FEDINSIDER.COM | WHITEPAPER

FEDInsider

WHITEPAPER

Protecting Elections and Enterprises with Innovative Cybersecurity Defenses

carahsoft

CARAHSOFT.COM

carahsoft

ELECTION SECURITY

Elections are the foundation of our democracy, and securing public sector election infrastructure is critical to ensuring its protection. As a government IT solutions provider, Carahsoft is uniquely positioned to help provide the technology that keeps elections secure and citizens informed.

Carahsoft holds numerous federal, state, and local contract vehicles to simplify the government procurement process. Our relationship with cybersecurity and complementary vendors allows us to make informed recommendations to any IT or Cyber personnel who is responsible for securing election infrastructure. We also employ election security experts who have learned the election systems and threat vectors facing them, allowing them to accurately match our entire cybersecurity and citizen engagement portfolio with our customers' specific needs.

Carahsoft has assembled a robust collection of tools and training critical for protecting the nation's most important elections and voting assets. A comprehensive approach to securing elections infrastructure needs to include voter outreach, cybersecurity assessments, information sharing, awareness training, and detection and preventions tools.

VOTER OUTREACH & ENGAGEMENT

Adobe · GRANICUS · Hootsuite · mapbox · New Relic · tableau

ASSESSMENT

bugcrowd · CONTRAST SECURITY · EXPANSE · F5 · GitLab · MICRO FOCUS Government Solutions · NowSecure · Qualys · RAPID7 · RISKSENSE · SecureWorks · tenable

INFORMATION SHARING

Akamai · Attivo NETWORKS · exabeam · IronNet · Recorded Future · ThreatConnect · THREATQUOTIENT

TRAINING

COFENSE · Global Knowledge · Inspired eLearning · RANGEFORCE

PREVENTION, DETECTION, & RECOVERY

aws · vmware Carbon Black · Centrify · druva · exabeam · fidelis Cybersecurity · FIREEYE · FORESCOUT · FORNETIX · Gigamon · Lookout · McAfee · okta · paloalto NETWORKS · proofpoint · RSA · SailPoint · NS2 · solarwinds government · splunk> · THALES · Trustwave Government Solutions · VERITAS

Carahsoft's election security solutions are available through its reseller partners on a variety of contracts including Carahsoft's GSA Schedule 70, NASPO ValuePoint, NCPA, OMNIA Partners, and additional state and local contracts. To learn more, visit Carah.io/SLG-Contracts.

11493 SUNSET HILLS ROAD, SUITE 100 | RESTON, VA 20190 | 888.662.2724 | CYBERSECURITY@CARAHSOFT.COM

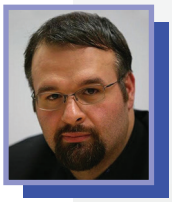
FEATURED CONTRIBUTORS:

- **Justin Herring**
  Exec. Deputy Superintendent, NY Department of Financial Services

- **Dan S. Wallach**
  Professor, Dept. of Computer Science, Rice University

- **Justin Berardino**
  Operations Manager, Orange County Registrar of Voters

- **Sumit Sehgal**
  Chief Technical Strategist, Government Healthcare & Education, McAfee



- **Marc Rogers**
  Executive Director, Cybersecurity Strategy, Okta

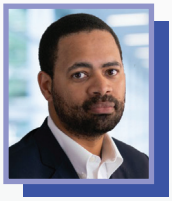
- **Dr. Juan E. Gilbert**
  Endowed Professor & Chair, Computer & Info., Sci. & Eng. Dept., University of Florida

- **Paul Lux**
  Supervisor of Elections, Okaloosa County, FL

- **Benjamin Hovland**
  Commissioner, U.S. Election Assistance Commission

- **Pete Zurbach**
  Vice President of Innovation, NS2 Labs

- **Steve Moore**
  Vice President & Chief Security Strategist, Exabeam



- **Maurice Turner**
  Senior Advisor to the Executive Director, U.S. Election Assistance Commission

- **Daniel Persico**
  Chief Information Officer, Virginia Department of Elections

- **David Levine**
  Elections Integrity Fellow, Alliance for Securing Democracy

- **Steven Feldman**
  Intelligence Analyst, Foreign Influence Task Force, FBI

- **Mark Loveless**
  Senior Security Researcher, GitLab

- **Alex Whitworth**
  Director, Core Cyber, Carahsoft

Both private companies and government institutions have their cybersecurity defenses tested all the time. Attacks are commonplace regardless of an organization's size or their industry. As such, good cybersecurity and all of the various techniques and tactics used by defenders to protect their networks and assets have become a fundamental requirement for conducting any kind of business or online activity.

