Securing Future Elections

VETTING STRATEGIC PARTNERSHIPS USING LESSONS FROM THE 2020 GENERAL ELECTION

By: Mike Wons, *President*
Calvin Simmons, *Chief Information Security Officer*

2020 tested election officials on every level. Voter turnout was at its highest in over a century, shattering records in almost every state across America and taxing election processes made even more vulnerable by a pandemic.[1] Those responsible for administering elections had months to pivot strategies to accommodate the safety of their constituents, and they had no playbook. Cybersecurity threats were unrelenting in their attempt to infiltrate state and local databases, and yet the 2020 General Election was the most secure in US history.[2]

How was this possible? One advantage of successful states was the partnerships they relied on to extend their teams' limited resources and help secure their elections. By looking at the successes of 2020, states can enhance their own strategic partnerships to better prepare for future elections.

1. CYBERSECURITY STAND OUTS

Partners that claim to have impenetrable systems and perfect records may seem like the obvious choice. But with highly sophisticated techniques, malicious actors can exploit almost any network. States must rely on technology partners with formal security policies that demonstrate what kind of assurances they can make regarding the protection of their applications.

Formal security policies establish goals and provide mechanisms that identify gaps, providing a clear roadmap for their efforts. Detailed policies should align with the NIST Common Security Framework. Though this is a tedious process, it pays dividends when considering the costs of a cybersecurity attack. Because an effective security program is always maturing, vendor policies and playbooks should show signs of regular monitoring to confirm all efforts are on track and current.

2. HONESTY WAS (AND IS) THE BEST POLICY

Ensuring election security requires an honest assessment of an agency's IT systems and potential vulnerabilities. Common frameworks, testing, audits, and third-party certifications can help.

Technology partners that undergo independent, outside assessments (i.e. NIST) and build on platforms that are SOC 2 and FedRAMP certified can provide client states with verified audit results that provide an honest assessment of the security posture. Other best practices include penetration and malicious behavior testing employed by vendors early in their development processes. These practices reveal vulnerabilities and catch potential issues before they become problems.

Vendors, eager to win business, should be able to provide evidence of independent testing, audits, and certifications to back security claims, and client states, counties and cities should demand it.

3. MOVING IN-PERSON TO ONLINE

2020's obstacles forced some states to adopt technology that alleviated the burdens of in-person voting practices and increase voter confidence. While the introduction of absentee ballot software was initially politicized, the technology worked. States that allowed voters to apply online for absentee ballots eliminated the need to download and mail paper forms, cut the potential for delays in mail delivery, and guaranteed that the information provided by voters was accurate.

IT modernization also meant greater transparency in the election process – a key element to voter confidence. Technology that allows voters to track their registration and ballots in real-time builds trust in election systems and reinforces the ideal that every vote counts and that every vote was counted.

Transparency also extends to election results. Election night reporting tools give constituents access to election results in real-time. Sharing this information as vote tallies are posted demonstrates that the tabulation process is fair and verifiable and gives confidence in the election outcome.

While COVID-19 may have precipitated the desire by many to vote from the safety and privacy of their own homes, it's likely this trend will continue beyond the pandemic. State legislatures and elections officials that can move quickly to facilitate remote voting practices will be better positioned to meet this demand in the future.

4. THE FUTURE IS IN THE CLOUD

The Cloud brought a host of benefits to state and local governments in 2020, saving costs and reducing demands on in-house IT staff by making technology solutions accessible to verified users anytime, anywhere. It ensures data is protected with high levels of security and when configured correctly with redundancy it allows for quick recovery following a disaster regardless of the conditions on the ground.

When choosing a Cloud partner, states should look for size and scale. Dedicated configurations leverage the elasticity of scale and provide a higher level of security. And having multiple geographic data centers means systems remain available across various zones.

Some providers offer Cloud environments built specifically for government agencies. These Cloud infrastructures are purpose-built for SOC 2 and FedRAMP High compliance, giving states the peace of mind that their hosting environment meets the most stringent U.S. government security and compliance requirements.

5. PREPARE FOR THE WORST

Most important is to prepare and expect bad things to happen and expect them to potentially get worse if your partners aren't prepared. Vendors tasked with carrying out critical election missions should provide detailed policies around preparedness and response. These can include:

- Automated provisioning environments that take human error out of the equation
- Policy based automated deployments based on best practice security principles
- 24/7/365 continuous monitoring of event data
- Best of breed, always on security tools to provide 360 degree security services

Even with highly prepared systems, it is necessary to have robust response capabilities. An incident response plan is a must and will prioritize and order actions but it requires experienced GovTech Incident Management professionals capable of implementing them.

SUMMARY

Today's computing environments are complex and will continue to get more complex as new legislation is mandated to improve accessibility, validity, security and transparency. Having a strong partner eco-system is the only way to survive and deliver peace of mind that every vote is valid and every vote is counted.

LEARN MORE

Civix is a trusted software provider on a mission to transform the public sector.
For more information, visit gocivix.com or contact solutions@gocivix.com and 888-GOC1V1X.

TEAM BIOS

Mike Wons is the President of Civix Government who served as the former first ever statewide CTO for the State of Illinois. Mike is an active member in ISACA and has worked with GovTech companies for the past 25 years solely focused on helping Government build out robust solutions that remove friction, improve accessibility and create a framework for trust and transparency in computing platforms for the future.

Calvin Simmons is the Chief Information Security Officer for Civix. Calvin is a Certified Information Systems Security Professional (CISSP) and has a Master of Science in Cybersecurity with over twenty years of IT and Security experience. He presents regularly at InfoSec conferences.

[1] Source: https://www.washingtonpost.com/graphics/2020/elections/voter-turnout/

[2] Source: https://www.cisa.gov/news/2020/11/12/joint-statement-elections-infrastructure-government-coordinating-council-election