WHITE PAPER

Strengthening Democracy: CISA's Blueprint for Election Security Success

carahsoft

Introduction

Election Security is a challenging subject because it involves so many different disparate systems that could be potentially exploited by bad actors. The best approach to ensuring comprehensive election security, which is paramount to protecting the democracy that our country was built on, is to enact a systematic approach that CISA has established.

In their documentation, they highlighted the following areas that are crucial to proper election security:

Cybersecurity Assessments

- Phishing Assessments
- Risk and Vulnerability Assessments
- Penetration Testing
- Vulnerability Scanning

Detection and Prevention

- Continuous Diagnostics and Mitigation (CDM)
- Incident Response
- Cyber Threat Hunting
- Malware Analysis
- Recovery

Information Sharing and Awareness

- Integration Strategies
- Threat Intelligence Feeds
- DHS and CISA Programs

Training and Career Development

- End User Training
- Analyst Training
- Vendor Training and Certifications

By properly adopting security tools and practices to meet all of the above requirements, we can ensure proper election security as the 2024 elections rapidly approach. There is no silver bullet to security but with a combination of awareness and deliberate implementation of controls and security tools, we can work to successfully combat today's hackers who are leveraging AI to be more dangerous than ever. Carahsoft is committed to being the trusted government IT solutions provider for any agency seeking to improve their security. Carahsoft has subject matter experts in this area and is happy to conduct complimentary assessments and consultations with clients.

Battlegrounds of the Digital Age: Securing Election Infrastructure Amidst Growing Cyber Threats

One of the challenges in election security is the myriad of ways bad actors can attack or influence systems. This includes the relative ease of voting machine hacking, threats to voter registration systems and voter privacy, and disinformation campaigns waged by foreign nation-states or other political actors aimed at inciting conflict or sowing discord among voters.

As global connectivity expands—especially through the increase in network-connected devices—the number of unprotected surfaces rises as well, providing growing vulnerabilities for malicious parties to exploit. Cyberattacks have rapidly evolved and are being carried out by more than just shadow organizations with small-scale agendas or individuals and small groups looking to make a profit. Nation-states have been increasingly using the internet and connected devices as new battlegrounds for nontraditional and asymmetric warfare.

What initially began as attempts at infrastructure disruption or information stealing by these groups has escalated to efforts to influenc
e elections. In 2016, the United States was targeted by a foreign nation-state intent on infiltrating and manipulating the electorate—the Department of Homeland Security (DHS) later found that 21 states were targeted by hackers leading up to the election. While five of these states denied that they had been attacked, and only a single state reported a breach in the voter registration system, experts have warned of future attacks on election infrastructure.

Such attacks will likely target not only federal elections but key state elections coming in 2024 in an attempt to either influence the policies of the United States or to destabilize faith and security in the electorate system. Based on these estimates, DHS designated the systems used to administer the country's elections as critical infrastructure in early 2017.

Free and fair elections are a central pillar of American democracy. With bad actors attempting to shift the balance of power in their favor and undermining confidence in election results, election security is quickly becoming paramount. To this end, the Cybersecurity and Infrastructure Security Agency (CISA) has worked to ensure the physical and cyber security of electorate assets and systems. CISA's approach to securing electorate infrastructure include cybersecurity assessments, detection and prevention, information sharing and awareness, and training and career development. As the trusted government solutions provider, Carahsoft has assembled a robust collection of tools and training critical for protecting the nation's most important elections and voting assets, which can also be leveraged to harden organizations' digital infrastructure.

Cybersecurity Assessments

Tools that fall into this category enable the evaluation of operational resilience, cybersecurity practices, management of external dependencies, and the assessment of key elements of infrastructure. Assessments are critical to establishing a well-rounded understanding of an organization's digital assets and the threats they are most vulnerable to.

