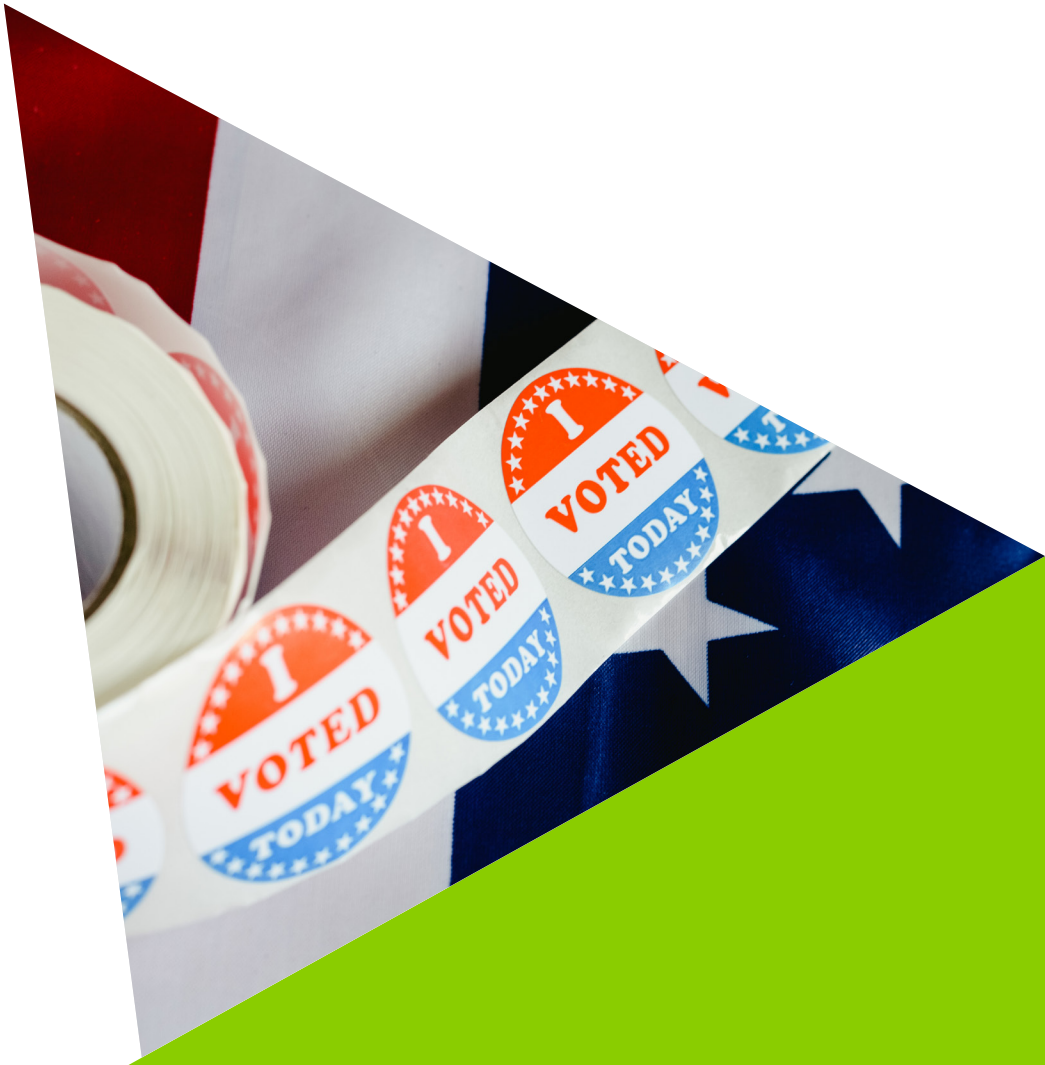
Guidehouse

Election Security in a Connected Era

What Election Officials Need to Know to Maintain Systems Integrity



Election officials work diligently year-round to prepare and maintain a process that is free, fair and accessible. Nonetheless, foreign interference in the 2016 presidential election exposed cracks in the security of America's electoral process. The many vulnerabilities in our country's election systems include the relative ease of voting machine hacking,[1] threats to voter registration systems and personal privacy,[2] and disinformation campaigns waged by foreign nations aiming to confuse voters and disrupt our electoral process.[3] State and local entities maintain much of the nation's election infrastructure, rendering them both key players in addressing these vulnerabilities and prominent targets of attacks. In the past, the focus of election security has centered almost exclusively on the physical security of the process. However, the interconnected nature of today's digital landscape requires that our focus shift to combating information operations and strengthening our defenses.

