CISA

CYBER+INFRASTRUCTURE

I-TEAM

How the Russians penetrated Illinois election computers

SQL, an acronym for Structured Query Language, is a database programming language. An "SQL injection" is a common piece of cyber-trickery used to illegally gain access to government, financial, business and private computers. Experts estimate that 8 of every 10 data breaches occur as a result of SQL injection.

The favored tactic of hackers usually begins with certain commands typed on a public web form and ends with broad access to the site's server. In the case of Illinois, after hackers typed a specially-crafted code into the election database search box, records were stolen and the board had to shut down registration for ten days.

"Processor usage had spiked to 100% with no explanation" state investigators determined. "Analysis of server logs revealed that the heavy load was a result of rapidly repeated database queries on the application status page of the Paperless Online Voter Application (POVA) web site" they said.

DDoS Attack Hits Knox County, TN Results Reporting Site On Election Night

By Doug Chapin May 7, 2018

CISA
CYBER+INFRASTRUCTURE

Matt Masterson
February 12, 2020

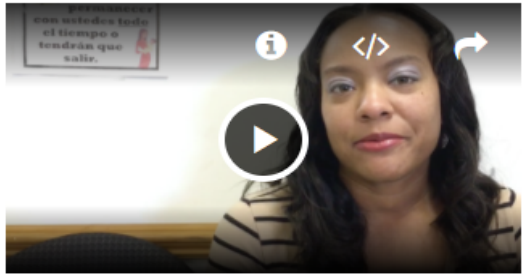
31°
Sign In | Subscribe

The News&Observer

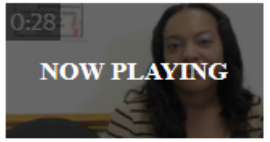
FULL MENU LOCAL NEWS SPORTS LIVING CLASSIFIEDS

North Carolina's elections board provided this image to state lawmakers in a December 2017 presentation. . - State Board of Elections and Ethics Enforcement

VIDEOS



Can food stamps cover the costs of a healthy diet



Can food stamps cover the costs of a healthy diet

Senate leader Phil Berger discusses jail deaths

CISA
CYBER+INFRASTRUCTURE

Ransomware

Six days after a ransomware cyberattack, Atlanta officials are filling out forms by hand

By Kimberly Hutcherson, CNN
Updated 3:00 PM ET, Wed March 28, 2018

Source: WSB

Atlanta mayor: Ransomware an attack on us all 01:38

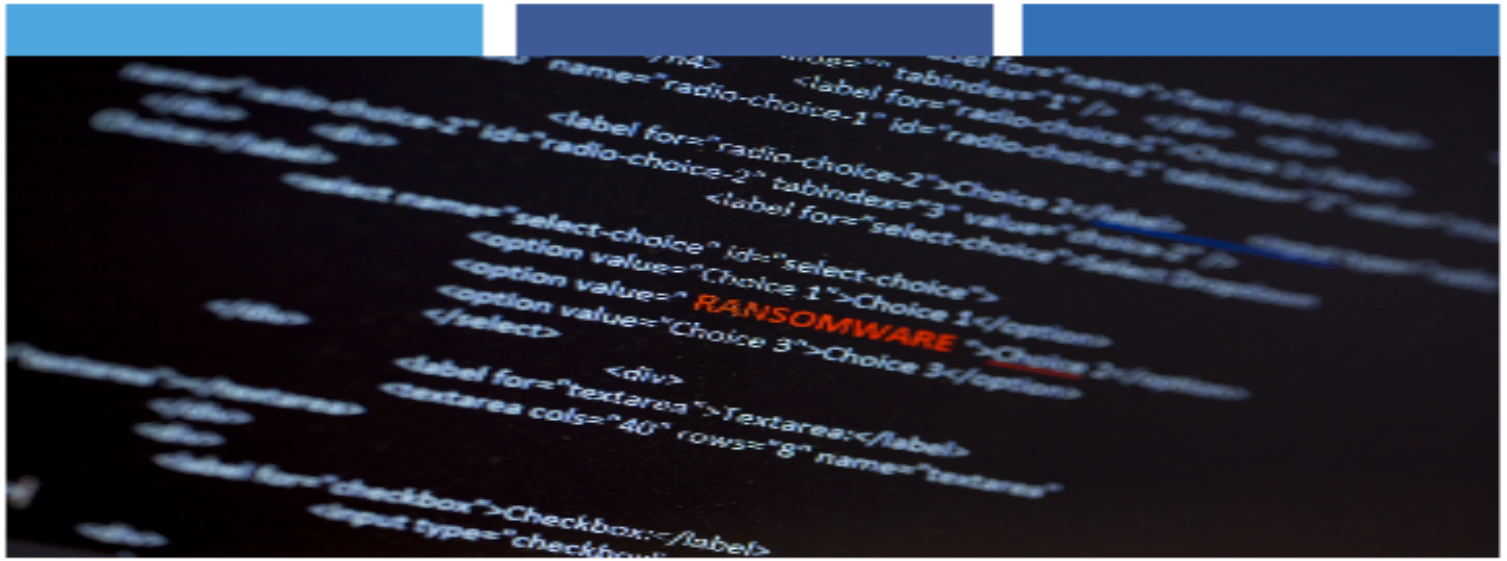
City of Atlanta Needs $9.5 Million More for Ransomware Recovery

