POLICIES THAT STRENGTHEN ELECTION SECURITY

Secretaries of State and state election directors are at the forefront of public scrutiny when it comes to election security. These leaders hold responsibility for defending elections throughout the state against sophisticated and motivated cyber criminals to prevent attacks and the accompanying negative headlines. Yet, taking the necessary action to increase security on the frontlines of the election, where defenses are most effective, falls to county election directors and their teams, the only ones tactically able to implement the right security measures.

The most effective election cybersecurity programs are those that involve both state and local levels of government. Secretary of State offices and state election directors have a critical role to play in making sure there are no barriers that could make it difficult for counties to implement stronger security controls. Even more important than removing obstacles, state leaders are in the position to ensure that counties are equipped with the right information, resources and approvals to confidently move forward in making needed security improvements.

Achieving this level of enablement, support and motivation is a delicate balance of providing effective structure without stepping beyond the boundaries of healthy county autonomy. What can make it more complex is the fact that states often control how federal funding, such as the money made available through the Help America Vote Act (HAVA),

is distributed to counties. In many cases, responsibility for ensuring that the money translates into statewide results rests with the state, but control over how the dollars are directly spent lies with counties. It can be a challenge to make sure that each disparate part contributes to a successful whole.

USING POLICY TO DRIVE CONSISTENCY AND ENABLE AUTONOMY

Policies, both at the legislative level and the local level, can be an effective way to coordinate consistent, streamlined cybersecurity efforts across all counties in the state. What's more, carefully structured policies can simplify the distribution of federal funding. Providing election security guidance in the form of policy enables states and counties to synergistically work together in determining how grant money is used to create a cohesive statewide cybersecurity program, even with the necessary variations in security initiatives that must exist for each county.

PROVIDING CLARITY IN A CLIMATE OF UNCERTAINTY

A key challenge when it comes to improving election cybersecurity is a lack of clarity around which threats are most likely to affect elections and the security technologies and practices that will be the most effective in defending against these threats. This uncertainty is fueled by sensationalized scare tactics and doom predictions that serve political and business agendas. While some media have focused on unused HAVA funds, implying that the delay in using the money is a false sense of complacency, those of us on the frontlines of the election security challenge know this is definitively not the case.

Complacency is far from the underlying collective feeling regarding election security. A lack of dependable facts about the threats we face and the best way to combat them has necessitated a thoughtful approach that leads to an understanding of the intricacies involved in securing the vote and helps sift through the myths to develop a clear plan of action.

Legislative policies can be a useful way to aggregate the best insights and responses to cyber threats and disseminate this guidance at the county level to drive clarity and certainty.

THE NEXT STEPS IN ADVANCING ELECTION SECURITY

Many states are already successfully proposing and implementing cybersecurity bills and directives that are helping counties define the improvements they need to make ahead of the 2020 election, and every election before and after.

Several states have passed bills that establish an office of election cybersecurity or an election cybersecurity task force. Others are defining state authority to declare a state of emergency in the

event of a cybersecurity incident, and a few are making cybersecurity training mandatory for all election departments.

Some states are adopting legislative measures that are more technical and granular, such as specifying best practices for the electronic storage of data and requiring multi-factor authentication for access to voter registration records. These bills are all solid steps toward building stronger defenses, but they also demonstrate that cybersecurity improvement needs are distinct and varied among jurisidictions and states..

As election security programs continue to mature, state leaders will have an opportunity to refine statewide security by introducing bills and directives aligned to evolving attack methods and emerging best practices. Establishing truly effective guidance for counties will require a combination of legislative action and statewide directive mandates as well as internal department policies defined by each election team to accommodate their unique environment and requirements.

FOUR AREAS WHERE STATE AND LOCAL POLICIES CAN MAKE AN IMPACT

Cybersecurity by nature represents a broad collection of actions and practices. When developing policy, it can be difficult to distinguish which functions warrant definition and enforcement and which items fail to be universally effective. Another consideration is avoiding policies that only create unnecessary red tape.

