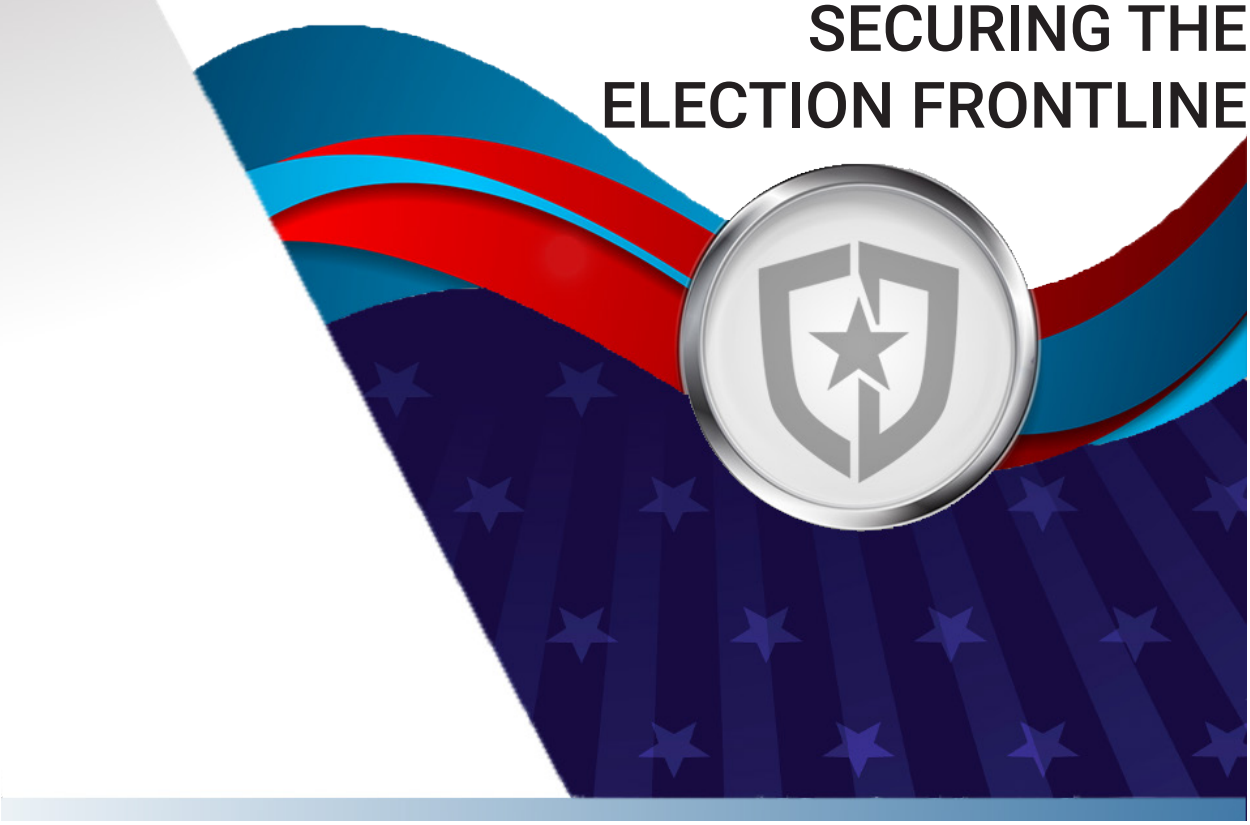
CYBERDEFENSES

SECURING THE ELECTION FRONTLINE



RESPONDING TO THE URGENT NEED FOR STATES TO TRANSFORM SECURITY CULTURE AT THE COUNTY LEVEL

Securing elections against cyberattack has been top of mind and top of the headlines in recent years. Federal and state leaders are taking significant steps to secure election infrastructure. While these advancements are securing centralized state and federal operations against relentless cyberattackers who continuously work to infiltrate and affect elections, most states are still challenged with updating security where it can be most exposed, at the election frontline — the county.

Cyberattackers will always target the weakest link in the election process, and too often that weak link is a county. Every county that uses technology or the Internet, including the day-to-day use of email, can present an avenue of attack that a threat actor can exploit. Without significant focus and effort to increase defenses at the local community level, counties can become an attacker's way into the infrastructure of the entire state.

Unfortunately, the urgency to secure all points of attack is growing as the motivation for disrupting elections, affecting results, and stealing voter data increases. A larger number of attackers seek political or financial gain by infiltrating elections. Nation-state attackers are creating chaos by influencing results and casting doubt on election operations.

Similarly, domestic activists want to undermine the democratic process to advance their cause, and local activists attack the elections in their region to skew voting results and cause embarrassment in support of their political cause or for monetary reward.