Posted by **Kevin Raske**

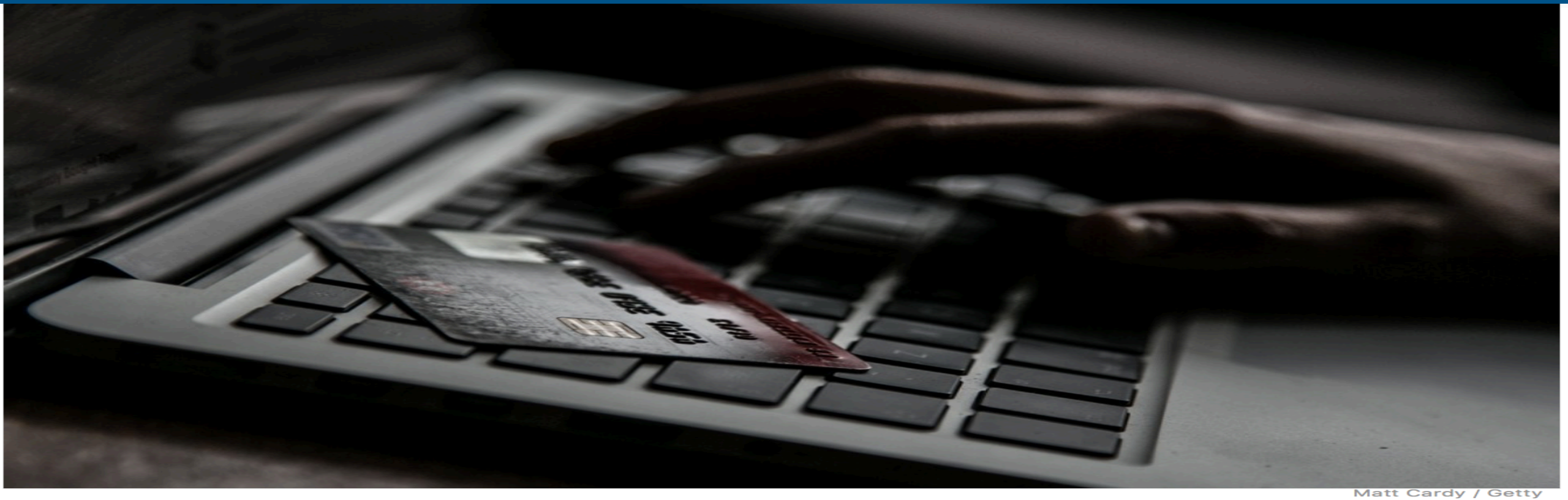
According to **multiple sources**, the City of Atlanta will need to find another $9.5 million to recover from the **"SamSam" ransomware attack which brought their city government to a grinding halt**. The number of applications and government services impacted by the attack has been revealed to be far greater than originally estimated, with the attack even affecting applications of the city police department and court system.

RANSOMWARE THUGS EXTORT INDIANA COUNTY FOR OVER $130,000 IN BITCOIN

By Mark Emem / 13/07/2019 / 3 Min read / In Bitcoin Crime, Cryptocurrency News, News



Ransomware extortionists get another bitcoin payday. | Source: Shutterstock



Matt Cardy / Getty

A Cybersecurity Breach at Equifax Left Pretty Much Everyone's Financial Data Vulnerable

For Americans who want to protect their personal information, there is no way, in our current system, to do so.

