SECURING ELECTIONS CRITICAL INFRASTRUCTURE

PRACTICAL ADVICE FOR VENDED SOLUTION SELECTION

A GCR COMPANY

The Vermont Secretary of State was faced with a challenge. Like many central election offices across the country, the state of Vermont's voter registration and election management systems are automated and networked. While this provides tremendous efficiencies, it may expose the state to a risk of cybersecurity breach. That risk became real for Secretary Condos in 2018, as he prepared his state for midterm elections that promised to turn out record numbers of voters.

According to reporting by Pete Williams and Ken Dilanian of NBC News in their October 15, 2018 coverage captioned, *"DHS Finds Increasing Attempts to Hack U.S. Election Systems Ahead of Midterms"*:

> *"We are aware of a growing volume of cyber activity targeting election infrastructure in 2018," the [US Department of Homeland Security's] Cyber Mission Center said in an intelligence assessment issued last week and obtained by NBC News. "Numerous actors are regularly targeting election infrastructure, likely for different purposes, including to cause disruptive effects, steal sensitive data, and undermine confidence in the election."*
>
> *The assessment said the federal government does not know who is behind the attacks... The techniques used by the hackers are available to nation-state and non-state hackers alike, DHS said, including malicious e-mails that appear to be legitimate and denial of service attacks. The attempted hacks have been intensifying and were detected as recently as early October.*
>
> *For example, the assessment said, three different methods were used in late August in an attempt to get access to Vermont's online voter registration database, but they were unsuccessful.*
>
> *Vermont Secretary of State Jim Condos confirmed that account, which had not been previously reported, describing it Monday as the kind of attempted hack that states face every day.*
>
> *"The good news is that our defenses are robust, were in place, and did their job," he said in a telephone interview. The voter registration list is backed up every day, Condos added, "so if it were somehow to be breached, we would just go back 24 hours and reset it. We'd only lose one day's worth. And we also have same-day voter registration, which means that no one would be denied on election day."* [i]

Secretary Condos was prepared. His office implemented reasonable measures to combat cyberattacks and those measures worked.

Vermont also advanced precipitously from #38 in 2012, to #16 in 2014, and to #1 in 2016 (the last year indexed to date) for United States election administration performance, according to the scientifically researched Massachusetts Institute of Technology Elections Performance Index (MIT EPI). [ii]

THE PROBLEM

The Help America Vote Act of 2002 (HAVA) required each state, acting through its chief election official, to "implement, in a uniform and nondiscriminatory manner, a single, uniform, official, centralized, interactive computerized statewide voter registration list defined, maintained, and administered at the State level that contains the name and registration information of every legally registered voter in the State and assigns a unique identifier to each legally registered voter in the State." [iii] The pressing goal that led to the passage of HAVA was to minimize disenfranchisement and promote citizen participation in elections. The landmark legislation was predicated on the fact that automating voter file administration poses tremendous advantages in terms of efficiency and auditability.

AUTOMATION PROVED TO BE A DOUBLE-EDGED SWORD, HOWEVER, AS THE RISK INHERENT IN CENTRALIZING AND AUTOMATING VOTER RECORDS AND ELECTIONS PROCESSES HAS BECOME MORE APPARENT IN RECENT YEARS.

Press accounts since 2016 have exposed potential vulnerabilities in the electoral systems of the United States. That year, the U.S. Department of Homeland Security (DHS) uncovered cyberattacks that attempted to breach the elections systems of 21 states. While none of those attempted hacks penetrated systems in such a way as to alter voter records or election processes, they served as a wakeup call to the country that the proverbial barbarians are at the gate.

> *"The American public's confidence that their vote counts—and is counted correctly—relies on secure election infrastructure" -* ***Kirstjen Nielsen, Secretary of Homeland Security*** [iv]

In 2017, DHS intervened and exercised federal power to assert a degree of influence over state-run elections when it officially classified elections infrastructure as a "critical infrastructure." Not without controversy, DHS deemed such action was warranted based on the prevalence of the cyber threats and the harm such threats posed for our democracy and our overall security and safety. The "critical infrastructure" designation meant that DHS recognized elections systems as being so vital to the United States that the incapacity of such systems would have a debilitating impact on national security, safety, and health. The Department cited cyberattacks on American systems as potentially more sophisticated and dangerous than ever, and elections as a primary target of cyber criminals.

THE SOLUTION

GOOD NEWS

Despite the scary nature of the threat, there is encouraging news. The implementation of well-designed software deployed and supported by a vigilant vendor partner enables states to continue to benefit from technology while limiting their risk to a tolerable level.

