The U.S. Election Assistance Commission

Matthew V. Masterson
Chairman
NASED
Election 2016: Where, when and how to vote on Nov. 8

Voters stand near a voting sign before casting ballots during early voting at the Franklin County Board of Elections in Columbus, Ohio, October 28, 2016. / REUTERS/SHANNON STAPLETON

34 Comments / Share / Tweet / Stumble / Email
Russian agents hacked US voting system manufacturer before US election - report

- Federal contractor arrested and charged with removing classified material
- NSA report: cyber-attack on software supplier and phishing emails hit officials

Russian intelligence agents hacked a US voting systems manufacturer in the weeks leading up to last year's presidential election, according to the Intercept.
Russia hacked voting systems in 39 states before the 2016 presidential election

This goes way deeper than we first thought.

Updated by Alex Ward | @AlexWardVox | alex.ward@vox.com | Jun 19, 2017, 2:00pm EDT
Researchers find link between North Korean hackers and Wanna Cry

BY JOE UCHILL - 05/17/17 06:27 PM EDT

154 SHARES

SHARE (154)

TWEET

PLUS ONE

www.eac.gov

havainfo@eac.gov

MEDICARE ADVANTAGE
LEADING THE WAY

LEARN MORE
Websites of Ohio's Kasich, others hacked with ISIS message

By Dakin Andone, CNN

Updated 8:07 AM ET, Mon June 26, 2017
MASTERING DATA

How Hackers Broke Into U.S. Voting Machines in Less Than 2 Hours

Barb Darrow
Jul 31, 2017
Swing State Counties with Election Official Cybersecurity Training

- **Yes**
- **No**
- **Somewhat**
- **No reply in NBC inquiry**

40 counties

Pennsylvania

Michigan

Arizona

Data: NBC News analysis

NBC NEWS

www.eac.gov

havainfo@eac.gov
FARMER SHOOTS
23-LB. GRASSHOPPER!
Fed-up fatties kill aerobics instructor!
Thousands of gals want to marry Mr. Fuzzy-wuzzy!
Things that matter

Things you can control

What you should focus on
Core Competencies

• In 2016, what are the Core Competencies of an Election Administrator?
  • Lawyer – must know election law and how it is implemented within the jurisdiction
  • HR Specialist – must know how to recruit, train, compensate and evaluate election workers
  • Communication Officer – must know how to compose precise and persuasive communications across a spectrum of platforms
  • Accountant – must know how to create operating budgets and make less, go further
Core Competencies

- **Auditor** – must be able to create and implement audit programs to identify and correct errors to improve efficiency and effectiveness of operations

- **Trainer** – must be able to develop and implement training programs for poll workers and voters

- **Information Technology Manager** – managing large numbers of complex information systems, data, vendors and technical staff
Core Competencies

• The typical county election official may be managing more technology than the county’s IT department:
  • DREs
  • Scanners
  • EPBs
  • Servers
  • Desktops
  • Laptops
  • Tablets
  • Printers
  • Vendors
  • Phone systems
  • Copiers
  • Fax machines
  • Smart phones
  • GIS interfaces
  • VR system clients
  • Voter services
  • Software versions
  • Contracts

• What part of an election officials job does not involve IT?
IT Management

- Election Officials must view themselves as complex IT system managers (because their bosses – the voters - do)
  - How does each decision impact the process and protection of data?
  - Every aspect of election administration should be viewed through the lens of the integrity of the process(es).
  - EOs must understand the systems in the office in order to make best decisions
  - *What is the relationship between the IT and Organizational strategic goals?*
Cybersecurity Risks

- Denial of Service (DDOS)
- Ransomware
- Petya/NotPetya - Wiper
- Stolen Personally Identifiable Information (PII)
- Stolen credentials and login information
- Phishing and Spearphishing

- Disruption
- Doxxing – Publishing damaging information
- Database Targeting/Injection
Defense in Depth

DATA

Application Security
Host Security
Network Security
Physical Security
Security Resources Available

• **Security Checklists**
  • Securing Voter Registration Data
  • Securing Election Night Reporting Systems
  • Incident Response Planning

• **Guidance Documents**
  • Security Planning
  • Contingency Planning
  • Managing aging voting systems
  • Ransomware response
  • DHS Online training

• **Machine Testing and Auditing Information**
  • Clearinghouse of state practices and information
  • Best practice documents
Database Security

• **Access Control** - only authorized personnel should have access to the voter registration database. Each person with authorization to the database should only have access to the data and information necessary for them to perform their job duties.