To help narrow down the options, there are four key areas in which policy, instituted at the state legislative and directive level or at the local county level, has proven to accomplish the most in securing the vote.

1 ELECTION SECURITY ASSESSMENTS

Whether mandated by the state through bills or directives, or defined by county election officials, requiring regular cybersecurity assessments is a critical function of election security. An assessment should cover the county's entire election process, from voter registration to results publishing as well as day-to-day election management. It should also include Darknet intelligence that identifies compromised URLs and credentials or relevant hacker chatter. A review of voting equipment vendors should be part of an assessment too.

Additionally, Chief Information Security Officer (CISO) or cyber navigator guidance needs to be a non-negotiable component of security assessments. The knowledge of the threat landscape, potential risks and up-to-date cybersecurity best practices that these professionals possess is integral to developing a plan of action.

Election security assessments should also be considered at the state level to catalyze defense improvements for state-wide election systems, like voter registration and results reporting processes.

Assessments provide fact-based insights that enable states and counties to efficiently point their resources to the precise threats they face. The recommended cadence for an assessment is every two years to keep up with emerging technologies, staff changes and new cyber threats.

2 ELECTION NETWORK SECURITY AND MONITORING

Most states require that election voting and tabulation systems remain isolated and disconnected at all times from the Internet and other networked systems. However, county election departments require computers, servers and networks to support the election process. These systems can introduce risk and impact the security of elections. It is crucially important that election leaders establish policies setting minimum standards and parameters while still providing counties with the flexibility to implement the hardware and software solutions as well as configurations that best address their environment and staff skillset.

A good practice for network security policies is outlining required functionality aligned to industry-accepted best practices such as the Center for Information Security's Handbook for Election Infrastructure Security. Some examples of recommended capabilities include network segmentation, data encryption, access control and multi-factor authentication.

Continuous threat monitoring is another key element of ensuring the election network infrastructure is consistently protected from attacks. Having policies that articulate an expectation of 24/7 monitoring will pave the way for consistent levels of immediate threat detection across all counties statewide.

3 INCIDENT RESPONSE AND CONTINUITY OF OPERATIONS PLANNING

While protecting election systems is an important priority, being able to quickly respond to a threat and keep an election operating during an attack are capabilities that can not be over-valued. Having an Incident Response (IR) Plan and a Continuity of Operations Plan in place is often a deciding factor in whether an election is disrupted by an attack.

Beyond establishing a policy that requires election teams to develop IR and Continuity of Operations Plans, there are pieces to each of these plans that could warrant standing alone as policies. The National Institute of Technology and Standards (NIST) Framework for Improving Critical Infrastructure Cybersecurity (CSF) is a good resource for recommended IR and Continuity of Operations functions including containing the incident, notifying key stakeholders, and executing a recovery plan.

4 ELECTION SECURITY TRAINING

The most advanced technology in the most secure network can still be compromised when a well-meaning employee unknowingly shares information or clicks on a link that grants a cybercriminal access to the county's election infrastructure. As a result, cybersecurity training is a prime candidate for becoming a state or locally mandated policy.

Training in general can be specified as a requirement, but to be more effective, the policy should outline topics that must be covered. Topics to consider include understanding hacker motivation and methods, how passwords are compromised and what to do to protect passwords in addition to how phishing and vishing campaigns work and how to avoid falling prey to them.

Election security training can also be required for election leaders, not only staff. The curriculum should consist of topics like understanding how attackers move once they are inside the organization, how to secure the election process, election security risk management and crisis management.

CONSISTENT AND DISTRIBUTED

Thoroughly developing parameters and baseline standards in each of these areas will form a defensible foundation for an effective cybersecurity program that maintains a consistently high level of protection against current and future threats. Policies can be a valuable tool in enabling states to coordinate consistent and effective cybersecurity practices across counties. They can be the unifying tie that consolidates the distributed nature of local government into an impenetrable whole at the state level.