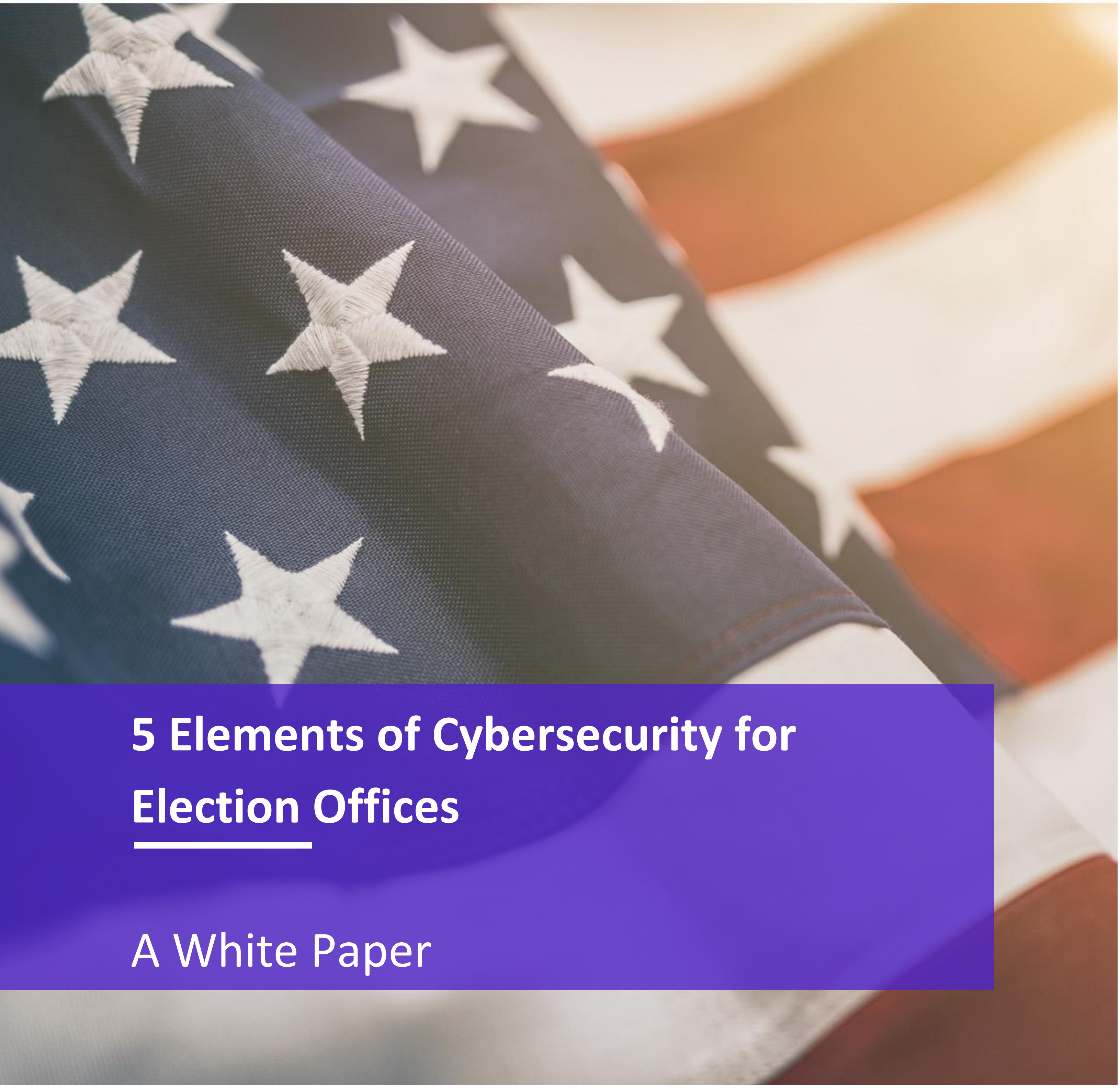
SMARTMATIC



5 Elements of Cybersecurity for Election Offices

A White Paper

January 2023

In a survey of 5,400 IT managers in 30 countries (including those in government), 61% of respondents reported increased cyber-attacks on their organization in 2020. Respondents working in central government positions reported the largest increase in attacks (74%) among all sectors – public and private – represented in the survey. Further, 54% of all respondents said cyberattacks are now too advanced for their IT team to deal with on their own.[i]

There's more bad news for US organizations in particular. According to a report by Microsoft, the US was the target of 46% of all cyberattacks recorded between July 2020 and June 2021 – more than double that of any other country.[ii]

These trends affect election organizations as well. Even jurisdictions that exclusively use paper ballots typically rely on electronic solutions for voter and candidate registration, vote tabulation or communicating results to citizens. Thus, cybersecurity is an issue for elections personnel at every level.

