5 Cybersecurity Steps that Make a Big Impact

Steve Simon

Minnesota Secretary of State

Bill Ekblad

Election Security Cyber Navigator,
Office of the Minnesota Secretary of State

1. Coordinate with your state partners and utilize state resources outside of your office
2. Utilize the many federal resources available to your office
3. Look to leverage private resources through a Vulnerability Disclosure Program
4. Don’t forget the basics – multifactor authentication, network segmentation, etc.
5. Coordinate and support local partners – Minnesota’s Cyber Navigator Program

Coordinate with State Partners

State IT, Fusion Centers, etc.

- **State IT Services**
- **State Fusion Center**
- **State National Guard**
- **State Emergency Management**

Utilize Federal Resources

Risk and Vulnerability Assessments, ongoing scanning and support, etc.

- **Risk and Vulnerability Assessment (RVA)**
- **Cyber Resilience Review**
- **Phishing Campaign Assessment**
- **Weekly Cyber Hygiene Scan**
- **Malicious Domain Blocking and Reporting**
- **Web Application Scanning**
- **Federal Virtual Training Environment (FedVTE)**
- **Tabletop Exercise Package**
- **Community Webinars**
- **Information Sharing: MS/EI-ISAC and Homeland Security Information Network (HSIN) - CISA Cyber Portal**

Look to leverage other resources

Consider a Vulnerability Disclosure Program

Vulnerability Disclosure Programs (VDPs) are a formalized method for external individuals to report vulnerabilities in systems.

Minnesota looking to create a VDP prior to the 2022 election.

Don’t Forget the Basics

MFA, Network Segmentation, etc.

Multifactor Authentication – Deployed on systems such as email, VPN access, and key systems accessed by outside users.

Network Segmentation – Key to minimizing the exposure risk in case of a breach or unauthorized access.

Coordinate with Local Partners

Minnesota Cyber Navigator Program

- **87 Counties**
  - Traverse County ~ 3,200
  - Hennepin County ~ 1,280,000

Cyber Navigator
Program Overview

- Background / Purpose
- Program Launch and Initial Efforts
- 2020 Election Year
- Lessons Learned (so far!)

Cyber Navigator
Background and Purpose

- Driver: 2016 Presidential Election cyber activity
- Key Enabler: HAVA resources
- Our Focus: Raise awareness
  - Cyber threats to elections-related systems
  - Resources available to reduce risk

Cyber Navigator
Program Launch and Initial Efforts

- Build the Network
  - Elections Leaders
  - IT Leaders
  - State agency and Federal partners
- Build the Relationships
  - Communicate regularly (up, down, sideways)
  - En masse, but also individually
- Provide Value

Cyber Navigator
2020 Election Year*

- Leveraged Relationships
- Real-time election event collaboration
  - System outage provided a useful test!
- Prepared for more cyber activity (but grateful for less)

*(*Covid-19 and Physical Security aspects overshadowed cyber threats)*

Cyber Navigator
Lessons Learned (so far!)

- Cyber Security is a team sport!
- Personal relationships matter
- Focus on the low-hanging fruit (there’s lots of it!)
- Help and resources are already there, but the right connections may not be…
- Stay flexible; each jurisdiction is unique!
- Any progress is valuable