While local officials have always worked diligently to secure elections, it is now even more imperative that they drive transformation of culture, processes and tools to constantly protect the election from cyberattack. A single product or cookie-cutter effort that doesn't factor in the unique political, economic and geographic environment of each county is not enough. Adequate security in today's climate of dynamically evolving attack methods and motivations requires a new mindset that acknowledges the heightened threat to our democracy. It demands an approach that integrates county-specific security knowledge, methods and tools into the election process and team culture at the local level.

EFFECTIVE ELECTION SECURITY TRANSFORMATION MUST BE PERVASIVE ACROSS THE ENTIRE ELECTION PROCESS

In the past, election security was predominantly centered on securing voting machines or tabulation systems, but it is a mistake to only focus on securing voting technology. The reality is cyberattackers infiltrate elections using a variety of different methods across the entire election process (see Figure 1).

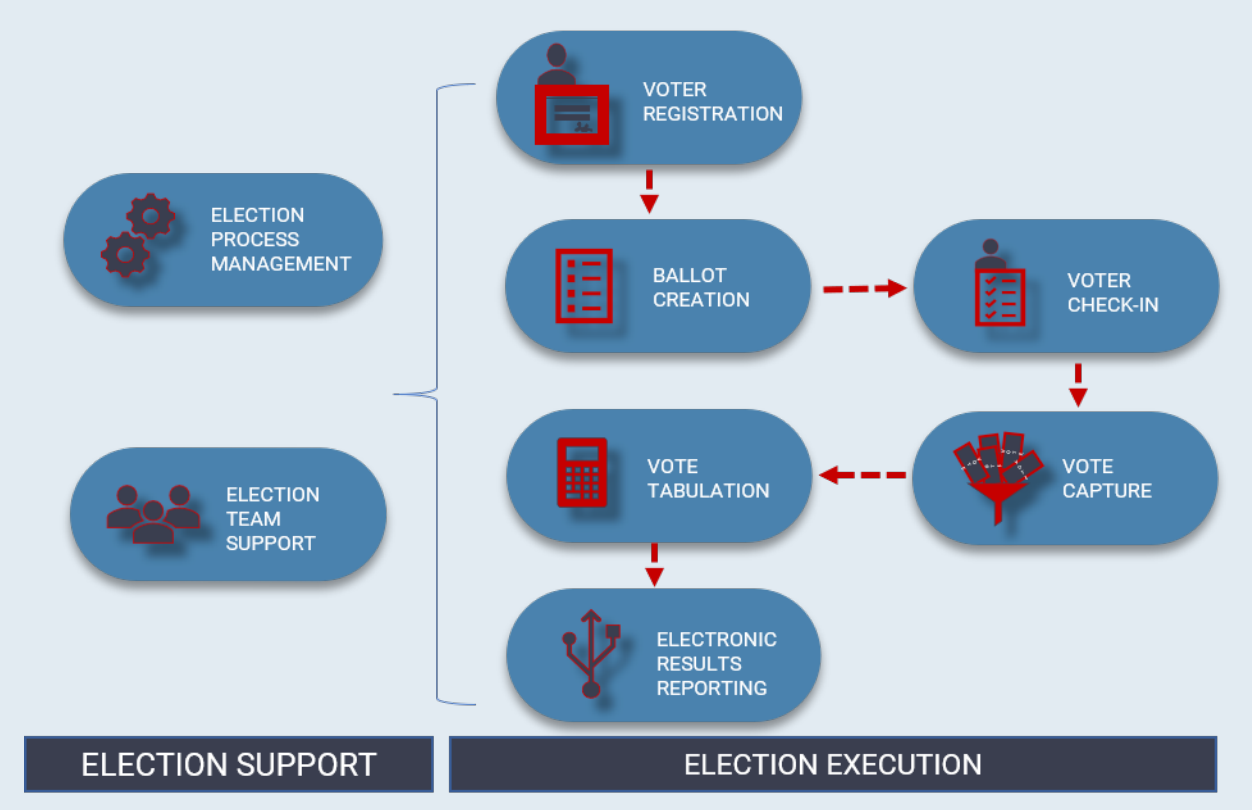


Figure 1: *Supporting and executing elections is a multi-faceted process that presents opportunities for attack and tampering at many different points.*

For example, an attacker could purchase an election administrator's login credentials from the Darknet. Armed with this data, the attacker can access the county network, the voter registration database or potentially the administrator's vendor accounts. Or an attacker could use a stolen email address to execute a phishing attack. By pretending to be an election volunteer's supervisor, they can gain access to the volunteer's computer and install malware that locks down access to important functions enabling the attacker to demand a ransom.

From the moment a voter registers or a candidate files until the election results are certified and published at the state and federal level, there are many points where data or voting functions, if not protected, could be intercepted or tampered with, online or physically. Effective security goes beyond securing voting machines and tabulation systems to include every aspect of the election process.

