

CASE STUDY
State Government

New Mexico Secretary of State

Improving Voter Access while Minimizing Election Risk

CUSTOMER PROFILE

The New Mexico Office of the Secretary of State is responsible for managing all business services and elections for the state. Its Bureau of Elections administers and enforces all local, state, and federal election laws. The New Mexico Secretary of State Information Systems Division maintains the Secretary of State's computer systems, and assists the Bureau of Elections with the management of the voter registration and election management systems.

"RiskSense has partnered with us over the last seven years—enabling us to continuously assess vulnerabilities and threats to reduce cyber risk exposure and increase the security of our valuable election ecosystem."

*– Kari Fresquez,
CIO and Elections Director,
New Mexico Office of the
Secretary of State*



THE CHALLENGE

Kari Fresquez has been with the New Mexico Secretary of State's Office since July 2011 and is currently the State Elections Director and Chief Information Officer. During her tenure, she has led significant system modernization and automation efforts, with a focus on bringing more services and information online.

"We have a relatively small team of IT and security professionals," Fresquez said. "They are all extremely skilled at what they do and work very hard, but there's always more work than IT admins in our department. Some people assume we're only busy on election day, but we are busy all year round making improvements, protecting our systems, and managing all of the data we continually receive."

New Mexico Secretary of State's Office relies upon a collection of interconnected IT systems from multiple hardware and software vendors. "Our biggest challenge is balancing the need to improve site security while facilitating voter access," explained Fresquez. "Those are two equally important—but often conflicting—operational and IT goals. Election security can never be compromised, but we also want to enable greater ballot access to all New Mexico voters."

Defending Against Foreign Actors and Adversaries

One of the biggest issues facing New Mexico Secretary of State's Office is the increased threat of 'foreign actors' that could potentially affect election outcomes. "Many view this threat as a 'new thing', but we've been bolstering ourselves against it for quite a while," Fresquez said.

"Election tampering has risen to a higher level of public visibility recently, due to increased coverage in the media. This definitely places an extra burden on state election officials, since we're answering to a lot more people. But it also creates an opportunity for us—the added visibility has opened more people's eyes to the importance of technology in minimizing election risk. It also means we're going to have support from a broader ecosystem of partners that actually understands the unique nature of IT systems in the context of elections."

Increasing Online Voter Registration and Reduce Voter Fraud

New Mexico Secretary of State's Office's IT department also provides and supports the systems for online voter registration and voter eligibility. "The benefits of having online voter registration for the electorate and to the

The RiskSense Platform safeguards election systems.

administrators of elections far outweigh the risks it introduces. It makes voter registration accessible and easy for all of our citizens. We also get better quality data, because we can walk a voter through the process line by line and catch errors before they get submitted, as opposed to the old way of accepting paper forms that are possibly illegible or incomplete, and therefore invalid." Integration with other systems of record, including the Motor Vehicle Department, allows for proper validation and eligibility of the voters and prevents fraud.

Maintaining Chain of Custody

In addition to ensuring security, the New Mexico Secretary of State's Office elections team faces other IT challenges. "We have to build up temporary networks at each of our polling locations, and then tear them down immediately after the election," noted Fresquez. "There's a lot of equipment, different people at each site, and multiple vendors involved in that process. Maintaining 'chain of custody' processes and documentation is essential to make sure that the systems aren't tampered with as they are moved."

The mock election logic and accuracy testing of all equipment before every single election takes several weeks to complete, according to Fresquez. "We have to program the voting machines to correctly read the ballots and ensure the vote results are being read correctly. We also plan ahead and prepare contingencies for any possible glitches or things that could go wrong. There's a lot of coordination across all election officials, including poll officials, county clerk officials, and their staff, and we must accomplish everything within a short amount of time. It's a complex process for each election, and ensuring security is no small task."

THE SOLUTION

The New Mexico Office of the Secretary of State decided to use RiskSense to provide a 'continuous attacker's view' of the organization's attack surface and cyber risk exposure. This allows the state to proactively understand attack susceptibility, validate whether vulnerabilities are exploitable, confirm that the current security controls can prevent an attack, and quantify (risk scoring) risk based on diagnostic and operational data.

RiskSense Platform

RiskSense is disrupting the cyber risk market with its Risk-as-a-Service based platform. The intelligent platform uses domain expertise and data in ways that are beyond human cognition to correlate vulnerability data with threat intelligence and business impact to measure risk, provide early warning of weaponization, predict attacks, and prioritize remediation. RiskSense is empowering its customers to reduce vulnerability fatigue, improve efficiency, and quantify risk based on diagnostic and operational data.