• **Auditability** - the database should have sufficient logging capabilities, including who has made modifications, the nature of the modifications, the authority to make those modifications, and to determine if there has been any unauthorized or inappropriate activity.

• **Detection** – use an intrusion detection system and monitor the incoming and outgoing traffic for signs of irregularities, such as multiple log-in attempts, above average traffic, large amounts of data being transmitted, etc. If detected have a response and mitigation plan in place.
Database Security

• **Data Backups** – the database should be backed up routinely. If any unexpected modifications to the data were to occur, the database could be restored to the last known state prior to the unexpected modifications. The ability to perform backups and restores should be tested and validated.

• **Data Suppression** – any data provided to outside sources is suppressed to only contain the data necessary for that entity to perform its legally authorized functions.
  - if an entity wants to obtain a copy of the data files to determine where specific voters live for GOTV campaigns, it does not need data field containing ID numbers and therefore, the additional information should not be provided.

• **Remote Access Control** – only allow remote access through secure networks, such as Virtual Private Networks (VPN).
Database Security

- **Encryption** – encryption should be used throughout, including but not limited to encrypting the database, server, backups, any files used for distribution, all data transmission and communication.

- **Firewalls** – implementation of the proper use of network firewalls for the environment in use. Unauthorized access (or attempts to access) to the data should be detected, prevented, reported and escalated.

- **System Interconnection** - do not connect the voter registration database to any other information system that is not required for its use. When the voter registration system is required to be interconnected with another information system make sure the necessary security controls are in place for each system individually, as well as the communication channel between the systems.
Incident Response

- **Create an incident response policy and plan** - Election officials should be prepared to respond quickly and effectively to a cyber incident. The first step of developing a policy or plan is to identify which events are considered incidents and provide an organizational structure, including roles and responsibilities, for responding to these events. This may also include incidents that occur on systems the organizations uses but are outside of their physical control, such as service-oriented systems provided by vendors.

- **Develop procedures for performing incident handling and reporting** - The incident handling and reporting procedures provide a detailed process for carrying out the incident response policy and plan. (See “Incident Handling Checklist” from the NIST SP 800-61).
Incident Response

• **Set guidelines for communicating with outside parties** - Election officials should create a communications plan that describes which incidents need to be reported to which outside parties such as the media, law enforcement agencies, and incident reporting organizations. The guidelines should also address the timeframe for this report, as well as identify the members of the incident response team that are integral in implementing the plan, such as public affairs office, legal department, and management.

• **Select a team structure and staffing model** – There are many resources for developing a team structure and staffing model, but the first consideration an organization should make is whether it will create an internal incident response team or outsource it. Organizations should take into account that an incident can occur at any time, response can require specific expertise across a multitude of technical and non-technical sectors of the organization, and these incidents can often be both stressful and costly.
Incident Response

• **Establish relationships and lines of communication** - between the incident response team and other groups, both internal (e.g., legal department) and external (e.g., law enforcement agencies). Every incident will require collaboration and cooperation of multiple team members and groups. The relationships and credibility of each team member and group is vital to a successful recovery from an incident.

• **Determine what services the team should provide** – Having well defined roles for which members and teams will provide what services will facilitate a smoother implementation.

• **Staff and train the incident response team** - Training staff and the incident response team ensures that the incident response procedures are accurately carried out. Additionally, the training should provide specific details on the transition from incident response to recovery.
5 things you can do right now

1. Ensure that **all** aspects of voting system (VS, EMS, Ballot Creation) are not connected to internet... clean media & air gaps

2. Audit your systems, data, processes & procedures
   - Pre-election testing, post-election auditing, chain-of-custody, access controls, physical security
   - Do what election officials do...

3. Secure your data

4. Develop an incident response & recovery plan

5. Take advantage of all available resources
Stay in Touch – Social Media

@EACgov  @mastersonmv
Facebook.com/eacgov1  BeReady@eac.gov  listen@eac.gov
YouTube Channel: Election Assistance Commission

www.eac.gov
Contact Us:

Matthew Masterson
Chairman
Email: mmasterson@eac.gov
Phone: (202)378-0561

U.S. Election Assistance Commission
Phone: 1-866-747-1471
Email: havainfo@eac.gov