In this environment, it's easy to dismiss the war between cyber attackers and IT defenders as a commonplace occurrence that happens every day. But there are certain times when cybersecurity is truly challenged, when hackers will try anything to hurt an event or activity. And within the list of high profile targets, it doesn't get any more serious than a United States presidential election. There are many well-funded attackers, with some even backed by nation states, that would literally do anything to disrupt or corrupt an election.

A collation of speakers from government, industry and educational institutions gathered to discuss these important issues during a series of FedInsider webinars sponsored by Carahsoft. Their insight, lessons learned and best practices from those events are highlighted throughout this whitepaper.

In this battle, attackers have a lot of advantages. The possible attack surface runs through every city, state and county from coast to coast. And even if they can't find a weak point, simply undermining confidence in the voting process might be seen as a victory for them.

"One of the challenges in election security is managing the countless ways bad actors can attack or influence systems," said Alex Whitworth, Director, Carahsoft's Core Cyber team. "This includes the hacking of voting machines, 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."

The good news is that despite some initial disadvantages in terms of an election's configuration, defending it can be done with the same level of training, tools and tactics used to protect critical infrastructure every day. In fact, a high profile election can be used as the ultimate test of those defenses, drawing on years of cybersecurity experience to harden and protect it. And once a safe election has been completed, lessons learned during that exercise can then be applied back to the daily cybersecurity activities that protect governments and private businesses every day.

"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," Whitworth said. "A comprehensive approach to securing elections infrastructure needs to include cybersecurity assessments, detection and prevention tools and processes, information sharing, and awareness training."

TRADITIONAL THREATS RAMP UP FOR ELECTIONS

There are a lot of unique characteristics regarding elections, which gives attackers leeway to try new things. But the bulk of the incidents are going to be more traditional attacks leveled against the networks set up to support elections. Attackers don't need to reinvent the wheel if they can find a weak link protecting an election.

"In terms of specific technical threats, one that we're really concerned about is spear phishing, as there's been heightened activity with that, and it can be really effective," said Orange County Registrar of Voters Operations Manager Justin

Berardino. “So when we’re addressing this along with any other threat, we have to make sure we’re approaching it from all the controls: the administrative aspect, the technical, and the physical. For example, for spear phishing, that includes extensive training on the administrative side, ensuring we have the correct email filters in place, and that we have a system to automatically check any link that anybody clicks on.”

Mark Loveless is a Senior Security Researcher for GitLab. Moving forward, he expects to see a lot of attacks every time an election is held, but is confident that good cybersecurity practices and cyber resilience can prevent anyone from damaging the voting process. This will be especially true if we can open up the process to examination so that everyone will feel confident that their vote has counted.

“There is a lot of conventional danger. One of the cures for some of that is just making sure we develop that confidence. I don’t know if we have time to do this before this election, but certainly moving forward, we need to put methods in place where we can actually trust the entire process,” Loveless said. “And also, we need to make that whole process as open as possible, so that we all can examine it, and we can all trust it.”

Executive Deputy Superintendent for the New York Department of Financial Services, Justin Herring also runs his state’s newly formed cybersecurity division. While speaking at a recent FedInsider Election Security webinar, he agreed that solid cybersecurity practices are the best defense no matter what system is being protected.

“Regardless of what you are defending, a lot of the fundamentals are the same like cybersecurity hygiene measures, robust asset inventory, doing a risk assessment and making sure that you have a program tailored to your risks, and also patching and access management,” Herring said. “This is true in part because the methods that attackers are going to be using are often going to be very similar. It doesn’t matter what their objective is, hackers specifically use attacks like phishing, exploiting unpatched systems, and looking for unsecured ports. So whether it’s an election hack or a financial hack, it’s the same type of threats that you have to be worried about.”