Phishing Assessment Tools

Social engineering and phishing attacks, in which perpetrators pose online as a stranger or acquaintance of the targeted victims, are on the rise—more than 80 percent of breaches in 2023 began in the form of a phishing email. When it comes to election security, phishing can be especially costly—during the 2016 election, Russian hackers attempted to phish people associated with Hillary Clinton's campaign and successfully snared campaign chair John Podesta. Political organizations are now training staffers to look out for phishing attempts with the help of vendors that carry out controlled attacks to see how vulnerable the organization is. Phishing assessments tools allow organizations to not only measure the awareness and readiness of an organization, but also reinforce critical best practices against malicious emails across the organization's user base.

Risk and Vulnerability Assessments

Vulnerability assessments are intended to identify threats and the risks they pose. Using network monitoring tools and onsite assessments, risk assessment platforms collect data and combine it with national threat and vulnerability information to provide organizations actionable outputs based on their risk level. Organizations can also implement penetration testing, vulnerability scanning, and security instrumentation tools to find vulnerability gaps within their environments and test out their systems against various types of malicious network traffic. The best vulnerability assessment tools can be integrated with threat intelligence feeds and utilize an assessment of multi-stage attack vectors rather than identifying or evaluating each potential vulnerability independently. Organizations facing an increased risk of cyberattacks, especially from nation-state actors, can benefit the most from risk and vulnerability tools.

Penetration Testing Tools

Penetration testing uses dedicated teams to test out vulnerability gaps in an organization's elections infrastructure—a critical component to continuous testing against potential threats. Penetration testing focuses on externally accessible systems by a team that tries to detect and exploit weaknesses in a system. This approach goes well beyond automated vulnerability testing—the addition of an actual person allows for a complete assessment of the network infrastructure and the impact a breach can have. Many third-party vendors offer penetration teams that partner with security research teams to conduct testing based on the latest threats. There are also options for simulated red team and blue team exercises with cyber ranges that could work to identify an organization's gaps and then accordingly set steps for remediation.

Environments should be tested whenever new network infrastructure or applications are added, significant upgrades or modifications are applied to infrastructure or applications, security patches are applied, and end user policies are modified. While penetration testing is an important part of evaluating organizational security, the recommended frequency can vary depending on the organizational mission, exposure to risk, and budget.

Vulnerability Scanning Tools

An increasing number of mobile and IoT-connected devices are being used to access organizational networks, creating potential unidentified vulnerabilities, including in voting machines and equipment.

> The hacking of voting systems was a suspected vulnerability in the 2020 election, and a report from Fall 2023 found that U.S. voting equipment is still susceptible to being hacked.

Having consistent vulnerability scanning enabled allows organizations to scan for potentially compromised equipment by looking at missing patches and outdated protocols, certificates, and services. New generations of vulnerability scanners go beyond simply working inside systems—information that could lead to breaches is reviewed, and pertinent information about an organization's security posture is sent to the proper personnel. Top-notch vulnerability scanning tools can examine and even discover assets, enabling customers to understand their complete attack surface. The range of asset discovery can also be very comprehensive to include devices like IoTs, IoMTs, and OTs.

Detection and Prevention

Once an organization has a well-rounded understanding of its election assets and vulnerabilities, it must put systems in place to identify and prevent those high-risk threats. Multiple layers of tools that continuously monitor and prevent against cyberattacks are critical to strengthen an organization's digital infrastructure.

Continuous Diagnostics and Mitigation (CDM)

CDM requires tools that will bring in information from all devices and systems within an IT infrastructure. That data must be analyzed on an ongoing basis, and any activity or event that reduces security posture must be flagged and addressed. Several tools utilize CDM to operate effectively.

Device behavior tools analyze device behavior and build a baseline. This type of tool can assess the operating systems and applications of an entire enterprise's devices and can enforce a security baseline on non-compliant devices.

Identity access management tools handle user authentication. A single sign-on system with built-in access control should be able to enforce stricter authentication methods based on security variables, such as location, device, or user role.

Firewall management network tools can view firewall events, track open ports, triage critical breaches, and mitigate risk. This also includes tracking devices that are on the network, especially in bring-your-own-device settings.