This whitepaper will look at applied cybersecurity for elections. It will cite industry best practices and offer recommendations for self-guided organizational assessment and practical first steps toward better cybersecurity.

The Threat Environment

We all know that the world is increasingly digital and that includes elections, too. In the elections space, digital technology is used to varying degrees to support some or all of the following:

- Political campaigns;
- Communication via the media;
- Supply chain;
- Voter registration;
- Casting of ballots;
- Counting of votes; and
- Dissemination of results.

Vulnerabilities in any of these may make it a target for malicious actors seeking to undermine the legitimacy of democratic elections. Examples of attack vectors that could be used against election organizations and processes include:

- Spear phishing;
- Distributed Denial-of-Service (DDoS) attacks;
- Data theft; and
- Malware infection.

Any examination of election cybersecurity must be holistic and address both technical security measures and the many human factors that affect security. According to the World Economic Forum, 95% of cybersecurity breaches are caused by human error.[iii] These errors, along with poor cyber-hygiene, can create vulnerabilities. These can include:

- Weak or “recycled” passwords;
- Sharing credentials, log-in IDs or passwords;
- Writing passwords on papers or files;
- Failure to purge users no longer employed; and
- Lack of knowledge and cyber-fatigue (apathy towards security measures).

The Five-Element Approach to Cybersecurity

Any holistic approach to sound cybersecurity for elections requires a multi-pronged effort that spans systems and the people who use them. While no cybersecurity strategy is foolproof, the following methodology is proven effective in deterring and mitigating cybersecurity issues. It has five core principles**:**

- Defense in Depth;
- Zero Trust;
- Least Privilege;
- Segregation of Duties; and
- Transparency.

These principles comprise a sound strategy for defending election infrastructure and generating credible evidence to prove that the election results are legitimate and trustworthy.

Defense in-depth: Defense in Depth is an approach devised by the military to protect its systems. Rather than a single, systemwide security measure, this strategy relies on multiple protocols and processes to create layers of protection. Evidence has shown that defeating several different and overlapping structures is far more difficult and time consuming than defeating a larger single security measure. Sometimes, a little bit of extra time is all that is needed to identify a cyber-incident and prevent it from succeeding.

In the elections space, example layers are surveillance cameras covering facility entrances and tabulation rooms, personal credentials (such as card key badges to enter sensitive areas), followed by account passwords, then encryption, asymmetric keys and digital signatures for data protection.

Zero trust: Zero trust is an approach to security architecture that assumes every interaction begins in an untrusted state. This applies to both people and to system functions. In its simplest terms, this approach requires all users and operations – internal or external – be initially authenticated and then be re-validated every time a new function or contact is initiated.

For example, a staff member must enter their credentials every time they log on to the network *and* every time within that session they attempt to access a different critical component in the network, such as a voter-registration database. The same holds true if that user leaves the database and attempts to re-enter the same database within the same network session.

This same model also applies to system components. An authenticated server that queries a database must be programmed to re-authenticate for each new query session.

Zero trust also demands that all of these authentications and validations be logged to a protected record. This creates a tool for forensic investigation should a breach occur.

Least Privilege: The Least Privilege principle is a containment strategy that ensures that each person, process or program can access only the information, resources or controls necessary for completing assigned tasks. This applies to both people and to system functions. For example, a sub-routine within a computer program should only have to access the networked databases necessary to complete its function and no others.

Elections involve thousands of workers and pieces of computer hardware and software. Containing access drastically reduces the potential for a system breach to spread. It also reduces mitigation time and efforts, since the compromise is confined to a known network segment or other definable portion of the deployed technology.