GILLIAN B. WHITE | SEP 7, 2017 | BUSINESS

CISA
CYBER+INFRASTRUCTURE

Matt Masterson

February 12, 2020

CISA
CYBER+INFRASTRUCTURE

Matt Masterson
February 12, 2020

POSSIBLE ACTORS

Nation-State Actors

Criminals

Black Hat Hackers

Insiders

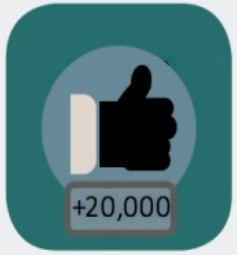
Terrorists

Politically-Motivated Groups

POSSIBLE MOTIVATIONS

Financial Gain

Retribution for Perceived Grievances



Fame and Reputation

Sow Social Division

Foment Chaos / Anarchy

Subvert Political Opposition

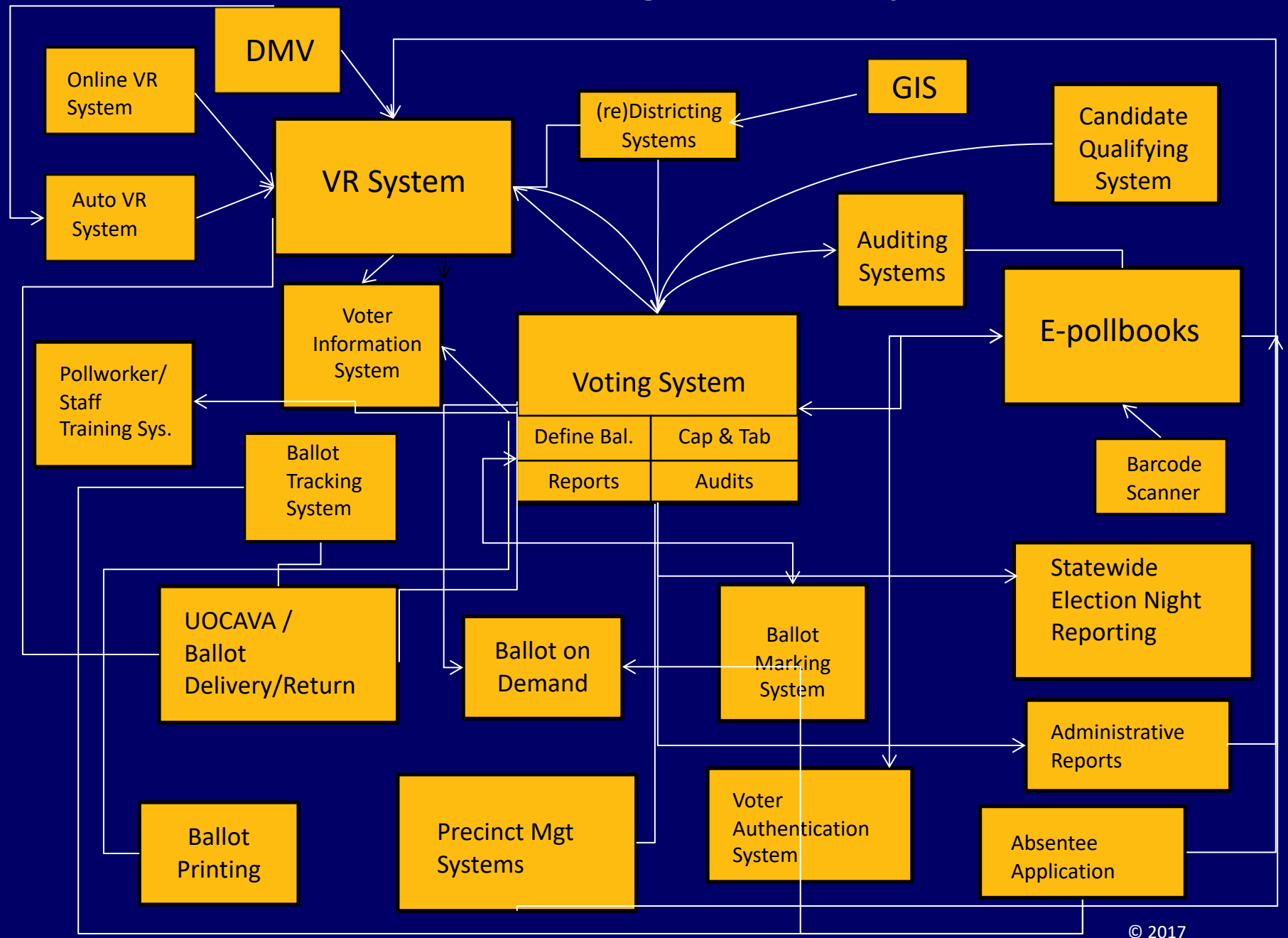
Foreign Policy / National Interests

Undermine Trust in Democracy

Cybersecurity – Common Attacks

- Social Engineering
  - Spear-phishing
- Hacking
  - SQL Injection
  - Port scans
  - Man in the Middle (MITM) Attacks
- Distributed Denial of Service (DDoS)
- Information Operations
  - Leaking stolen information
  - Spreading false or misleading information
  - Amplifying divisive content
  - Interrupting service to public facing online resources

Interaction of Voting and Election Systems

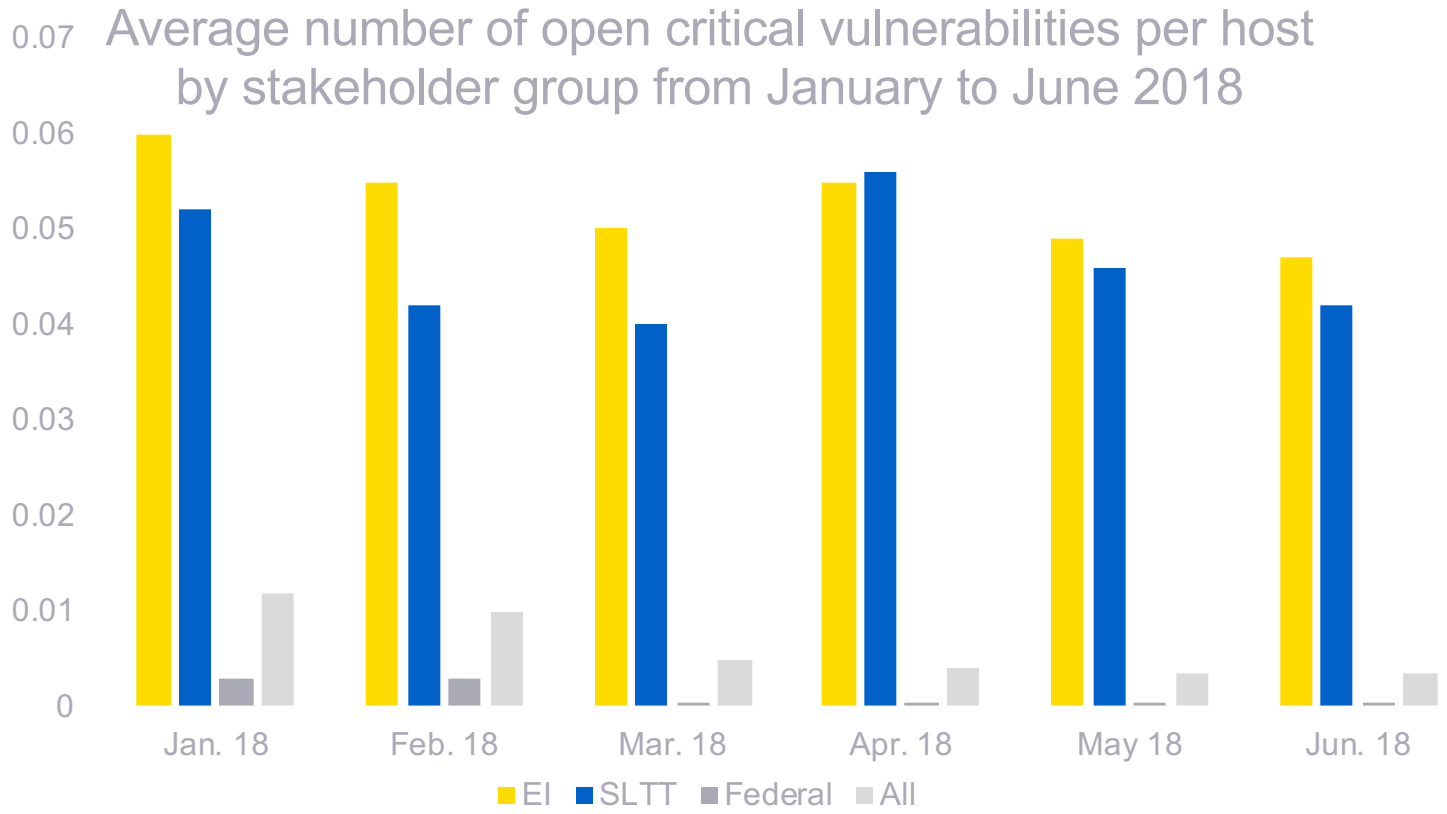


Top Vulnerability Findings Across All Assessments

Finding Description	EI Entities	SLTT Governments	Federal
Spearphishing susceptibility	X	X	X
Spearphishing weakness	X	X	X
Patch management	X	X	X
Administrator password reuse	X	X	X
Insecure default configuration	X	X	X
Clear text password disclosure	X	X	X
Unsupported operating system or application	X	X	X
Easily guessable credentials		X	X
Weak password policy		X	