Security information and event management (SIEM) tools correlate information from all solutions and hardware within an infrastructure. This tool allows analysts to view any event that occurs in a system and identify any infrastructure that it touched, reducing mean time to identify (MTTI) and mean time to resolve (MTTR).

Security orchestration, automation, and response (SOAR) products are easing the speed at which mitigation can occur. If a standard operating procedure (SOP) is in place to remediate a known issue, automated responses based on those SOPs can be programmed to take action with the security tools at an organization's disposal. If a human eye is needed in the process, a SOAR tool can gather intelligence from all solutions and prompt humans for a decision.

Incident Response

Following a cybersecurity incident, it is crucial to have tools that aid in IT forensics to reduce Mean Time to Identify (MTTI) and Mean Time to Resolve (MTTR). A number of Carahsoft vendor partners provide incident response services to coordinate efforts to reduce impact of the incident and investigate its root cause. In 2016, the Democratic National Convention hired incident response firms to investigate the breach to their systems and ultimately attributed the hack back to nation state actors.

In a robust security environment, an arsenal of tools can strengthen the response to a variety of attack vectors, including phishing, malware exposure, and privilege escalation.

Common incident response tools include:

- Alerting tools that notify pertinent personnel and quickly start the incident response timeline.
- A SIEM tool that aggregates all logs from any hardware or software for quick access when investigating.
- For mature security operation centers, a SOAR system with configurable playbooks from SOPs will allow this solution to take action on computerized time to resolve issues and repetitive incidents quickly, freeing up human personnel to conduct more thought-intensive threat hunting.
- A network segmentation tool that quickly identifies compromised hosts and quarantines any affected devices.

Cyber Threat Hunting

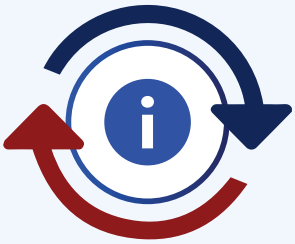
This approach proactively looks for threats that aren't picked up by the risk and vulnerability solutions in place. There are various types of threat hunting teams and technologies, each with unique specializations, so identifying which is the best fit for an organization is crucial. Threat hunting tools should conduct an in-depth review of all potentially relevant data, as opposed to other specific categories of tools that focus on information relevant to their immediate use or mission.

Malware Analysis

A malware analytics tool should identify patterns of attack and the operation of any malware that makes it into an organization's systems. In the case of infection by a known threat, steps can quickly be taken to contain and mitigate the damage that has occurred. Malware analysis tools assist in threat hunting and incident response, enabling analysts to reduce the time it takes to respond to a breach.

Recovery

Having a robust recovery solution in place in the event of a worst-case attack is paramount to restoring functionality. Recovery tools provide an automated approach to building resiliency across the organization and increasing the efficiency of continuity and recovery teams. By identifying the most critical areas of the business, effectively handling day-to-day incidents, and establishing and testing recovery plans, organizations can respond swiftly in crisis situations to protect ongoing operations.



Information Sharing and Awareness

Information sharing is a critical component to ensuring that organizations are aware of the latest threats and can respond effectively. Information exchange between public and private parties is imperative—the former owns the election process, while the latter owns and operates a significant portion of critical infrastructure and provides a majority of the leading detection and response tools available. Ensuring the holistic integration of an organization's security infrastructure allows cybersecurity and response tools to work to the fullest extent.

Integration Strategies

In recent years, many vendors have worked together to ensure that their tools align in goals and technology. Many of these vendors have even published applications, modules, or documentation that facilitate a painless integration. The advantages of integrating multiple tools should not be underestimated. For example, many monitoring-specific solutions excel at correlating data and identifying threats but have little or no management capabilities.

These tools can be configured to automatically take action based on triggered alerts, such as quarantining a host, blocking a URL, and preventing incidents. This not only enhances security but also reduces the analyst's workload.

Integrating monitoring and management tools allows a security team to have one tool that excels at identifying the threat and can feed that information directly to an endpoint, next-generation firewall, or network management tool. This approach could have made a difference in the 2020 election—had alerts been set up to notify administrators that their compromised contractor had activated vulnerable remote connection software to access a state's voter list management tool, those connections could have been terminated before the risk was introduced.