We can counter growing threats to election security by better understanding the inherent risks to our interconnected election system, securing the voting process, and building a culture where both agencies and the public are prepared for threats of election interference. In this document, Guidehouse identifies the best practices that should be top of mind for state and local election officials as they work to secure the free and fair elections that are a central pillar of our democracy.

[1] A Joe Uchill, "Hackers breach dozens of voting machines brought to conference," The Hill, July 29, 2017, available at http://thehill.com/policy/cyber security/344488-hackers-break-into-voting-machines-in-minutes-at-hacking-competition.

[2] Peter Reuell, "Voting-roll vulnerability," Harvard Gazette, September 6, 2017, available at https://news.harvard.edu/gazette/story/2017/09/study-points-to-potential-vulnerability-in-online-voter-registration-systems/.

[3] Massimo Calabresi, "Inside Russia's Social Media War on America," Time, May 18, 2017, available at http://time.com/4783932/inside-russia-social-media-war-america.

Introduction

The U.S. intelligence community has confirmed that a foreign government conducted widespread cyber and information operations during the 2016 presidential election. Special Counsel Robert Mueller's report on foreign interference in that election documented the targeting of individuals and entities involved in the administration of U.S. elections by Russian military officers operating within Russia's state intelligence service (GRU). Elections are regulated almost entirely by state law and are administered exclusively by the election officials of their respective states. It is therefore not surprising that the overwhelming majority of Russia's targets were state and local entities, including state boards of elections (SBOEs), secretaries of state and local/county government officials. Russia also specifically targeted government employees who work alongside these state and local officials and entities through spear-phishing email campaigns.[4] Outside of government officials, the Russians "targeted private technology firms responsible for manufacturing and administering election-related software and hardware, such as voter registration software and electronic polling stations."[5]

According to the Department of Homeland Security (DHS), these hackers explicitly targeted state and local voter registration databases and managed to thereby access election systems in at least 21 states.[6] In Illinois, the Russians compromised the computer network of the State Board of Elections by exploiting a vulnerability in the SBOE's website. The GRU gained access to a database containing information on millions of registered Illinois voters and extracted data related to thousands of those voters before the malicious activity was identified.[7]

Along with many who keep an eye on our national and local elections, we at Guidehouse expect this threat to increase as we approach the next election cycle. While testifying before Congress on his agency's preparations for the upcoming presidential election, FBI Director Christopher Wray stated plainly, "Make no mistake: The threat just keeps escalating and we're going to have to up our game to stay ahead of it."[9] If we fail to act, these vulnerabilities threaten to undermine the main tenets of our democratic process.

> "unprepared at all levels of government for a concerted attack from a determined foreign adversary."[8]
>
> **Senator Richard Burr**,
> chair of the Senate Intelligence Committee, describing the state of U.S. election security

Elections are complicated, but we have an obligation to safeguard the most fundamental part of our democracy. In order to protect the integrity of U.S. elections, we identify several concepts applicable to election security nationwide, despite variations in the different election systems utilized across states and communities. We explore leading trends in election security, and examine emerging patterns in the strategies being pursued by our adversaries, along with potential solutions. All of these elements should be given proper consideration by secretaries of state, election administrators and other leaders of municipal jurisdictions.

[4] Special Counsel Robert S. Mueller, III, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election: Volume I," U.S. Department of Justice, March 2019, 1 ("Mueller Report").

