerns to dealing with the problem is certainly a step in the right direction, Jones said. But there's plenty of work left to be done.

Over the summer, researchers at the Def Con hacker conference in Las Vegas **found that** a cybersecurity flaw first discovered more than a decade ago is still plaguing a ballot-counting machine used in nearly two dozen states. Another machine — a DRE used in 18 states, including swing states like Pennsylvania and Florida — could be hacked in two minutes, less than the six minutes it takes an average person to vote, according to the researchers.

Replacing these vulnerable and aging machines needs to be a top priority, Deluzio said, pointing to the Brennan Center's late March report finding that 41 states this year will be using voting systems that are at least a decade old, with even more jurisdictions using equipment that's no longer manufactured.

On Tuesday, voters in states like New York and Georgia were greeted with malfunctioning machines, leaving some waiting hours to cast their ballots.

Earlier this year, Congress appropriated $380 million for election security, which was a great start, but not nearly enough, Deluzio said. Pennsylvania, for instance, received about $13.5 million, a fraction of what the state needs to replace its machines, he noted.

The funding also wasn't coupled with new standards about election equipment or procedures that would ensure the money is well-spent, Halderman said, explaining that many states are using it to maintain their systems and others are holding onto it for the future.

Lawmakers unsuccessfully floated several pieces of legislation this year to require paper records for federal elections, including the Secure Elections Act, which enjoyed bipartisan support and seemed poised to advance — until the Senate Rules Committee canceled the scheduled markup at the last minute.

Strong national leadership on this issue would go a long way, Halderman said. But for now, there's nothing left to do besides wait and see how the midterms played out.

To Halderman, one of the scariest things to come out of the Senate Select Intelligence Committee's May report on the Russian meddling efforts is that the infiltrators were in a position to alter or destroy records when they broke into state voter-registration systems. They simply chose not to.

Speaking ahead of the election Tuesday, he said that if voting systems go unscathed, "it will be because our adversaries decided not to pull the trigger, not because they didn't have the technical ability to pull off a sophisticated attack."

--Editing by Pamela Wilkinson and Orlando Lorenzo.