To help protect our elections infrastructure and provide for the continuity of our democracy, DHS has staked out a position of partnering with states, rather than imposing a federal legal framework that infringes on states' rights. According to DHS:

> *Securing election infrastructure is a partnership between federal, state and local government and private sector entities. DHS collaborates with federal departments and agencies, state and local government, election officials and other valued partners such as the National Association of Secretaries of State, National Association of State Election Directors, International Association of Government Officials, National Association of Election Officials and the Elections Assistance Commission. In partnering with these officials through both new and existing engagements, DHS and the involved partners both in the public and private sector are enhancing efforts to secure election systems.*[v]

PARTNERSHIP WITH THE PRIVATE SECTOR: *CAVEAT EMPTOR*

Many states do not appropriate sufficient funds to allow the chief election official to carry a robust IT staff that can continually retrain on ever-evolving security threats and countermeasures. Generally speaking, the private sector provides a more conducive environment to grow and maintain a workforce that is capable of developing domain expertise on a continuing basis. As a result, many states naturally elect to engage vendors to supply their elections infrastructure. While this arrangement has served states well, offloading mission critical functions to a vendor is not without risk.

CAVEAT EMPTOR: SELECTING THE RIGHT VENDOR AND THE RIGHT SOFTWARE IS CRITICAL TO THE OVERALL SUCCESS OF A STATE'S ELECTION SYSTEM

States in the market for vended voter registration and election management software systems (VR-EMS) must abide the ancient admonition of *caveat emptor*; let the buyer beware. Selecting the right vendor and the right software is critical to the overall success of a state's election system. This paper recommends qualities to demand in a vendor and in a vended software solution that can most effectively mitigate the risk associated with cyberattacks on election critical infrastructure (NB: This paper is addressed to VR-EMS software and does not seek to address voting systems and voting technology.).

Once a state determines its needs would be best met by a vended solution, success rests on two critical pillars:

1. The vendor must possess a complete understanding of the cybersecurity threats facing the elections domain and exhibit a firm commitment to deploying cybersecurity best practices; and
2. The software itself must be purpose-built to withstand the kinds of cyberattacks that prevail, while also being flexible to ward off ever-evolving threats.

THE RIGHT VENDOR

Effective technological mitigation and prevention of cyberattacks begins with a thorough understanding of the business cases that have helped shape national security policies and standards. This policy-driven approach to securing a system ensures that the technology is informed by industry consortiums and best practices that have been vetted and evaluated by a broader business and security industry. The National Institute of Standards and Technology (NIST) and the Center for Internet Security (CIS) lead the industry, in concert with DHS, in establishing elections cybersecurity best practices. Continual participation in efforts to develop industry best practices and to share threat information through established industry networks can aid a vendor in anticipating threats and mitigating conditions that could otherwise lead to the next vulnerability.

IT IS IMPORTANT TO PARTNER WITH A VENDOR THAT PARTICIPATES IN THE DHS SECTOR COORDINATING COUNSEL, AND WHO SHOWS A COMMITMENT TO LEADERSHIP IN THE INDUSTRY.

In addition to its commitment to continual education and security threat research, a strong vendor partner will be able to offer heightened security and performance monitoring of the following:

- Application
- Database
- Security
- Network
- Storage
- Virtualization

A good vendor will perform patches on a regular basis to fend off ever-evolving vulnerabilities. Patches should be conducted to address browser upgrades, defect fixes, and upgrades to the most stable, current version of an operating platform (ex .Net, Java).

THE BEST TECHNOLOGY IN THE WORLD IS NOT HELPFUL IF IT CANNOT BE MAINTAINED DURING SINGULAR ELECTION EVENTS. THERE ARE NO DO-OVERS IN ELECTIONS

The best vendor partner will have the resources to provide an excellent, multi-tiered support contract, to conduct training and retraining as necessary, and to cover election and other high-volume periods with adequate staffing. Seek out a vendor with dedicated, knowledgeable support staff who will not be learning on the job on election day.

THE RIGHT SOLUTION

Finding a strong vendor partner is only half the battle. This section offers specific recommendations to ensure that a software system meets best practices and will mitigate your risk to an appropriate degree.

First, vended voter registration and election management software systems should incorporate industry best practice standards into their design. Such standards should be inherited from, or informed by the following:

- NIST SP 800-63, 800-53
- EI-ISAC Election Infrastructure Security best practices
- SOC-2 Type 2 and FEDRAMP compliance
- National Association of Secretaries of State (NASS) best practices and continuing education efforts
- National Association of State Election Directors (NASED) best practices and continuing education efforts

This document is solely owned by PCC Technology Inc. and is for the exclusive use of recipients PCC has provided this document. This document contains copyrighted and otherwise protected information which is confidential and proprietary to PCC. This document may not be copied, distributed, used to create derivative works, or otherwise misused without the prior written consent of PCC Technology Inc.