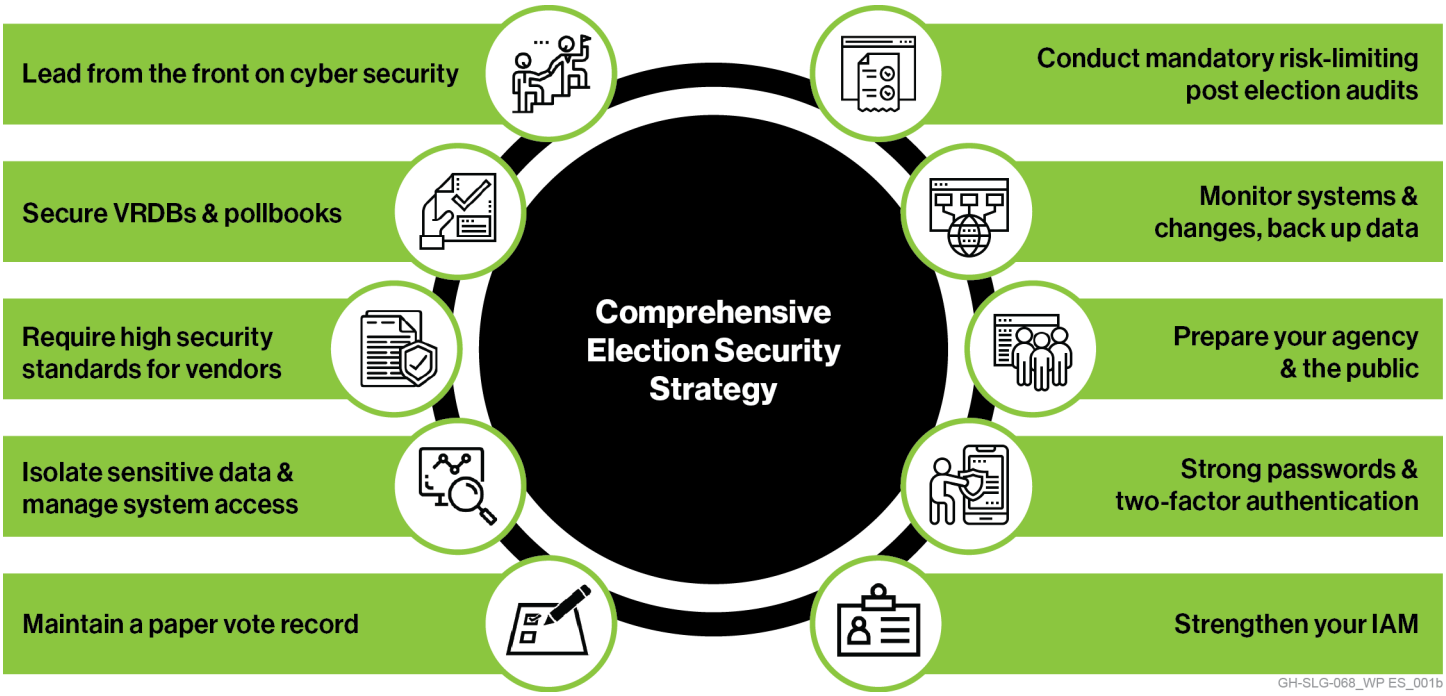
[5] Ibid.

[6] Matt Zapotosky and Karoun Demirjian, "Homeland Security official: Russian government actors tried to hack election systems in 21 states," The Washington Post, June 21, 2017, available at https://www.washingtonpost.com/world/national-security/homeland-security-official-russian-government-actors-potentially-tried-to-hack-election-systems-in-21-states/2017/06/21/33bf31d4-5686-11e7-ba90-f5875b7d1876_story.html?noredirect=on&utm_term=.aab751473564.

[7] "Mueller Report."

[8] Transcript of "Senate Select Intelligence Committee Holds Hearing on Russian Interference in the 2016 Elections, Panel 1."

[9] Todd Ruger, "FBI director wants to 'up our game' on election interference," Roll Call, May 7, 2019, available at https://www.rollcall.com/news/fbi-director-wants-game-election-interference.



Address the challenges inherent in an interconnected election system

Every piece of our electoral process is a potential target for bad actors. This is not exclusive to the individual parts, but includes the connections between them as well. Hackers will search for the weakest point, attack there and then navigate within the network to their actual target. The Russian attacks of 2016 showed that private firms, vendors and state agencies not involved in the elections process are critical vulnerabilities. Because a successful cyberattack on these outside organizations could allow adversaries to tamper with our elections, such organizations must be a part of overall defenses. This is particularly true for other state agencies with access to voter registration databases (VRDBs). In several states, other agencies—such as Departments of Motor Vehicles and Health and Human Services agencies—feed data to the VRDB in order to keep voter records current. This means that if a hacker can penetrate those agencies, they may be able to manipulate the VRDB. For states that have embraced the convenience and benefits of online voter registration, we see additional risks. Giving voters the ability to register and update their voter information through a public-facing internet portal exposes the VRDB to the internet and makes it more susceptible to internet-based attacks. However, simply removing the VRDB from the internet would not entirely mitigate this risk. The system does not need to be connected to the internet to be vulnerable, since hacks can also be carried out via external storage devices.