Top Vulnerability Findings Across All Assessments

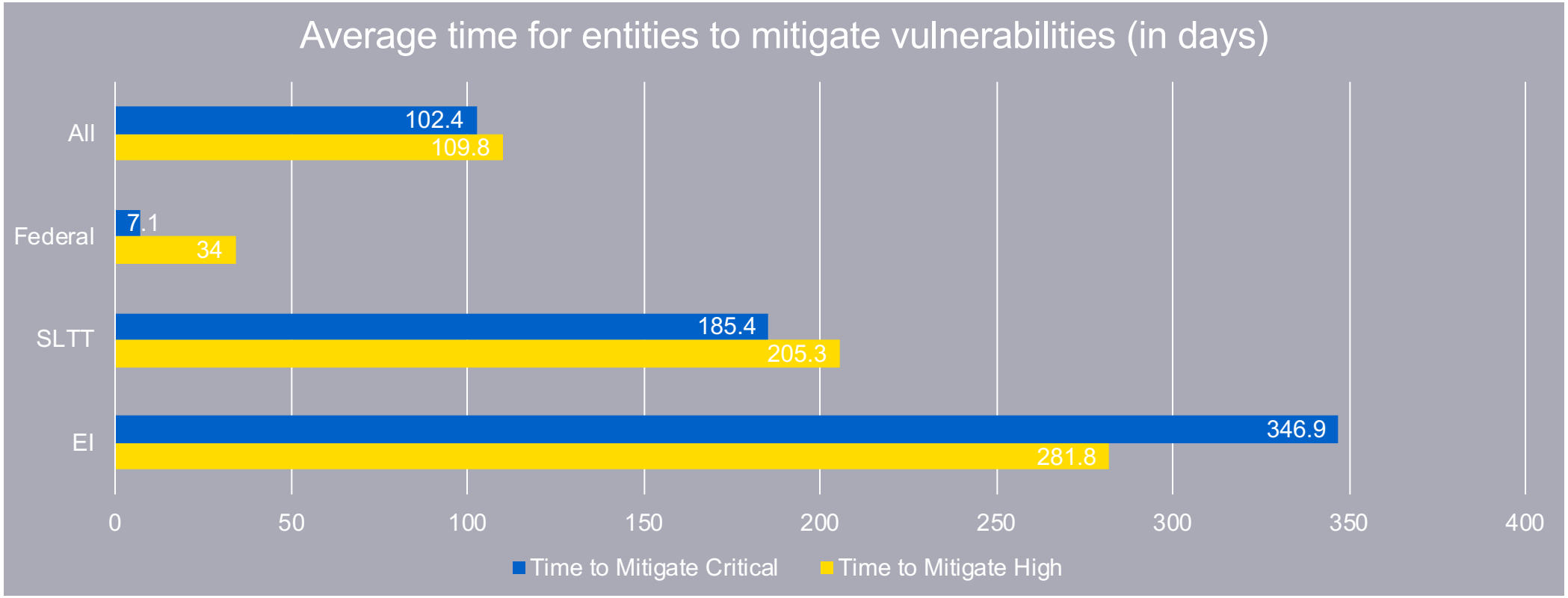
This service tracks and reports the vulnerabilities identified for each system scanned and rates the most severe vulnerabilities identified as a “high” or “critical” severity level. While comparing the raw count of vulnerabilities, or vulnerabilities per sector, is statistically misleading, a comparison of the vulnerabilities, averaged per stakeholder group, provides a snapshot in time to compare across stakeholder groups.



CISA
CYBER+INFRASTRUCTURE

Network Vulnerability Scanning

The time it takes to mitigate vulnerabilities can be important information about the “health” of a network.



