Targeting the biggest cybersecurity threat to voting in the 2020 election

September 17, 2020 10:30 AM Roger Dunaway
roger@tulane.edu
(504) 452-2906

Tulane University cybersecurity expert William “Bill” Rials says cybercriminals could disrupt the election process by targeting voter registration databases and modifying the voter data. (Photo by Shutterstock)

Tulane University cybersecurity expert William “Bill” Rials says cybercriminals could disrupt the election process by targeting voter registration databases and modifying the voter data. (Photo by Shutterstock)

Voting is the staple of democracy and has been done in person in the United States since its founding. While the controversy over the integrity of mail-in votes continues, never in our country's history has voting in person been more fraught with potential security risks that could alter the outcome.

The U.S. has an agency dedicated to protecting the country from cyberattacks and protecting American voters from interference from foreign countries, as was alleged in 2016. The Cybersecurity and Infrastructure Security Agency (CISA) is the nation's primary department tasked with national security related to the internet and technology.

But who protects the voting machines that most Americans use to submit their ballots on election day? According to William "Bill" Rials, an expert and associate director in the Tulane University School of Professional Advancement's Information Technology program, local governments oversee the protection of these machines and their respective databases. They should be acting now to prevent cybersecurity attacks that can disrupt electronic voting.

"From a cybersecurity perspective, the biggest risk to elections is all the ancillary elements associated with the election process," Rials said. "Most voting machines today, from the well-known market leaders, are 'reasonably' secure from cyberattacks because the terminals are typically air-gapped from any connected network during the individual voting process. Any vote cast is usually stored locally and not transferred over a network until after the polls close and the tabulation occurs. One strategy of cybersecurity is limiting the attack surface and exposure to potential cyber threats. Nefarious actors have limited access during the actual casting of votes."

Even if the voting machines are not the primary targets of potential cyberattacks, the real threat is the American public who have registered to vote and are logged in large databases.

"One primary example is the availability and integrity of the voter registration databases on election day. These voter registration databases are typically stored and maintained by county clerks and election commissioners. These databases are susceptible to cyber threats, just like any other database," Rials said.

However, since elections are a constitutional responsibility of state and local election entities that consist of more than 6,000-plus local subdivisions nationwide, election security is not always consistently maintained.

“Unfortunately, many local governments are still struggling to increase their cyber defense capabilities and are easy targets. Cybercriminals wishing to disrupt the election process are likely targeting these voter registration databases months and even years leading up to election day. Incorrect or modified voter data could have an impact on the election process. Local governments responsible for the cyber protection of these databases should be working now to improve the cybersecurity posture associated with the voter databases,” Rials said.

"Cybercriminals wishing to disrupt the election process are likely targeting these voter registration databases months and even years leading up to election day." Tulane professor William "Bill" Rials