Linked to VRDBs are pollbooks, copies of the voter rolls used by election officials to process voters on Election Day. Some states use paper pollbooks, while others use electronic versions (e-pollbooks) which are networked into the state's central VRDB. Either format requires that information be transmitted from the VRDB to the pollbook (whether directly, in the case of e-pollbooks, or via printing). Some states build and maintain the software used for the development and maintenance of both VRDBs and e-pollbooks in house, while others outsource that work to external vendors. Such use of external vendors provides an additional target for potential hackers, as the vendor's systems are also linked to the election databases.

Guidehouse Recommendations:

Secure voter registration databases (VRDBs) and electronic pollbooks (e-pollbooks)

The Help America Vote Act requires that all states implement a "single, uniform, official, centralized, interactive, computerized voter registration list." In 2016, hackers managed to gain access to VRDBs in at least 21 states. Fortunately, there is no evidence that any votes were altered; however, once a bad actor gains access to a VRDB, they could manipulate the database by adding, editing or deleting voters. These types of attacks could result in false votes being cast, citizens being prevented from voting or voters being forced to cast provisional ballots. Even if this type of attack did not manipulate the outcome of the election, it could undermine the election's credibility through the public perception of vote manipulation or voter suppression.

Organization leadership should ensure all networked devices that interact with VRDBs or e-pollbooks are secure, including the devices of vendors and other outside state and local government agencies. As discussed below, a strong system should also be in place for the VRDB and e-pollbooks. To best monitor the security of the VRDBs, all changes should be securely logged and periodically reviewed. Reviews (whether automated or conducted by an election official) should specifically search for atypical behavior to quickly identify potential security breaches.

Make sure all vendors meet the agency's security standards

The networked systems of any vendors working with state and local election officials increase the number of targets for would-be hackers. Since many vendors are involved in the development and maintenance of elections systems such as voter tallying machines, VRDBs and e-pollbooks, their systems must meet the same high cybersecurity standards held by state and local election officials and their agencies.

When selecting a vendor, agency leadership should evaluate the vendor's cybersecurity operating procedures. They must also ensure that any potential vendor will be an agency partner in addressing cybersecurity concerns as they arise and evolve. Moreover, vendors should be required to conduct vulnerability scans and update their software and procedures as new risks are identified.

Isolate sensitive data and manage system access

External system access to the VRDB should be limited. If a state's VRDB is fed data from an outside agency, such as the Department of Motor Vehicles, that information should be periodically validated for accuracy. In order to prevent the database from being maliciously edited if an external agency is compromised through a cyberattack, outside sources should not be permitted to write directly to the VRDB. Additionally, access to the VRDB within an agency should be limited to only those who need it—and access should be tailored to the specific job duties of those individuals. For example, the county elections manager for county A should not be able to edit the section of the VRDB specific to county B. This same principle can be applied to devices. This policy would limit the potential manipulation when specific accounts or devices are compromised.

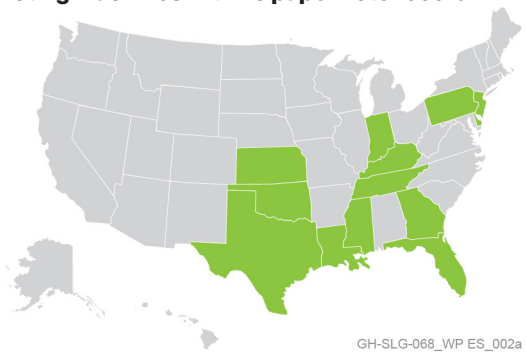
Applying software updates and patches on all devices connected to the VRDB as soon as they become available is essential in preventing malicious actors from gaining access. If this updating is done by a vendor, they will require temporary access to the VRDB. That access should be revoked as soon as their work is complete. As well, the use of external storage devices should be heavily restricted.

Secure the voting process

Foreign interference in the 2016 presidential election and subsequent investigations taught us that hackers have the tools, abilities and motivation to penetrate voting systems and vote-tallying devices. Hackers can breach these systems even if they are not connected to the internet.[10] The fact is that all direct recording electronic (DRE) voting machines are susceptible to local hacking, and those connected to the internet can be hacked remotely. These vulnerabilities are most concerning when there is no paper vote record used in association with the DRE voting machines to audit vote tallies and ensure that each DRE machine functioned as intended.