Vulnerability to Phishing

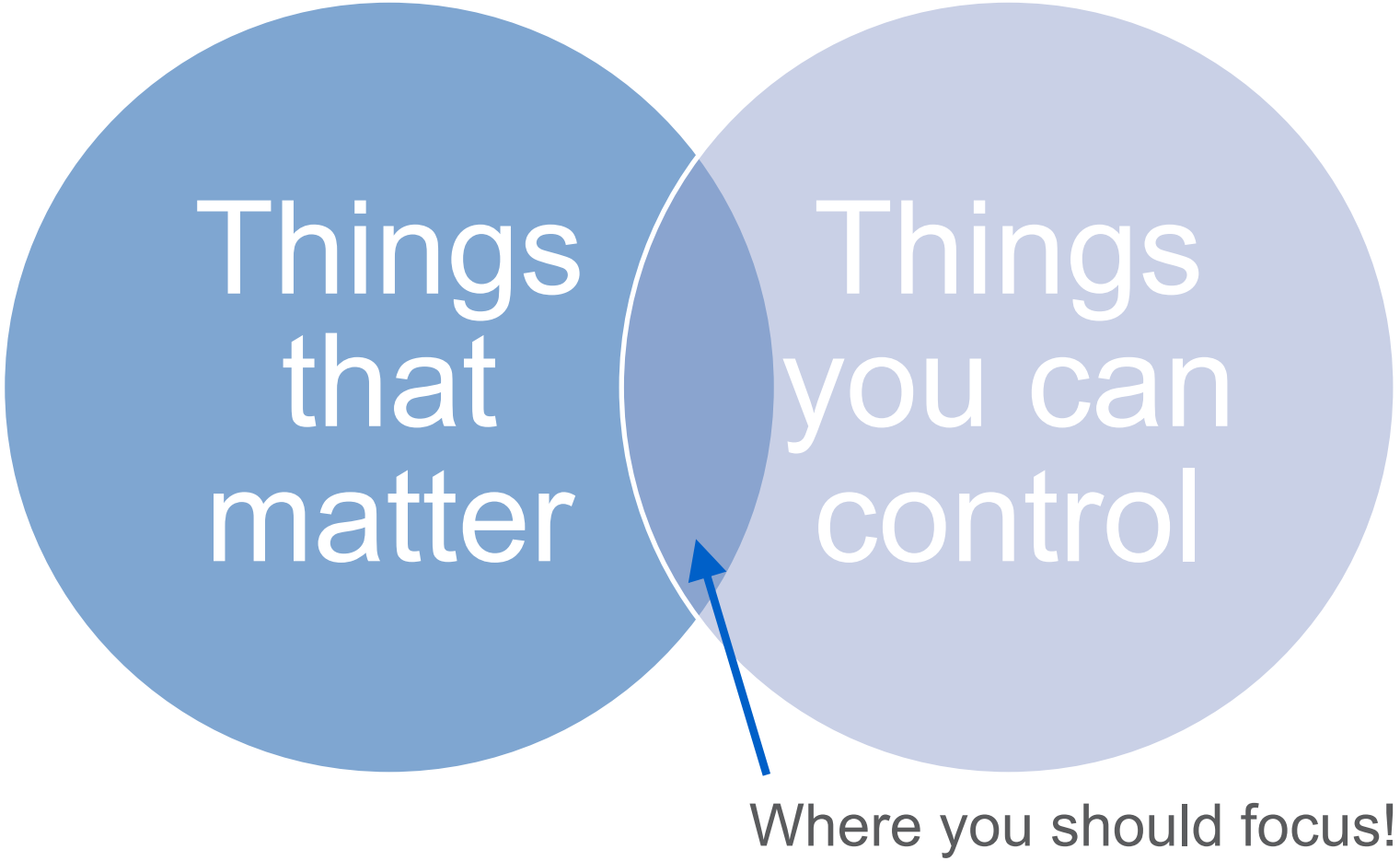
Phishing remains one of the primary attack paths used by threat actors. As part of their assessment offerings, DHS provides focused PCAs. The amount of an organization's users that click on the DHS phishing email—called user click rates—and the ratio of users that interact with a potentially malicious email can often indicate the success, or lack thereof, of an organization's user training and awareness.

Stakeholder Group	Median percentage of user click rates
Election Infrastructure entities	6.15%
SLTT Government entities	6.91%
Federal entities	6.05%
Total user click rate across all assessments	**6.71%**

CISA
CYBER+INFRASTRUCTURE

Matt Masterson
February 12, 2020

With so many factors…



CISA
CYBER+INFRASTRUCTURE

Elections Systems: Designated Critical Infrastructure

“Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.”

16 Sectors: Chemical; Commercial Facilities; Communications; Critical Manufacturing; Dams; Defense Industrial Base; Emergency Services; Energy; Financial Services; Food and Agriculture; Government Facilities; Healthcare and Public Health; Information Technology; Nuclear Reactors, Materials and Waste; Transportation Systems; and Water and Wastewater Systems.

- Authorities: Patriot Act, (Sec. 1016(e)); Department of Homeland Security, National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience; Presidential Decision Directive 63, 199; Homeland Security Act of 2002, 6 U.S.C. § 131.
  - See https://www.eac.gov/assets/1/6/starting_point_us_election_systems_as_Critical_Infrastructure.pdf

Elections Systems: Designated Critical Infrastructure

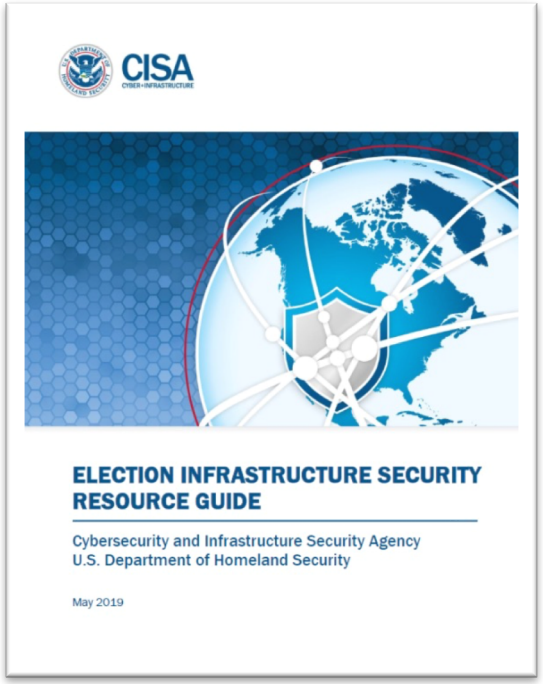
The 2017 designation of election infrastructure as critical infrastructure provides a basis for the Department of Homeland Security and other federal agencies to:

- Recognize the importance of these systems;
- Prioritize services and support to enhancing security for election infrastructure;
- Provide the elections community with the opportunity to work with each other, the Federal Government, and through the Coordinating Councils;
- Hold anyone who attacks these systems responsible for violating international norms.

Before I get too far…

My team's mission: To ensure the Election Infrastructure Community has the necessary information to adequately assess risks and protect, detect, and recover from those risks.