Segregation of Duties: Segregation of Duties is an assignment and approval strategy that is primarily designed to mitigate the impact of corruption and/or collusion among key individuals. The two key elements are: splitting duties among individuals and requiring combined consent for critical decisions, changes and access to vital system features and data.

Spreading essential duties among non-aligned personnel means that no one person can undermine multiple processes and procedures. This separation also increases accountability. In this way it is somewhat similar to Least Privilege: containing access drastically reduces the potential for any compromised situation to spread. The second element – combined consent – reduces the chances of collusion among individuals to compromise a system.

Transparency: Ensuring transparency in elections is critical to engendering trust in processes and outcomes. Transparency efforts must be easy for those outside the organization to understand and corroborate. Tools that support transparent processes include system certifications, system audits and producing both digital and paper artifacts of things like votes and tally reports. Cryptography further strengthens trust in transparency efforts, ensuring confidentiality and security.

Transparency efforts should also be applied to the human aspects of elections. This can include vetting processes for new hires, background checks, and activity logs that show who accessed physical sites and digital systems. Audits that can be observed and verified by interested citizens also contribute to transparency.

Practical Steps Toward Cybersecurity

Preventing a cybersecurity incident is a never-ending process of continuous evaluation and improvement. The greatest challenge in this, however, is that the goalposts are continually moving. Those with malicious intent work just as hard to overcome your security measures as you do in creating them. That said, there are some practical measures you can take as you work toward improvement.

Assess the risks: The first step in mitigating risk is to assess it and your organization's security environment. This process, however, is far too big to detail here. *Securing U.S. Elections: A Method for Prioritizing Cybersecurity Risk in Election Infrastructure* by Quentin E. Hodgson, et al, is an excellent fact-based guide to help election officials implement their own risk assessment. It was published in 2022 by the Department of Homeland Security (DHS), in conjunction with the nonprofit research organization RAND Corporation. The report is free to download.[iv]

Become and stay informed: Stay on top of updates from the Department of Homeland Security's Cyber Security and Infrastructure Security Agency (CISA) and other cybersecurity experts. Don't limit your research only to election systems. Virtually all information targeted to private industry and government has some application in election organizations.

Educate voters: Mis- and disinformation are inextricably entwined with cyberattacks. States and jurisdictions can help counteract misleading information by encouraging voters to rely on trusted sources, first and foremost their own website. Further, educate voters on your organization's actions to add new protections or enhance existing ones. Nothing is too small. Are staff taking cybersecurity training? Publish the news to your website.

Collaborate and cost share: Budgets and resources are always at issue. So remember that elections aren't the only targets in government for cyberattacks. Look to other departments within your local, regional or state government to form "buying co-ops" so costs for cyber defenses and other security upgrades can be spread across more budgets.

Get expert help: Election organizations can easily become overwhelmed with cybersecurity issues, so outside support is a good idea. *The State and Local Election Cybersecurity Playbook,* published by the Belfer Center for Science and International Affairs, Harvard Kennedy School, recommends using "external resources to assist in improving cyber defense capabilities and building expertise." The report suggests experts such as the cybersecurity centers in the National Guard, computer science centers at universities, and technology providers within the election space. Many technology providers are members of the Homeland Security Sector Coordinating Council, which helps the entire election ecosystem to share information and build capacity to thwart attacks on US elections.

[i] "The IT Security Team: 2021 and beyond", whitepaper by Sophos, June 2021; downloaded on January 4, 2023 from https://assets.sophos.com/X24WTUEQ/at/hr6gj5b5v8btxpq68xqh34/sophos-it-security-team-2021-beyond.pdf

[ii] Microsoft Digital Defense Report, October 25, 2021; downloaded on January 5, 2023 from https://www.microsoft.com/en-us/security/blog/2021/10/25/microsoft-digital-defense-report-shares-new-insights-on-nation-state-attacks/

[iii] After reading, writing and arithmetic, the 4th 'r' of literacy is cyber-risk, Paul Mee, et al, December 17, 2020; downloaded from https://www.weforum.org/agenda/2020/12/cyber-risk-cyber-security-education

[iv] Download available at https://www.rand.org/pubs/research_reports/RRA512-1.html