Currently there are DRE voting machines in use without any paper vote record in 14 states.[11] This is problematic: In the event of a suspected cyberattack, it would be almost impossible to conduct an audit of the vote tally, since the only record of the individual votes would exist on the compromised voting machine. Even absent hacking attempts by malicious hackers, voting machines are susceptible to programming errors, which can lead to erroneous election results. For example, a software error in a vote-tallying system used in a March 2012 municipal election in Palm Beach County, Florida led to votes being allocated to the wrong candidate. This resulted in inaccurate election results being reported to the public.[12] The error was discovered during a post-election audit, and election results were subsequently changed following a court-ordered recount of the paper vote records.[13]

Voting machines with no paper vote record



GH-SLG-068_WP ES_002a

Guidehouse Recommendations:

Maintain a paper vote record registration

While implementing best practices will improve both an agency's deterrence and defense against potential hackers, there is no guarantee that election systems and networks will be impenetrable. As mentioned previously, software or hardware failures could lead to an erroneous vote count even without interference from a malicious actor. To safeguard against both outside manipulation and technical failures, election systems should never rely solely on a computer system to tally votes. Every election system should include a paper vote record to ensure definitive results. If an agency's election system uses paperless voting systems, agency leadership should replace them immediately. Viable options include using paper ballots with optical scanner systems or electronic voting machines that generate a voter-verified paper record. This guarantees an auditable paper record for every vote cast in every election. Additionally, leadership should institute strict chain-of-custody requirements for paper records to make sure they cannot be manually altered.

[10] Bradley Barth, "WikiLeaks: CIA's Brutal Kangaroo toolset lets malware hop onto closed networks," SC Magazine, June 22, 2017, available at https://www.scmagazine.com/wikileaks-cias-brutal-kangaroo-toolset-lets-malware-hop-onto-closed-networks/article/670395/.

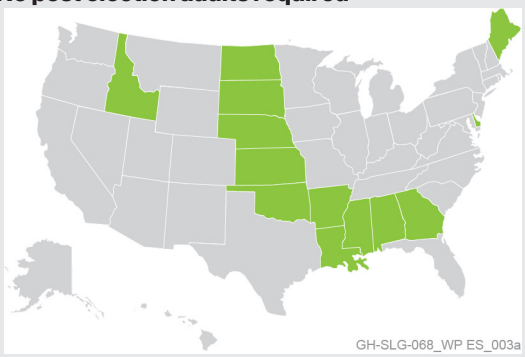
[11] Ballotpedia, "Voting methods and equipment by state," available at https://ballotpedia.org/Voting_methods_and_equipment_by_state.

[12] Jaikumar Vijayan, "E-voting system awards election to wrong candidates in Florida village," Computerworld, April 3, 2012, available at http://www.computerworld.com/article/2502640/vertical-it/e-voting-system-awards-election-to-wrong-candidates-in-florida-village.html.

[13] Ibid.

Conduct mandatory risk-limiting post-election audits

No post election audits required



Paper vote records are only useful in determining whether malicious interference or technical failures took place in an election if election officials carry out post-election audits—preferably risk-limiting ones. Audits bring transparency to the vote-counting process, thereby helping to build public trust. They also confirm the accuracy of—or uncover inaccuracies in—reported election results. Because a full hand count of all votes would in most cases be prohibitively costly and time-intensive, different methods for conducting audits more efficiently have emerged. One common practice is to audit a fixed percentage of votes cast. A fixed-percentage audit is certainly better than conducting no audit at all. However, such audits can be inefficient due to inaccurate estimates of the number of votes necessary to confirm the reported election results. In an overestimation, the audit does too much and is a waste of time and resources. In an underestimation, the audit might not fulfill its purpose.

A more accurate and efficient method is the risk-limiting audit. This approach uses statistical methods to determine the minimum number of audited votes necessary to confirm the accuracy of the reported election results. Election officials must determine an acceptable risk limit in order to conduct this type of audit. A common limit is 5 percent, which would create a 95 percent confidence interval for the post-election audit. In other words, setting a 5 percent limit for an election in which there was tampering would mean there is at most a 5 percent chance the audit will fail to expose the tampering and, at minimum, a 95 percent chance the audit will correctly determine there is likely an error in the election results. In order to maintain statistical accuracy, the number of votes audited would be determined by the desired risk limit and the reported margin of victory. According to Jerome Lovato, the testing and certification director at the U.S. Election Assistance Commission, "a risk-limiting [audit] provides strong statistical evidence that the election outcome is correct, and has a high probability of correcting a wrong outcome."[14]

Risk-limiting post-election audits represent an independent confirmation of the reported election results. As such, these audits should be transparent and their results made public. Election officials should make risk-limiting audits standard practice statewide, and ensure that the necessary data from each audit is publicly available so that independent bodies are able to verify the results. Furthermore, it is crucial to conduct these audits using only voter-verified paper vote records.