The RiskSense Platform ingests data from a variety of security and IT tools, as well as outside threat data feeds. Ultimately, it preserves existing technology investments and enhances their value by automating data aggregation, correlation, and normalization processes. The result is a contextualized, risk-based view of an organization's cyber security posture, allowing security and IT teams to collaborate and move from detection to remediation in minutes, not months.

Proactively Addressing Risks and Vulnerability Prioritization with RiskSense

New Mexico Secretary of State's Office uses the RiskSense platform and performs security posture assessments and penetration testing of its Election Ecosystem, which includes all connected IT systems managed and co-managed by the New Mexico Secretary of State's Office, Voter Registration System, Campaign Finance System, Election Management System, and the partner-built and hosted applications that support the elections.

As a best practice, New Mexico Secretary of State's Office uses RiskSense to provide AI-assisted penetration testing to validate the security controls of all in-house and partner (vendor) developed web applications before they go into production. The RiskSense platform:

- Provides visibility, prioritization, and actionable remediation recommendations to shrink the attack surface and overall cyber risk exposure;
- Enables detailed attribution of all critical vulnerabilities mapped to known exploits, malware, and exploit pulse, presented with detailed remediation action plans;

- Performs Attack Surface Validation (penetration testing);
- Identifies the vulnerabilities that are mostly likely to be used by adversaries to carry out infiltration and utilizes post-exploitation techniques to launch a successful lateral attack across the enterprise; and
- Quantifies and measures resilience against cyber-attacks by validating the attack surface and its susceptibility to attacks.

THE RESULTS

Gaining Visibility across the Election Infrastructure and Obtaining Informative Reports

Fresquez has been very impressed with the reporting capabilities of the RiskSense solution. "I like the way RiskSense packages and reports on vulnerability assessments and the penetration test results," she said. "It's easy to track how we're trending from one month to the next, to see if we're making improvements or if we're neglecting something. I like the risk context, clarity, and consistency I get in the RiskSense reports, and the ability to compare data between each assessment."

Getting Other Vendors to Assess Risk in Their Solutions

New Mexico Secretary of State's Office is now requiring all of its technology partners to address any high vulnerability items within their solutions. "We are asking our software vendors to perform and submit to an application assessment before we accept their solution into our system," noted Fresquez. "With

RiskSense penetration testing, we now have an 'independent set of eyes' that enables us to triple-check the solutions and find any vulnerabilities. All of our vendors have been responsive to this request, and they are working hard to fix any issues in their solutions. They realize that the RiskSense penetration testing results enable them to improve their own products."

NEXT STEPS

New Mexico Secretary of State's Office replaced and modernized the IT business filing components for the Secretary of State's Office in 2011. Once that project was finished, they moved on to the election system replacement, and are now commencing on a third modernization effort for campaign financing. "Our new IT system for campaign finance is being designed now," reported Fresquez. "Before we move that application into production, we'll ask RiskSense to do an assessment and identify any vulnerabilities. RiskSense has partnered with us over the last seven years—enabling us to reduce IT risk and increase the security of our valuable election systems."

WHY RISKSENSE

RiskSense as a partner, supported New Mexico's Secretary of State's need to improve the security of its election infrastructure and voting system security by:

- Performing a security risk and vulnerability assessment of the state's election infrastructure which is carried out by a provider of cybersecurity services
- Assisting with the prioritization and the maintenance of election infrastructure, including addressing risks and vulnerabilities which are identified under the security risk and vulnerability assessments
- Providing increased technical support for any information technology infrastructure that the chief state election official deems to be part of the state's election infrastructure or designates as critical to the operation of the state's election infrastructure
- Enhancing the cybersecurity and operations of the information technology infrastructure
- Improving the cybersecurity of New Mexico Secretary of State's Office's voter registration systems



Contact Us Today to Learn More About RiskSense

RiskSense, Inc. | +1 844.234.RISK | +1 505.217.9422 | info@RiskSense.com

© 2018 RiskSense, Inc. All rights reserved. RiskSense and the RiskSense logo are registered trademarks of RiskSense, Inc.

CONTACT US

SCHEDULE A DEMO

READ OUR BLOG

CaseStudy_NewMexicoSecretaryofState_8012018