Vice President of Innovation for NS2 Labs, Pete Zurbach agreed, and added that documents like the NIST Cybersecurity Framework can be invaluable resources to help configure good cybersecurity practices. The framework can be used to create a baseline of security and present a unified front against attackers.

“There’s 8,800 election officials across the county,” Zurbach said. “So with elections handled at the local level, I think it’s very valuable to have a common reference report such as the NIST Cybersecurity Framework to help form and tie approaches together across the country and to give an idea of some easy steps to improve security.”

A BURDEN SHARED IS A BURDEN HALVED

The Chief Technical Strategist for Government, Healthcare and Education for McAfee, Sumit Sehgal says that in addition to good cybersecurity, information sharing is paramount. For local governments that is handled best by the Multi-State Information Sharing and Analysis Center (MS-ISAC).

“MS-ISAC is good for that, and I like the pace that they’re getting information that’s needed from a security perspective to make decisions, or to see where some potential improvements could also be made,” Sumit said. “And then they are reaching out and doing educational efforts and outreach to citizens within their local counties or at the state level to make them more aware of things like the effects of phishing and basic security hygiene from a consumer’s point of view.”

Senior Advisor to the Executive Director of the U.S. Election Assistance Commission (EAC) Maurice Turner added that the commission exists to help local governments safely run elections. "EAC has been around for almost 20 years now, being established with the Help America Vote Act, and so that really guides our efforts to make sure that we're developing the voluntary voting system guidelines," Turner said. "We're a national clearinghouse of information for election administration officials, so we can put those best practices out there and help make sure that at every step along the way the voter is confident in the process."

In addition to just sharing information between government groups, the Executive Director of Cybersecurity Strategy for Okta, Marc Rogers recommends partnering government agencies with civilian groups of experts. One that Rogers works with is called the CTI League, a global volunteer emergency response community which has recently been working in the area of election security.

"Some of the things that we've tackled within the CTI League have amazed me in terms of how fast we can resolve issues," Rogers said. "We've identified critical vulnerabilities in major government institutions, taken down campaigns exploiting them, and had the infrastructure vulnerability fixed in a matter of hours--something that would normally take days or even weeks."

Some states like Virginia are taking their partnerships seriously, especially to deal with newer threats like disinformation.

"I am very concerned with misinformation and disinformation and combating that is one of the areas that my leadership team is focused in on," said Chief Information Officer of the Virginia Department of Elections Daniel Persico. "One of the ways that we are dealing with those type of things is by establishing great partnerships not only with other state, local, and federal entities, but also organizations like social media platforms and things like that."

And it is those kinds of government and private sector partnerships that can be the most effective in securing an election or any kind of infrastructure.

"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," Whitworth said. "Information sharing is a critical component to ensuring that organizations are aware of the latest threats and can respond effectively."

DISINFORMATION: AN OLD THREAT CLOAKED IN NEW TECHNOLOGY

Disinformation campaigns have been around for a long time, but they were most often confined to the realm of international spies and military intelligence. Now it is emerging as a mainstream threat, especially in elections.

Vice President and Chief Security Strategist at Exabeam, Steve Moore studies this issue. He says that the United States got a first glimpse of Russian disinformation campaigns when a spy named Yuri Bezmenov defected to Canada in the 1970s. He showed Western governments how Russia was using subversion, active campaigns and psychological warfare to try and change attitudes over time. Those efforts have not changed very much, but the tools available to attackers have advanced considerably.

"The first step of this, which is sort of this demoralization or producing disinterest in whatever the topic is, used to take sometimes

a generation or more to take hold or to have any effect," Moore said. "Now with social media, Instagram, Facebook and other sorts of similar mechanisms, it may only take months."

Endowed Professor and Chair of the Computer, Science and Engineering Department at the University of Florida, Dr. Juan E. Gilbert studies election security. He says that disinformation campaigns will likely be the biggest threat to elections moving forward.

"From my perspective, that's going to have the most potential influence on elections," Gilbert said. "Meaning that people getting mis- and disinformation decide not to vote, or vote based on the wrong information one way or another. As far as someone actually hacking some machine and changing votes, that threat in my opinion has a much lower chance of actually happening."