[14] Jerome Lovato, "Risk-Limiting Audits – Practical Application," Elections Assistance Commission, June 25, 2018, available at https://www.eac.gov/assets/1/6/Risk-Limiting_Audits_-_Practical_Application_Jerome_Lovato.pdf.

Prepare your agency and the public

Following rampant reports about manipulative fake news stories, the vulnerability of our election systems and the hacking of campaigns by malicious actors, Americans are generally aware that the integrity of our elections is at risk. Open, effective and transparent communication from election officials is the best way to maintain public trust in the electoral process. Timely and effective communication can counter malicious information operations aimed at casting doubt over the election process and its results. An adversary could launch a website that appears to be a local election information site but is aimed at spreading disinformation regarding election dates, polling locations or registration information. Simply supplying the public with clear instructions regarding the appropriate place to find the aforementioned information could be enough to counter malicious actions like these. And by instituting appropriate monitoring practices, election officials are more likely to be able to recover data quickly and communicate issues to the public before they become unmanageable.

Guidehouse Recommendations:

Continuously monitor your systems, log changes and back up data

Monitoring, logging and backing up your data systems aides in attack detection and ensures system data recovery after an incident. It is best to use both human and technical means of monitoring, as input from local election officials and workers can minimize the cost of procuring and implementing new automated monitoring systems. Local officials know their jurisdictions well and will likely spot discrepancies quickly; however, some gaps in detecting malicious attacks will invariably remain, and should be covered through automated forms of data monitoring. These additional automated systems are crucial in detecting manipulation of, or intrusion into, election systems.

Election officials should mandate that all changes to VRDBs are logged, and that the database is monitored by both humans and automated technology. They should institute policies requiring that data systems are regularly backed up, so that accurate data can quickly be recovered and restored following an attack. These backup files should be in read-only form, meaning that no user anywhere in the system has the authority to edit them, thus protecting the backup data from manipulation by a malicious actor.

Prepare your agency and the public for information operations

Election officials should establish updated processes and communications materials to respond in a timely and effective manner in the event of an attack. They should consider developing a cyber interference incident communications plan and develop standard operating procedures for communication with the public—thereby reinforcing the fact that election integrity is a top priority. Before any votes are cast, election officials should clearly communicate both general and specifically identified cyber threats to the election. Citizens should be assured that officials have taken and are taking all necessary steps to counter election interference. Agency leaders should work to build relationships with key stakeholders to develop clear communication channels before an attack occurs. This becomes especially important when it comes to candidates and party officials, as a cyberattack on a campaign or political party could be the precursor to an attack on the election itself, giving election officials advance warning of an impending attack.

Make every employee an asset, not a liability, in preparedness

The first instinct of senior leadership is often to procure and deploy new technology to combat the growing election security threat; however, such an approach can be an expensive and time consuming undertaking. Many election officials struggle to acquire the necessary funding to implement these changes, and, in the interim, the election process remains vulnerable. The fastest way to mitigate current threats is for state and local leaders to foster awareness and a strong culture, not just within their own organizations, but across all agencies that are potential targets. Most technical compromises start with human error. In fact, the individual user is the weakest link in an organization's defense against increasingly sophisticated attacks. Research indicates that over 55% of all email traffic was spam in 2017[15] and that 4% of all internet users fall for an email phishing attempt.[16] Most systems are compromised within minutes of an incident, making swift reporting of potential incidents critical[17]—yet breaches in the public sector can often go undetected for years. The first step toward protecting the security of our electoral process should encompass an internal education and awareness campaign. The most effective defenses build on a foundation that consists of a strong culture and organization-wide understanding of related threats and protocols.

Guidehouse recommendations:

Lead from the front

Organization leadership should promote a top-down culture of cyber-awareness. Through modeling and encouraging best practices, leaders demonstrate the importance of adhering to established standards within the organization. Leadership should implement a mandatory, recurring and informative security-awareness training program for all personnel. Every employee must understand the relevant risks, as well as the agency protocols for countering them. Most importantly, leaders should build a culture in which employees feel comfortable reporting possible threats without fear of reprisal, especially if they believe their own account or system has been compromised.