Threat Intelligence Feeds

Many vendors have published lists of IP addresses and domains that have linked to malicious actors. There are entire teams dedicated to researching their attack patterns and methods and obtaining access to this information would assist in securing election infrastructure as you would be able to proactively block any attempts to connect from these bad actors. Or if personnel attempts to navigate to a malicious domain it would be immediately blocked.

DHS and CISA Programs

There are many DHS and CISA initiatives that facilitate information sharing and cybersecurity awareness. These include the Cyber Information Sharing and Collaboration Program (CISCP), the Information Sharing and Analysis Centers (ISACs), Information Sharing and Analysis Organizations (ISAOs), Automated Indicator Sharing, Protected Critical Infrastructure Information Program (PCII), Homeland Security Information Network, and subscription-based information designed by the National Cybersecurity and Communications Integration Center. Through these programs, CISA has developed ways to share information with the private sector as well as state, local, tribal, and territorial governments, and international entities. More information about how to enroll or become associated with these programs can be found at https://www.cisa.gov/information-sharing-and-awareness.

Training and Career Development

Security tools can only be as effective as the administrators configuring them or the analysts using them. With a growing shortage of cybersecurity analysts—a gap that reached 1.8 million in 2022—it is paramount to maximize the abilities of each analyst on a team. Training is essential to establishing a proficient cybersecurity workforce and keeping current cybersecurity workers up to date on skills and evolving threats. It's also important to train end users on best practices so they can avoid compromise through negligence and recognize threats as the first line of defense.

End User Training

Many incidents and breaches occur because of a lack of awareness from the end user, resulting in higher risk exposure and higher fatigue for the security teams at organizations. End user training can greatly reduce an organization's risk. When choosing how to conduct end user training—or whether to use a third party to do so—it is important to look for data that validates the effectiveness of the training.

Look for organizations with reportable reductions in introduced threats by end users.

Some organizations working with top third-party training providers have reported up to a 95 percent reduction in malware and viruses over a period of two years.

Such training further validates and reinforces end user knowledge by periodically testing end user response to potentially malicious messages or links through fake phishing emails or other penetration testing.

Analyst Training

Consistent and continuous training provides analysts and other cybersecurity professionals the ability to learn best practices and build proficiency in identifying and responding to an evolving landscape of threats. Some of this can be accomplished internally, but many organizations invest in third-party training teams that specialize in training SOC analysts and others in quickly identifying and responding to incidents and breaches. Such training should simulate real-world circumstances to provide the most value to security teams.

Vendor Training and Certifications

Security teams must know how to effectively use the tools at their disposal—most vendors offer training tracks that provide detailed and hands-on approaches to using their technology. Vendor education—both formal, through longer purchased classes, and informal, through workshops or webinars—can help close the cybersecurity skills gap. Many of these come with certifications to validate the knowledge so that organizations can be confident in their ability to use a tool to maximum effectiveness.

CISA's election security best practices will be rolled out at the national, state, and local levels in the lead up to the November elections. Further, election security will be an ongoing process as we collectively engage in various elections across the country each and every year. A densely layered approach of assessment, detection, and mitigation tools, along with ongoing training and public-private partnerships, will strengthen the electoral process. Moreover, the approach CISA recommends can be used by any organization looking to harden its digital infrastructure.

carahsoft.

Carahsoft is able to assist in securing public sector election infrastructure due to its unique position in the supply chain for IT resources for public sector. Carahsoft has access to the state and federal contracts from a procurement standard. Furthermore, Carahsoft's relationship with cybersecurity vendors allows them to make informed recommendations to any IT personnel that might be responsible for securing election infrastructure. With numerous subject matter experts in house who have learned about election systems and the threat vectors facing them, Carahsoft is able to offer cyber consultations to evaluate an agency's current security posture and thereby provide recommendations to fill any gaps that could potentially compromise the integrity of our nation's elections.

www.carahsoft.com sales@carahsoft.com 703-871-8500