FEDInsider

Identifying and Mitigating Election Security Threats in 2024

State and local governments are preparing for the election year by leveraging federal and private sector partners along with security tools to uphold election integrity.

Security is top of mind for election officials this year, especially considering past events and the rise of cyber threats. Since individual states are responsible for conducting elections, the National Association of Counties held workshops and panels at its annual legislative conference on the threats facing election workers and voters. Physical threats remain a concern, but election officials can also face doxing, swatting and ransomware attacks. Voters themselves might additionally encounter things like malicious text messages or misinformation campaigns redirecting them to fake polling locations.

Thought leaders from government and industry recently spoke at a FedInsider panel to discuss election security challenges and the steps officials can take to prepare for threats before Election Day.

Preparing for Threats Impacting Election Integrity

"The 2020 election saw a range of cyberattacks, DDOS events and vendor supply attacks," said Lester Godsey, chief information security officer of enterprise technology for Maricopa County in Phoenix, Arizona. In addition to monitoring those types of threats, state and local officials must also consider misinformation campaigns, some of which could encourage violent acts. This calls for monitoring "various media to look for indicators of potential increased cyber threats as well as kinetic or physical effects," Godsey added.

Godsey's team has observed various media outlets and seen an increase in activity there that subsequently translates to increased amounts of physical or kinetic threats. "I think it also has to do with how a social media platform is being leveraged," he said. "Some act not only a source of intelligence, but also as a platform where logistics research and things are being done along those lines from an adversarial perspective." It's an evolution his team has had to address and combat.

Ryan Mulhall, chief information officer for Iowa Communications Network, said monitoring is also a huge part of his team's approach to thwart threats that could potentially disrupt the election process – like ransomware.

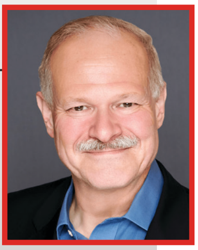
"If you are running an [Endpoint Detection and Response] tooling platform, you need to make sure that you're not only monitoring for threats, but also looking for the check-ins and updates for those tools as well," Mulhall said. "If the tool has not checked in for a week, then it's not necessarily running and protecting you to the best of its ability."

Featured Experts:

- **Lester Godsey**
  CISO, Enterprise Technology, Maricopa County, Phoenix, AZ

- **Ryan Mulhall**
  Chief Information Officer, Iowa Communications Network

- **Jim Richberg**
  Head of Cyber Policy & Global Field CISO, Fortinet



To protect enterprises and networks from DDOS attacks, Mulhall said to look to upstream service providers to help take some of that load, and for help with managing and mitigating bigger threats.

The Triple Threat of Misinformation, Disinformation and Malinformation

Electoral integrity isn't primarily about technical security. Rather, it's about the perceptions of integrity, said Jim Richberg, head of cyber policy and global field CISO at Fortinet, who was involved in the assessment of Russian interference in the 2016 elections.

"If the public doubts the validity and legitimacy of the outcome, you have a problem, and that is what misinformation, disinformation and malinformation (MDM) campaigns really play into," he said. "It's a semi-cyber threat because, yes, we are not out there trying to police social media, but it's really about the flow and transmission of information."

With the increase of foreign actors accelerating their use of MDM and the legitimate use of social media by constituents, the election space has become a multi-actor field. In fact, some of the biggest threats come from Russia, China and Iran actively exploiting social media and trying to increase genuine U.S. societal divisions by using MDM to shape information in favor of candidates who are most favorable to their agenda, according to Richberg. "Frankly, in some cases, they try to paralyze government by heightening hyper-partisanship… if you have a Congress that cannot pass a budget, you don't worry as much about them taking foreign policy actions."

Russia used these tactics during the 2016 and 2022 elections, and China is attempting to follow suit with a slew of fake social media accounts targeting candidates and sharing misinformation. Iran also sent intimidating emails to voters in 2020. Generative AI will only strengthen these efforts.

The reality is that election officials aren't information operations specialists, and it is not their job to know how exactly to counter MDM, Richberg said. He recommends election security teams turn to guidance from the Election Infrastructure Subsector Government Coordinating Council and the Elections Infrastructure Information Sharing and Analysis Center.

MDM is challenging for cybersecurity teams, as it doesn't have to be factually correct – it just needs to gain traction to be threatening. It must cast enough doubt in people's minds to cause the public to lose trust in the election process. "This is something that is very unique and something that maybe not all cyber teams are fully equipped to deal with," Godsey said.

He recommends organizations treat this like a team sport where cybersecurity needs to be involved in planning the overall strategy. And most importantly, communication must happen throughout the entire organization.

Responding to Threats Against Election Security

Securing the nation's elections should also be a team sport between state and local governments, and it is advised they leverage each other as well as all available federal resources. When monitoring cyber activity, Mulhall also recommends organizations adopt endpoint network security solutions and tools, and they should use machine learning to automate anomalies in network behavior. "Prepare now, and do everything you can that is in your best interest," he said.

In addition to potential cyberattacks, physical threats can also be a problem, especially when altercations at voting sites are encouraged by the spread of misinformation on social media. Unruly citizens, death threats to election staff and discourse taken too far can also become a major problem on election day. That's why Godsey's team created an incident response playbook, not only for cyberattacks, but for how to respond to credible threats of potential violence and the physical risk to individuals.

To truly be prepared for the gravity of any attack – physical or cyber – Mulhall relies on collaboration. "When it comes to the state of Iowa, our secretary of state has made cybersecurity – especially around election security – a focus," he said. The state will involve CISA, cybersecurity and election security advisors, and the private sector when necessary.

For Maricopa County, the protocol is similar – Godsey said his team communicates with the state's secretary of state office, CISO, the state fusion center, and both federal and private sector partners to ensure they are up to date on any and all threats or misinformation campaigns they may be facing. "Collaboration has only gotten better, and a lot of it has to do with the role that CISA has played," he said.

Ultimately, panelists agreed that while each state is responsible for the security of its elections, collaboration, training, communication and network visibility are key to upholding election integrity and protecting the election process. Although it will certainly be a difficult challenge, with good collaboration between federal, state, local and private sector partners, the integrity and safety of the upcoming 2024 election can still be secured and protected.

FEDInsider

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

☎ (202) 237-0300
✉ Info@FedInsider.com
🌐 FedInsider.com
f Facebook.com/FedInsiderNews
in Linkedin.com/company/FedInsider
X @FedInsider

carahsoft.

Carahsoft
11493 Sunset Hills Road, Suite 100
Reston, VA 20190

☎ (703) 871-8548
✉ Info@Carahsoft.com
🌐 Carahsoft.com/Fortinet
f Facebook.com/Carahsoft
in Linkedin.com/company/Carahsoft
X @Carahsoft

FORTINET.

Fortinet, Inc.
909 Kifer Road
Sunnyvale, CA 94086

☎ (833) 386-8333
✉ Fortinet@Carahsoft.com
🌐 Carahsoft.com/Fortinet
f Facebook.com/Fortinet
in Linkedin.com/company/Fortinet
X @Fortinet