- CISA can provide you free services and assessments for cyber and physical security
  - **nccicustomerservice@hq.dhs.gov**
- We share tailored information through the Election Infrastructure Information Sharing and Analysis Center (EI-ISAC)
  - **https://www.cisecurity.org/ei-isac/**



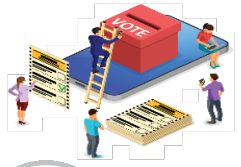
CISA's #PROTECT2020 Initiative

WHO WE SUPPORT

State and Local Election Authorities

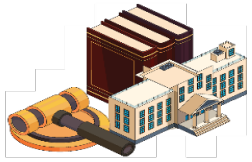
Election Technology Providers

Campaigns and Political Infrastructure



Electorate

WHO WE PARTNER WITH



Federal, State, & Local Government Agencies

Academic Institutions and Think Tanks

Non-Governmental Organizations (NGOs)

Media, Tech, & Social Media Companies

Cybersecurity/Threat Assessment Firms

#PROTECT2020

1. Support the security efforts of the election community – elections officials and technology providers.
2. Advise and support the security of campaigns and political infrastructure.
3. Raise awareness of and build resilience against the threat of foreign influence operations.
4. Improve Warning and Response.

CISA
CYBER+INFRASTRUCTURE

CISA's Support to Election Community

- Increase engagement and support provided to local election officials
- Raise awareness regarding the need for regular investment in election infrastructure
- Further develop CISA's understanding and conversations about risks to election infrastructure
- Improve communications and information sharing across the subsector
- CISA resources available to election officials and technology providers to #PROTECT2020
- Increase support to election system private sector

CISA Core Elections Services

Vulnerability Scanning

- A scanning of internet-accessible systems for known vulnerabilities on a continual basis. As potential issues are identified, CISA notifies impacted customers so they may proactively mitigate risks to their systems prior to exploitation. Conducted remotely and fully automated.

Remote Penetration Testing

- Utilizes a dedicated remote team to assess and identify vulnerabilities and work with customers to eliminate exploitable pathways. The assessment simulates the tactics and techniques of malicious adversaries and tests centralized data repositories, externally accessible assets, and web applications.

Phishing Campaign Assessment

- Measures the susceptibility of an organization's staff to social engineering attacks, specifically email phishing attacks. The assessment takes place during a six-week period. An assessment report is provided two weeks after its conclusion. The assessment report provides guidance, measures effectiveness, and justifies resources needed to defend against and increase staff training and awareness of generic phishing and spear-phishing attacks.

- **To request services email: NCCICcustomerservice@hq.dhs.gov**

Physical Support Services

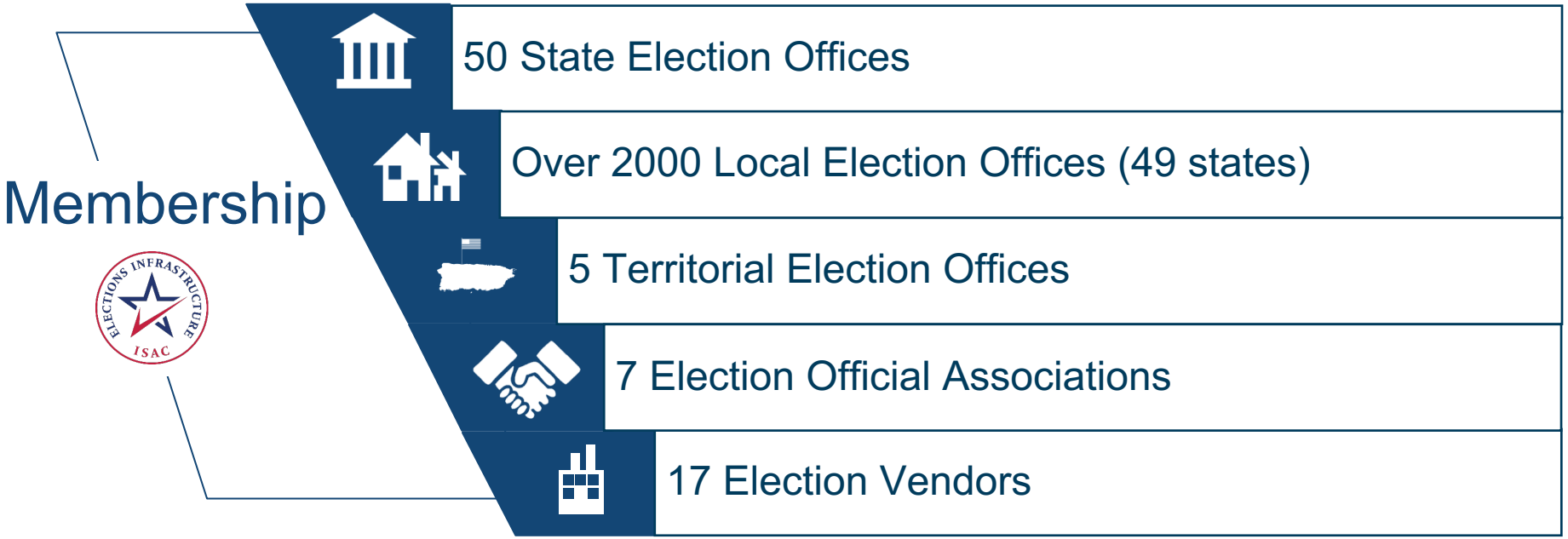
- Protective Security Advisors Serving 73 districts in 50 states and Puerto Rico
- Protective Security Advisors (PSAs) serve as the link to CISA infrastructure protection resources and the Federal Emergency Management Agency (FEMA).
  - Trained in the physical aspects of infrastructure protection, PSAs share information and conduct resilience surveys and vulnerability assessments
- PSAs assist facility owners and operators with resources, training, and access to other DHS products and services. For more information, or to reach your local PSA, contact nicc@hq.dhs.gov.