- Council on Governmental Ethics Laws (COGEL) best practices and continuing education efforts

A STRONG SOFTWARE SOLUTION WILL EMPHASIZE FRONT-END SECURITY IN ITS VERY ARCHITECTURE AND DESIGN, AS MOST ATTACKS APPROACH THROUGH THE WEB.

Next, a vended solution must provide three-tiered protection, deploying security in the Web tier, the Application tier, and the Database tier. Such protection should include the following:

- Role-based system access for various classes of users
- Strong Password technology
- Two-factor/Multi-factor Authentication
- Application Whitelisting
- IP Address Whitelisting
- Vulnerability/Pen Testing (DAST's – Dynamic Application Security Tests)

At the Server level, the solution should employ a Least Privilege server management access model.

At the Database level, automated Log Analysis tools should be incorporated to sweep for unusual activity and red flag system monitors. The database should employ Direct Access Restriction to limit management-level access to those individuals who have a business need to access the database. Also, the system should protect PII (Personal Identifying Information) and be flexible to meet the particular state's PII laws.

A HEALTHY SOLUTION FROM AN ARCHITECTURAL PERSPECTIVE IS ONE THAT SHOULD BE ABLE TO OPERATE EQUALLY WELL WHETHER DEPLOYED ON A MAINFRAME, IN A VIRTUAL SERVER ENVIRONMENT, OR IN THE CLOUD.

At Data Exchange Interfaces with external systems, the solution should employ:

- Dedicated Service Account integrations rather than Named User Account integrations
- Secure FTP (SFTP) that enables access logging, whenever file exchanges are needed
- Data Encryption for data at rest (Transparent Data Encryption – TDE), as well as data in transit (TSL/SSL Certificates, and HTTPS)

The network should be guarded utilizing the following protections:

- WAF Firewall
- IPS/IDS Monitoring Service (for centralized monitoring and endpoint reporting)
- Albert Sensor to monitor traffic and report malicious attempts
- Data Segmentation that allows PII to reside in a dedicated zone isolated from the Web
- TLS 1.2 Encryption

The suggestions above should be viewed as a starting point. States should take care to follow trends and include newer mitigation techniques and technologies in the Requirements sections of their procurement documents (assuming those advancements are vetted and proven).

A STRONG VENDOR AND A WELL-DESIGNED SOLUTION WILL BE CAPABLE OF ACCOMMODATING SYSTEM DESIGN AND ENHANCEMENT TO INCORPORATE NEW METHODS AND TECHNOLOGIES.

CONCLUSION

When it comes to guarding against cyberattacks in the elections critical infrastructure realm, all the emphasis is placed on technology. The perception is that "the technology failed" whenever a breach occurs. Nevertheless, it is important to recognize that the key to mitigating cybersecurity risk is to select not only superior technology, but also a superior vendor to design, implement, and support that technology (with adequate domain-experienced staff to cover election periods). Your defenses are only as strong as the weakest link in the chain. When addressing a mission critical need for voter registration and election management software, build best practice standards into your RFP and select a partner with the strongest solution-vendor combination.

[i] NBC News, **https://www.nbcnews.com/politics/national-security/dhs-finds-increasing-attempts-hack-u-s-election-systems-ahead-n920336** (October 15, 2018).

[ii] Massachusetts Institute of Technology Elections Performance Index Website, **https://elections.mit.edu/#indicator** (January 4, 2019).

[iii] US Election Assistance Commission Checklist for Securing Voter Registration Data, US EAC Website, **https://www.eac.gov/documents/2017/10/23/checklist-for-securing-voter-registration-data/**, (October 23, 2017).

[iv] Graphic citation: US Department of Homeland Security Website, Election Security page, **https://www.dhs.gov/topic/election-security** (December 21, 2018).

[v] US Department of Homeland Security Website, Election Security page, **https://www.dhs.gov/topic/election-security** (December 21, 2018).

This document is solely owned by PCC Technology Inc. and is for the exclusive use of recipients PCC has provided this document. This document contains copyrighted and otherwise protected information which is confidential and proprietary to PCC. This document may not be copied, distributed, used to create derivative works, or otherwise misused without the prior written consent of PCC Technology Inc.

READY TO INNOVATE?

Call now for a demo or for additional info:

860.242.3299

Our aim is to develop, implement, and support advanced automation solutions that assist agencies in achieving maximum efficiency, while driving unprecedented levels of transparency and public access to data. PCC is experienced in working with state clients to design, implement, and maintain effective election solutions across the country.

A GCR COMPANY

PCC Technology Inc.
100 Northfield Dr., Ste 300
Windsor, CT 06095

PCCtechnologyinc.com
info@pcctechnologyinc.com
t: 860 242 3299