Voter Registration Database Security | 2018 Survey

CENTER FOR ELECTION INNOVATION & RESEARCH

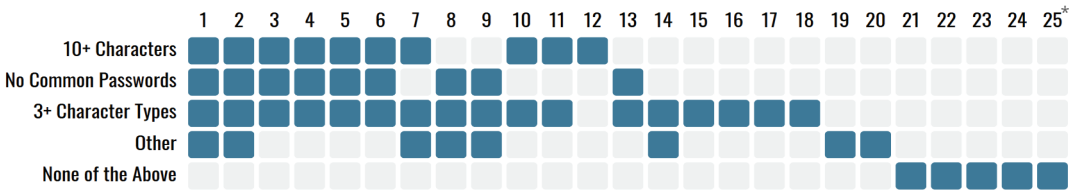
In 2016, several states' voter registration databases (VRDBs) were scanned and at least one was infiltrated. Between June and July 2018, CEIR conducted this survey to learn more about the current state of VRDB security. The survey looked at three major areas of cybersecurity: (1) **prevention**, (2) **detection**, and (3) **mitigation**.

Prevention

ACCESS

Access is the ability to retrieve and manipulate data from a VRDB. All surveyed states effectively **managed user privileges** by limiting access based on users' roles. Many states are also using **multi-factor authentication** and enforcing multiple **strong password requirements**, although more states could improve here.

Password Requirements



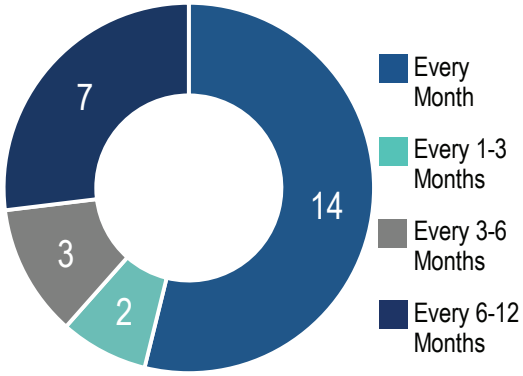
*1 state did not respond due to security concerns with disclosing this information.

13 out of **26** reported using **Multi-factor Authentication** at the time of the survey

SYSTEM INTEGRITY

Promoting **system integrity** means having measures in place to maintain a system and prevent cyberattacks on an ongoing basis. All surveyed states use **HTTPS** on websites with PII. They also have professional **IT support**. The majority of states use **CDNs, DDoS mitigation tools,** or both. And, as shown below, most states audit their VRDB systems monthly.

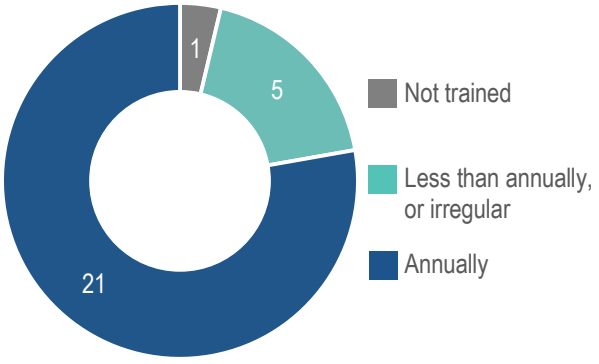
System Audit Frequency



TRAINING

A VRDB is only as secure as its users. That's why **training** is so important. Most states regularly train their VRDB users about cyberthreats, including **phishing**. And a large number of states are using **tabletop exercises** to practice real-world, worst-case scenarios.

How Often Authorized VRDB Users are Trained to Identify Cyberthreats

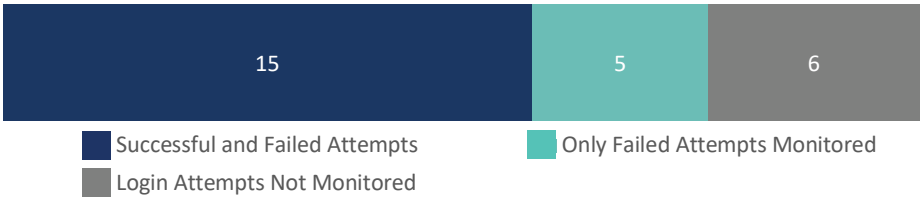


Detection

VRDB Monitoring Solutions*

*1 state returned a partially completed survey that included an answer to this question, so 27 states are represented here.

Login Attempts Monitored & Audited



No system is completely unhackable. That's why it's important to **detect and respond** to threats on an ongoing basis. Fortunately, most states:

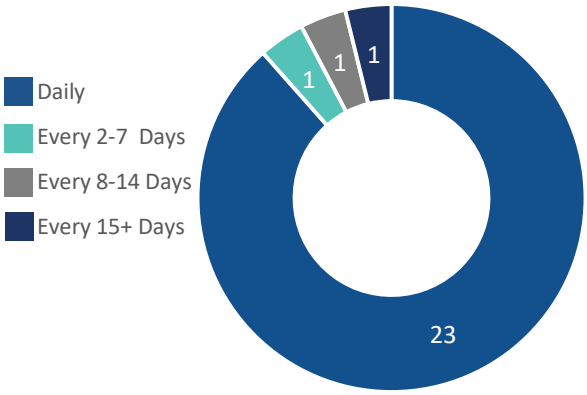
- Monitor **login attempts**
- Audit and monitor **API endpoints and online forms**
- Compare the **volume of VRDB traffic** to historic levels, and
- Use database monitoring solutions, like **Albert sensors**

Additionally, eighteen states have systems that **automatically alert** them about irregular VRDB activity. And half of the surveyed states conduct **VRDB audits** every month.

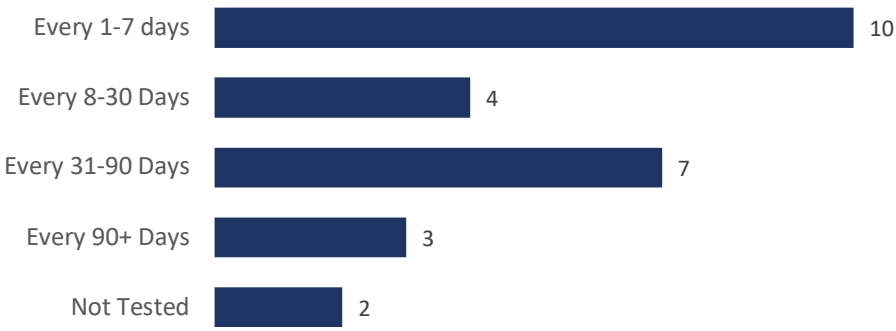
Mitigation

If all else fails and an attack successfully impedes a VRDB, then there must be a plan to **mitigate** the impact. Most states are frequently **backing up their VRDBs** and **testing their backups** to make sure they work. The states are also using a combination of paper pollbooks and backup paper voter lists (in e-pollbook jurisdictions) to make sure voter records are always accessible. And the vast majority of states are ready with **provisional ballots**, as required by federal law.

VRDB Backup Frequency



VRDB Backup Testing Frequency



About the Survey

The survey consisted of 23 multiple-choice questions addressing prevention, detection, and mitigation. It was sent to election officials in all fifty states and the District of Columbia. Of those, twenty-six states returned completed surveys, one state returned a partially completed survey, and three states indicated that they were not permitted to respond.

Learn more at https://electioninnovation.org/2018-vrdb-security and follow us on Twitter @electioninnov.

CENTER FOR ELECTION INNOVATION & RESEARCH