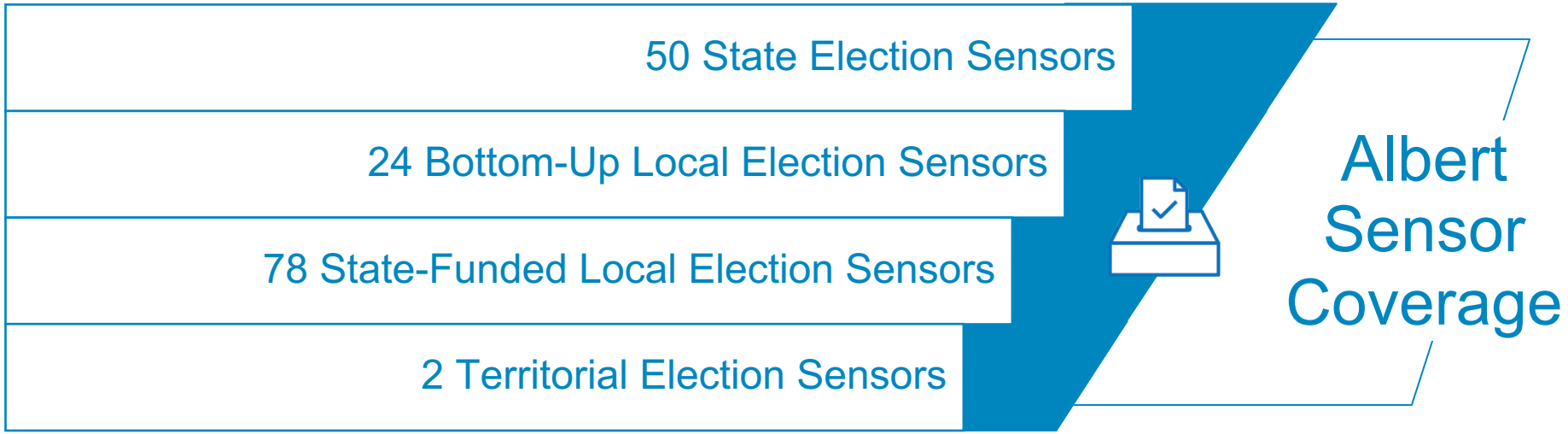
Join the EI-ISAC

- Provides cybersecurity support to SLTT governments.
- Furthers DHS efforts to secure cyberspace by distributing early warnings of cyber threats to SLTT governments.
- Shares security incident information and analysis.
- Runs a 24/7 watch and warning security operations center.
- Operates an election threat warning center, the Election Infrastructure-ISAC.
- Funded by DHS.

