**Experts: Wisconsin election security bolstered by strong cybersecurity, paper trails, decentralization**

***Editor’s note:****This column is provided to Wisconsin Newspaper Association members by WisPolitics.com. Proper attribution to WisPolitics.com is appreciated. Also, please publish the tagline that is included at the end of the column.*

On the eve of the 2018 midterm elections, computer security specialists from across the country descended on the DEFCON 26 Hacking Conference in Las Vegas. These “white hat” hackers sought to probe the security features of voting machines and election systems in an effort to identify weaknesses. The results were alarming to election security experts.

Hackers at DEFCON’s Voting Village found that an 11-year old trained only in basic coding techniques was able to hack into a mock-up of Florida’s election results website and change its reported vote totals.

Conference attendees were also able to identify a vote tabulation machine — the Election Systems & Software M650 — that could be hacked in under two minutes, or as the report says, “within the time it takes to vote.”

In recent years, Wisconsin’s election security practices have come under scrutiny, most notably by Democrats in the U.S. House Administration Committee, who concluded in July 2018 that Wisconsin was one of the 18 states most vulnerable to cyber attacks on election infrastructure.

But less than a year later and with spring elections on April 2, clerks and administrators across the state felt they were prepared to deal with the growing cyber threat.

“I’m sure everything can get hacked. There’s always a way, but it doesn’t keep me up at night,” said Chris Jenkins, who administers elections for the Village of Elmwood Park in Racine County.

Jenkins’ view largely reflects the consensus of elections officials statewide. Wisconsin has addressed cyber challenges by building an election framework its advocates say is both strong and decentralized, backed by laws that put safeguards in place to ward off bad actors.

Elections security concerns are two-pronged: Experts worry about the security of voter registration systems and vote tabulation devices.

The Wisconsin Elections Commission is the state agency tasked with overseeing the WisVote system. The system was built in-house, from the ground up. Other states use pre-built systems purchased from third-party vendors that have been shown to be vulnerable. The successful hack of Illinois’ election database by Russian operatives in July 2016, for example, was carried out using the same basic technique that the 11-year-old at the Voting Village used to hack a mock-up of Florida’s site.

But Elections Commission spokesman Reid Magney said Wisconsin’s voter registration system would have repelled that attack.

“Our system is not vulnerable to that type of attack, because it’s built on a modern platform, and in addition to the platform it’s built on, the system is protected by the State of Wisconsin’s enterprise firewalls and other security systems,” he said.

Those security features successfully repelled attacks on the state’s voter registration system in 2016. While the WisVote system is externally strong, its large number of users presents a security challenge. Doug Jones, a computer science professor at the University of Iowa who specializes in electronic voting security, noted that by aggregating voter rolls into one central location, potential bad actors are given a central target to attack.

“With so many users on the system, it’s comparable to links in a chain,” he said.

“You’re only as strong as your weakest link.”

But Magney said the Elections Commission has gone to great lengths to strengthen each of those links.

In 2018, the commission received an award from the U.S. Election Assistance Commission for the cybersecurity training it provides to every election official with access to the WisVote system. The training teaches clerks and their staff techniques to browse safely, develop secure passwords, detect and avoid phishing emails and shore up their computers’ security.

Despite all the precautions, there is still a scenario where a hacker gains access to the system and creates discord statewide by deleting voter information.

Even if that were to happen though, state law mandating same-day, in-person registration at the polls would serve as the ultimate safety net, according to Karen McKim, a former Legislative Audit Bureau manager who currently heads up the Madison-based Wisconsin Election Integrity, a nonprofit, nonpartisan group of volunteers that focuses on the election process.

“If you’re sitting in some foreign country or are some nefarious character within the U.S. who wants to mess with some state’s voter registration system, how far down your list is Wisconsin going to be?” she asked. “People can register to vote on Election Day, and if you delete their registration, they can just re-register to vote anyway.”

McKim conceded that could lengthen lines and in turn depress turnout, but it wouldn’t force an election to be called off entirely.

Jones concurred, saying same-day registration coupled with the security features of the WisVote system present a formidable deterrent.

“I don’t know if Wisconsin would be high up on the list of potential targets,” he said. But some raised concerns about the other prong of elections infrastructure: vote tabulation machines.

“Our registration system has wonderful deterrents, but there’s nothing similar for our tabulation system,” McKim said.

Experts have flagged a number of concerns with these machines, ranging from their physical hardware to the way they send and receive data.

In Wisconsin, ES&S and Dominion supply most of the voting machines, but both companies declined to answer questions from WisPolitics.com about their security measures, hiring practices and software.

While a litany of concerns surrounds the voting equipment, state law regulating voting puts several safeguards in place. Under state statute, all voting machines must produce a paper record that allows a voter to verify the choices they make before leaving the voting area. These paper tallies can then be used as a backup in case of a cyberattack or natural disaster. The paper backups are also used for the post-election auditing process that must be completed before the Elections Commission certifies results.

Wisconsin’s decentralized voting administration system also makes it difficult hacking into the machines to manipulate votes. In most states, elections are administered at the county level, or even at the state level in some cases.

“If you go to some states — Maryland and Georgia are famous for this — it’s a centralized system with counties as field offices,” Jones said.

But in Wisconsin, clerks from municipalities small and large independently run their own elections before reporting the data to their county clerks, who in turn report the information to the state.

Despite the safeguards provided by physical paper trails and decentralization, hacking municipalities and counties remains a real possibility. But it would be a complex operation requiring multiple agents on the ground to both compromise the paper trails and hack the transmission of data.

Magney likens a potential hacker’s task to the complex casino heist carried out in the fictional movie “Ocean’s 11.”

“It would take the team from ‘Ocean’s 11’ to be in essentially all 72 counties in the state,” he said. “Not only would you need somebody that had the ability to hack the equipment, but you would need people who could burgle and break into places.”

“It would be very complex to pull off. And then it would be even more difficult to be undetected, because we have the audits after the fact.”

*The Capitol Report is written by editorial staff at WisPolitics.com, a nonpartisan, Madison-based news service that specializes in coverage of government and politics, and is distributed for publication by members of the Wisconsin Newspaper Association.*

*Copyright © WisPolitics.com*