THREE ELECTION SECURITY INITIATIVES AT THE CENTER OF STATEWIDE CULTURAL TRANSFORMATION

The most effective county-level security initiatives are those that are organized from state election leadership to encompass all counties and the entire election process. This approach avoids inconsistent efforts and gaps that can leave points of attack exposed. Statewide election security uniformly implemented at the county level is attainable when state election officials clearly define the elements of effective security. By delineating a clear path that county election teams can follow, local communities can strengthen their security across the people, places, processes and technology associated with each aspect of their election infrastructure.

There are a multitude of different approaches, tactics and tools that election leaders can employ to improve security. Focusing on the following three key initiatives creates the strongest security programs. By putting a structure in place to achieve these three initiatives simultaneously, states can empower counties to aggressively and efficiently defend their election process.

1 EDUCATION AND TRAINING

Unfortunately, the current industry-wide approach to informing the election community about cybersecurity risks focuses on conference-level briefings that provide a blend of intense cybersecurity regulation rigor with dramatic, fear-inducing stories of what can go wrong. These sessions provide some value, but for many county administrators, they fail to explain how security breaches truly impact the county and, more importantly, what they can do about it.

Achieving cultural transformation requires a new education paradigm. Hosting longer, immersive regional security training sessions equips election officials to handle the

real-world scenarios they are likely to encounter. Successful sessions are led by experienced election security experts who understand how to communicate election security concerns in the language and context of the election process and who focus on the following key principals:

- **Hands-on Understanding of Technology Security** Every election leader must thoroughly understand what a computer virus (malware) is. Participating in hands-on exercises enables them to see how a computer is infected so they know how to prevent and stop an attack.

- **Motivations and Actors** It is important to understand who might be interested in affecting the election process and the common tactics they use.

- **Securing the Elections Business** Each aspect of the election process (see figure 1) must be reviewed and discussed to better understand how to improve security at every possible attack point.

- **Table-Top Exercises** By putting newly acquired knowledge and skills to use in sessions that practice responding to security incidents, election officials will know exactly how to quickly respond to and recover from an attack.

2 COUNTY-SPECIFIC INSIGHTS AND CULTURAL TRANSFORMATION GUIDANCE THROUGH ASSESSMENTS

Conducting thorough election security assessments onsite at the county level enables state election leaders to gain valuable insight into the state's overall security posture. Starting with a security assessment is an excellent first step in discovering areas that require immediate attention. An assessment also serves as a customized learning tool that enables county election administrators to have crucial discussions with county commissioners and other stakeholders about next steps, priorities and needed resources.

A best practice to consider is keeping the assessment results confidential at the county level. This protects county autonomy and gives communities the runway needed to address issues efficiently and effectively without fear of reprisal. States can have insight in the form of anonymous, aggregated results to benchmark overall progress and make data-driven decisions.

To be truly effective in today's threat environment, an assessment must go beyond traditional high-level questionnaires and remote website scans. Assessors must also factor in state-specific election code as they thoroughly evaluate each stage of the county's election process.

The most effective security programs require a commitment from county officials to make improvements based on the assessment results. Having election security experts who can provide regular checkpoints and facilitate conversations about progress is critical to driving change. This continued security advisory, sometimes referred to as cyber navigator or Chief Information Security Officer (CISO) advisory, is crucial to realizing security transformation at the county and state levels.

3 STATEWIDE SHARED SECURITY SERVICES

A path to better security will emerge from the assessment results, and making shared security services available to counties statewide is often the most efficient and cost-effective way to help counties make needed changes to strengthen their security. Most counties do not have the resources to employ highly qualified cybersecurity advisors and service providers. By selecting common services and products, states can dramatically improve the speed and quality of improvements that can be made in each county, often for negotiated pricing that reduces overall costs. The set of services can include:

- Templated policies and procedures that can be integrated into each county's processes
- Access to qualified security engineers for required technology updates
- Pre-selected product offerings such as firewalls and/or endpoint software with pre-negotiated pricing
- Access to qualified security advisory (cyber navigators or CISO advisors)
- 24x7 election team environment monitoring for security threats

SECURING ELECTIONS HAPPENS ON THE FRONTLINE

In the past, security was exclusively under the purview of technology and cybersecurity teams. Today, everything is different. Election attacks and voter fraud are a part of the mainstream conversation as they threaten the country's democratic process. Every election leader is responsible for realizing the threat that the Internet introduces into their process. It is up to them to take steps to improve security by transforming their culture and making security a foundational aspect of the entire election process.

To drive dramatic change, states must take the lead in educating and informing their counties. Only through an organized and aggressive push to execute security best practices at the county level, the frontline where most attacks occur, can we obtain the level of election security that truly protects democracy.

CyberDefenses is a premier managed security services provider specializing in election security and trusted as a contracted resource for state and federal governments. CyberDefenses is proud to partner with Runbeck Election Services, America's Election Partner and an innovator in the process of producing elections. Learn more at cyberdefenses.com and runbeck.net.