For more information, see https://www.cisecurity.org/ei-isac

Election Infrastructure: Information Sharing





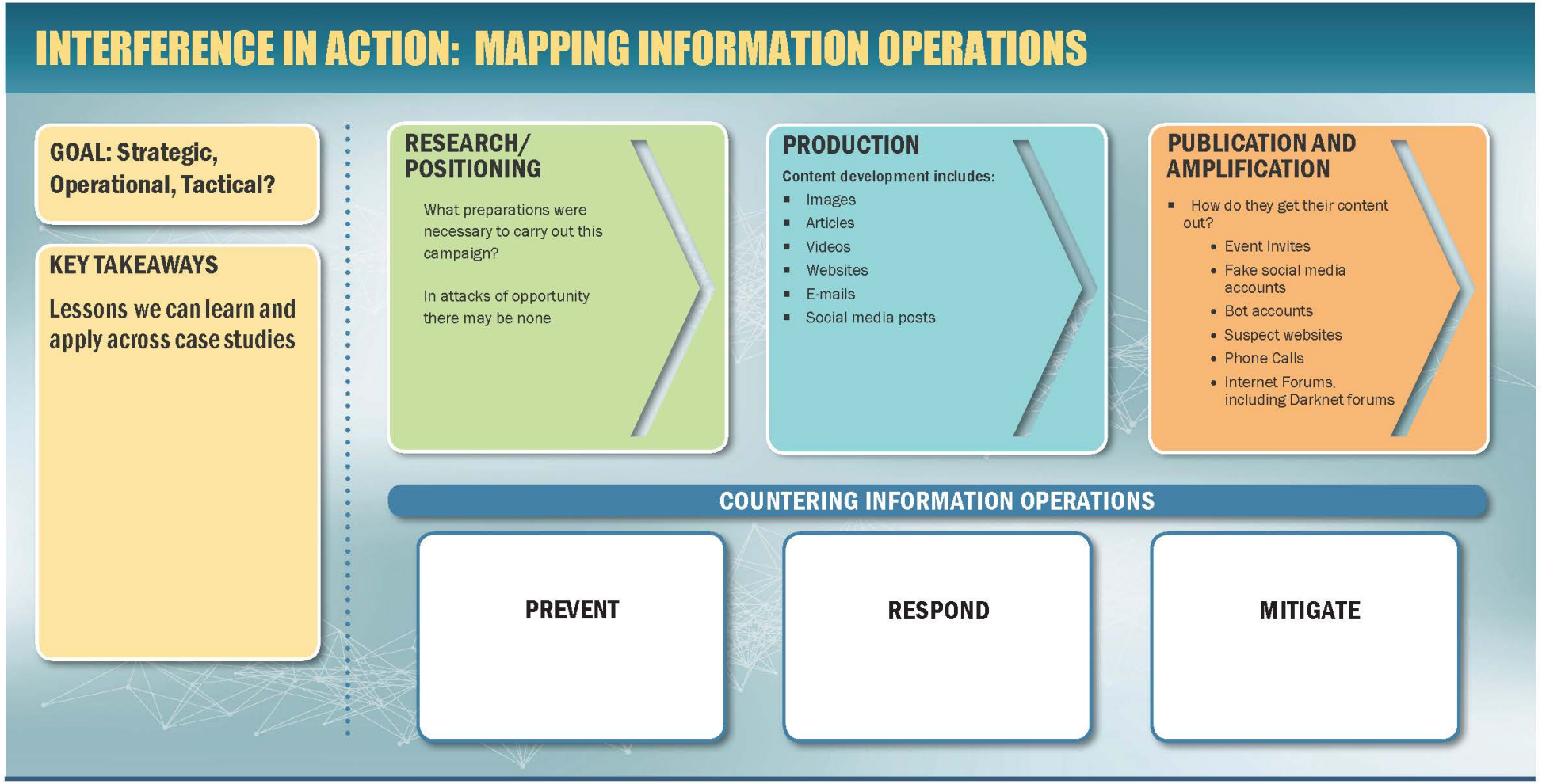
Ransomware

- Ransomware is a type of malicious software designed to deny access to a computer systems or data until a ransom is paid.
- If ransom demands are not met, the system or encrypted data remains unavailable, or data may be deleted.
- In elections this could be used to deny access or delete Voter Registration and/or Vote Tabulation data.

Prepare for Ransomware

- **Utilize CISA Services (NCCICcustomerservice@hq.dhs.gov)**
  - Remote Penetration Testing (RPT)
  - Vulnerability Scanning
- **Develop an Incident Response Plan**
- **Create Backups**
  - Backup your data regularly
  - Have access to your software and source code in case you need to rebuild the system
- **Test your plans and backups**

Breaking Down Information Operations



CISA
CYBER+INFRASTRUCTURE

Case Study: Louisiana Chemical Attack -- Russia

Goal: Undetermined. Breadth of techniques used on a limited scale could indicate testing in U.S.

Research/Logistics

- Access to cell phone numbers in local area
- Established social media accounts and bots
- Developed targeted media and key influencers list

Production

Content developed includes:

- Fake surveillance camera footage
- Doctored images of flames engulfing plant
- Fake YouTube video showing ISIS claiming responsibility
- Wikipedia page content
- Doctored CNN webpage showing disaster had made national news
- Text messages and social media messaging

Publication and Amplification

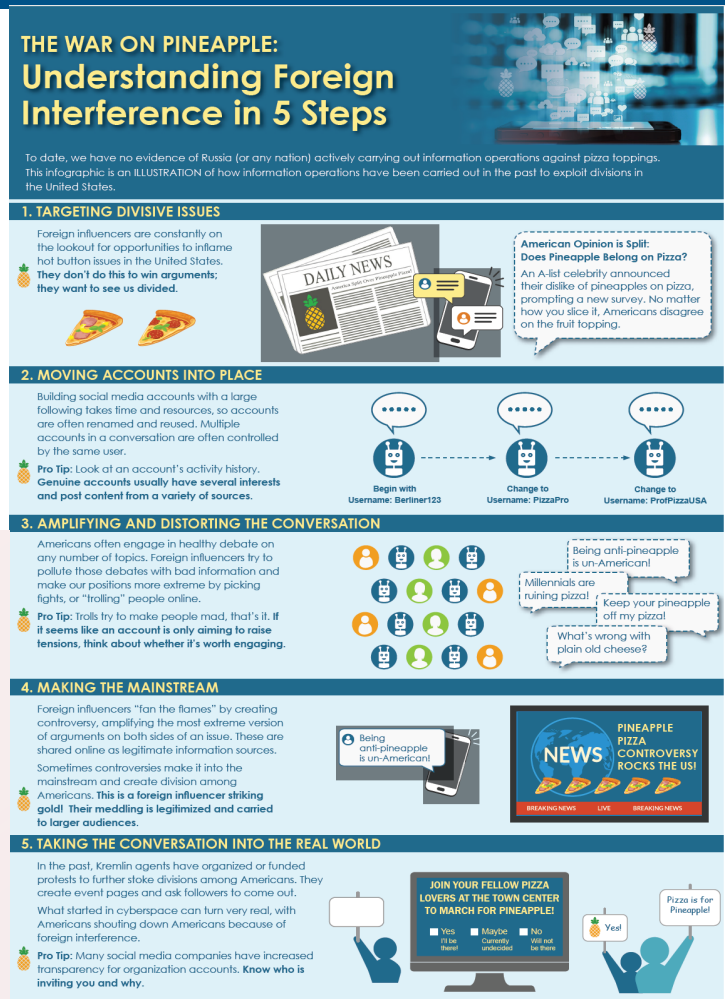
- Text messages to local residents
- Hundreds of Twitter accounts posting about "disaster" using hashtag #ColumbianChemicals and doctored images/videos
- Tweets targeting reporters at local and national media – New Orleans Times-Picayune, CNN, and NYT
- Tweets targeting political commentators

CISA
CYBER+INFRASTRUCTURE

Source: "The Agency," Adrian Chen, New York Times Magazine

Building Public Awareness

- **War on Pineapple**
  - Bring a non-divisive issue to the forefront to show how it could be used to sow discord
  - Raise awareness
  - Educate public on how they can mitigate the risk



Top Recommendations Provided Across All EI Assessments

1. Defend
   - Ensure all aspects of voting system are air gapped
   - **Update all software patches**
   - **Review and update system configurations & access controls**
   - Manage passwords & Implement multi-factor authentication
2. Detect
   - Join EI-ISAC: https://learn.cisecurity.org/ei-isac-registration
   - Have awareness and monitoring of your systems
   - **Protect and detect malware - viruses, spyware, ransomware**
   - Educate employees and pollworkers
3. Recover
   - Take regular backups & test them
   - Provisional ballot/backup ballot preparation
   - Auditable ballots & conduct audits
   - **PLAN, PLAN, PLAN, PLAN**
4. TAKE ADVANTAGE OF ALL AVAILABLE RESOURCE

CISA
CYBER+INFRASTRUCTURE

CISA Election Security 101

Matthew Masterson
Senior Cybersecurity Advisor
CISA
Matthew.Masterson@cisa.dhs.gov