Paul Lux is the Supervisor of Elections for Okaloosa County in Florida. He worries about disinformation campaigns because they are outside of his direct control, but says that county election boards can fight back by having the correct information ready to disseminate.

"If something does happen," Lux said, "we have created a group who are educated and who can speak to the issue and talk with those who voice concerns to control the spread of disinformation."

And ensuring that election results can be trusted will be a powerful weapon against disinformation used to discredit the election according Dan S. Wallach, Professor of the Department of Computer Science at Rice University.

"For jurisdictions that are using paperless electronic voting machines, it's time to start a procurement process to replace them," Wallach said. "For jurisdictions that have hand marked paper ballots, risk limiting audits are very effective and efficient and have been used in a number of real elections in real places like Michigan and Rhode Island."

Even the FBI is working to neutralize disinformation campaigns. Steven Feldman is an Intelligence Analyst for the FBI working with the Foreign Influence Task Force. He told a recent FedInsider podcast audience that disruption campaigns are not a new threat and can be countered.

"The FBI is already hard at work combating disruption campaigns," Feldman said. "The important thing to remember is that our adversaries start their influence campaigns a year or so out from elections, so we've actually already been in the thick of things for a while. And while the American people are thinking about something else, behind the scenes we've had our election strategy in place with our dedicated special agents and analysts already working all of the threats related to elections."

ELECTING FOR BETTER SECURITY

Elections will always be high profile targets for the worst kinds of threats and threat actors. But it's not like anyone should be surprised by this anymore. Knowing that any election could be attacked, either directly through traditional cybersecurity channels or indirectly through disinformation campaigns, puts defenders on alert. Armed with that knowledge, election officials can be ready to counter all threats with a combination of good cybersecurity practices, information sharing with other jurisdictions, and by forming good partnerships with security and IT firms from the private sector that can provide valuable expertise and support.

That total defensive strategy was created for the 2020 presidential election, and will act as a template to support all future voting activities.

"One of the great things about my job is that I get to see up close all of the amazing work that election officials do across the country," said Commissioner of the United States Election Assistance Commission Benjamin Hovland. "And I really can't overstate how well election officials have responded to both the foreign interference we saw in 2016 and the issues associated with the COVID-19 pandemic."

Other experts agree that the situation is improving. "There could still be improvement from some places in monitoring and auditing practices, and there are some states that don't monitor or audit their input forms to protect against malicious input, and that's really important because obviously in 2016, in a small number of cases, we saw Russia being able to infiltrate or breach voter registration databases," said Elections Integrity Fellow with the Alliance for Securing Democracy David Levine. "But I think it is important to note that broadly speaking, progress has been made."

Private sector companies including Carahsoft and its IT solutions providers are proud to do their part in defending voting and keeping up public confidence in this cornerstone of democracy.

"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. We have access to the state and federal contracts from a procurement standard," Whitworth said. "Furthermore, our relationship with cybersecurity and complementary vendors allows us to make informed recommendations to any IT or cyber personnel who is responsible for securing election infrastructure. We have subject matter experts who have learned the election systems and threat vectors facing them who are able to offer consultations and recommendations for products to fill in any gaps in a cybersecurity stack."

MORE FROM CARAHSOFT

If you would like to learn more about securing our elections, check out our on-demand webinar series and listen to the accompanying podcasts, *Election Security: The Foundation of Democracy*. Watch now: https://carah.io/Election-Security.

Hosky Communications Inc.
3811 Massachusetts Avenue, NW
Washington, DC 20016

(202) 237-0300

Info@FedInsider.com
www.FedInsider.com
@FedInsiderNews
Linkedin.com/company/FedInsider/
@FedInsider

Carahsoft Technology Corp.
11493 Sunset Hills Road, Suite 100
Reston, VA 20190
Contact: Alex Whitworth, Director, Core Cyber

(703) 871-8626

ElectionSecurity@Carahsoft.com
Carah.io/Election-Security/
Facebook.com/Carahsoft/
Linkedin.com/company/Carahsoft/
@Carahsoft