Make strong passwords and two-factor authentication mandatory

Hackers will often use stolen user credentials (e.g., username and password) to infiltrate organizations and their networks. Requiring strong passwords that are at least 10 characters long and include letters, numbers and symbols is important; however, such passwords, too, can be stolen. Two-factor authentication is widely accepted as one of the best defenses against account compromise. It provides superior security by requiring an additional piece of information (for example, a 4-digit code sent to the user's cell phone) along with the user's password to gain access to their account. Hackers may steal login credentials through a large data breach, a targeted attack against an individual or a phishing email campaign. Two-factor authentication ensures that, even if a malicious actor gains access to user credentials, only the individual user with both factors will be able to access their account. Election officials should require two-factor authentication for all employee accounts.

Tighten up your identity and access management (IAM)

IAM involves defining and managing the roles and access privileges of individual network users and the circumstances in which users are granted (or denied) those privileges. As previously mentioned, compromised user credentials are often a hacker's entry point into an organization's network and its information assets. Therefore, every user with access to the network is a potential target. The more users with access to the system, and the broader their access, the greater the opportunities for potential hackers. Organizations should proactively control and manage access by limiting the number of people with access exclusively to those who need it, restricting what each individual user is able to access in accordance with their needs as an employee, and quickly removing those who no longer need access (e.g., if someone is no longer an employee, or no longer involved in election-related work).

[15] Symantec Corporation, "Internet Security Threat Report (ISTR): Volume 23," March, 2018, available at https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf.

[16] Verizon, "2018 Data Breach Investigations Report: Executive Summary," 2018, available at https://enterprise.verizon.com/resources/reports/DBIR_2018_Report_execsummary.pdf.

[17] Verizon, "2017 Data Breach Investigations Report," 2017, available at https://www.ictsecuritymagazine.com/wp-content/uploads/2017-Data-Breach-Investigations-Report.pdf.

Conclusion

In its current state, our election infrastructure is highly susceptible to manipulation and hacking by malicious actors, software malfunctions and physical Election Day disruptions. The Russian interference in 2016 exposed the ease with which a foreign actor could disrupt one of the central tenets of our democracy—our ability to conduct free and fair elections. FBI Director Wray has warned us that the threat continues to escalate. Speaking specifically of Russia, Senator Burr said, "This adversary is determined. They're aggressive and they're getting more sophisticated by the day." If we want to get and remain ahead of our adversaries as we enter this new age of election security, we must bolster our defenses now.

The recommendations above are not exhaustive, but they are critical to defending our election institutions and systems. State and local election officials should work with their federal counterparts to secure additional funding to help offset the costs associated with upgrading election infrastructure. As Senator Ron Wyden of the Senate Intelligence Committee recently remarked, "We would not ask a local sheriff to go to war against the missiles, planes and tanks of the Russian Army. We shouldn't ask a county election IT employee to fight a war against the full capabilities and vast resources of Russia's cyber army." It is imperative that state and local election officials put in place the measures detailed above to safeguard our democracy. They are the first steps toward creating a more agile and evolved strategy of resilience at the state and local government levels.

Guidehouse acknowledges **Dennis Magnasco**, a joint-degree candidate at the Harvard Kennedy School of Government and Tuck School of Business, for his contributions to the development of this white paper as a Summer MBA Associate in our State and Local Government Practice.

About Guidehouse

Guidehouse is a leading provider of management, technology, and risk consulting services to the public sector and commercial markets. We help our clients solve their most complex issues through collaborative solution design, bold strategy, and innovation that advances conventional thinking that prepares them for future growth and success.

Following our recent merger with Navigant, we proudly serve both the public sector and commercial markets, with a focus on supporting client needs in Healthcare, Financial Services, Energy, Environment, National Security, and Aerospace & Defense.

Headquartered in Washington, DC, our reach has now expanded on a global scale. We are a team of seasoned professionals with proven and diverse expertise in traditional and emerging technologies, markets, and agenda-setting issues that drive national and global economies.

If you would like to learn more about how Guidehouse can help navigate you forward, please contact us at **www.guidehouse.com**

Email: statelocal@guidehouse.com / **Web:** guidehouse.com / @guidehouse linkedin.com/company/guidehouse/