Election Security: A Checklist for 2020

With major contests less than two years away, election officials need a multilayered approach to stay a step ahead of hackers.

As the next round of national and local elections draws closer, security experts expect cybercriminals will intensify their efforts to steal voter information, breach voting systems and influence outcomes. Blocking these threats can be a daunting challenge for government officials who must work with limited funds and manpower. The following checklist summarizes where to focus available resources to protect election infrastructure and preserve the cornerstone of democratic government.

☑ **CONTINUE TO TREAT ELECTION SYSTEMS AS CRITICAL INFRASTRUCTURE.** Like the power grid and water supplies, the election infrastructure is an essential resource for local communities, and the federal government now defines it as part of the nation's critical infrastructure. This means government stakeholders must understand not only the associated cybersecurity threats but also the larger emergency management implications of breaches. For example, an attack on voting and registration systems may provide an entrée into other essential services, such as networks used for public safety. Disruption to voting combined with the loss of essential services may result in political uncertainty, threats to public health and safety, and even civil unrest.

☑ **DRAW ON THE EXPERTISE OF VARIOUS GOVERNMENT AND PRIVATE SECTOR STAKEHOLDERS TO CREATE MULTIPLE LAYERS OF PROTECTION.** Election officials should organize discussions with senior government executives, state homeland security directors, IT personnel within the state and the Secretary of State's office, emergency managers, first responders, federal homeland security authorities and representatives from IT vendors.

"Encouraging collaboration among a cross-section of industry and public sector resources is something I can't emphasize enough. The days of going it alone by merely relying on an approach and technologies that have worked in the past are long gone," says Tom Guarente, vice president of external affairs and alliance, public sector at FireEye, Inc., a leading cybersecurity vendor.

This cross-section of experience ensures an election security plan covers not only cyberthreats but also the broader political, financial and social implications of protecting elections.

"When organizations approach cybersecurity as emergency preparedness and response versus merely an IT issue, they put themselves in a stronger position to minimize the impact on systems and individuals in the event of a cyber attack." Guarente adds.

> **"Encouraging collaboration among a cross-section of industry and public sector resources is something I can't emphasize enough."**
>
> Tom Guarente, Vice President of External Affairs and Alliance, Public Sector, FireEye, Inc.

TEST THE PLAN. IT'S NOT ENOUGH TO DELINEATE RESPONSIBILITIES AND POLICIES FOR PROTECTING SYSTEMS AND RESPONDING TO THREATS AS THEY UNFOLD.

Authorities must regularly test and continuously improve their election security plans. Run table-top exercises both with subgroups of stakeholders and with the full complement of people who are entrusted with election security to ensure everyone responds effectively under the pressure of an actual incident.

MODERNIZE THE VOTING SYSTEM INFRASTRUCTURE.

Multilayer election security requires more than just an IT response; nevertheless, state and local governments must still shore up their digital defenses. Start by focusing on protecting vote tallies, voter records and related information as it passes through networks and resides in databases. Data generated with voting machines can be safeguarded by segmenting these machines on dedicated networks that aren't linked to external networks or the internet. This reduces the chance that a hacking organization can steal credentials or circumvent network defenses to access this important data. Consider encryption technology to further protect information when it's in transit across networks, housed in databases, or stored on hard drives or thumb drives. Patch management is also critical. Automate patching frequently to ensure software updates are applied as soon as possible after vendors release them.

Since so much information is shared via email, endpoint security should be another focus area. Protect computers and portable devices with multi-factor authentication to mitigate unauthorized access to sensitive resources. It's also important to devise backup policies that create frequent copies of data that can be stored safely in offsite locations in case of a production-system breach or ransomware attack.

Extend security beyond internal operations to the larger supply chain of public sector peers and private sector companies, such as cloud computing vendors that outsource portions of the IT infrastructure. Meet regularly with partners to review their security policies and identify any gaps that should be addressed in the run-up to elections. The federal government offers help for these reviews. The External Dependencies Management Assessment is a no-cost service for identifying and addressing technology risks associated with external partners.

PROTECT PERSONAL TECHNOLOGY.

Security experts warn election officials may become bigger targets for hackers who try to tarnish the accuracy and fairness of elections. One tactic is to paint an official as being biased toward a candidate or party to bolster claims that election results were "rigged."

"Don't say or do anything publicly or online that you wouldn't be comfortable seeing on the front page of a newspaper," says Will Carter, deputy director at the Center for Strategic and International Studies, a public policy think tank. "And recognize how even innocent comments might be twisted or taken out of context."

Related to this is making sure personal computing devices and home networks attain government levels of security, with multi-factor authentication, strong passwords, encryption and backup capabilities.

This piece was developed and written by the Center for Digital Government Content Studio, with information and input from FireEye.

> **"Don't say or do anything publicly or online that you wouldn't be comfortable seeing on the front page of a newspaper."**
>
> **Will Carter, Deputy Director, Center for Strategic and International Studies**

Produced by:

CENTER FOR DIGITAL EDUCATION

www.centerdigitaled.com

In collaboration with:

FIREEYE™

www.FireEye.com