Office of the Minnesota
Secretary of State

MNOSS Partnerships

Cybersecurity Objectives

Challenges & Initiatives

Cyber Navigator Program

Legislative Commission on Cybersecurity
January 10, 2022

Office of the Secretary of State
Overview

- **Office Composition**
  - Administration
  - Business Services
    - Notary Registry
    - Business Registrations
  - Elections
  - Safe at Home Program
  - IT Team
    - Not part of the MN.IT consolidation
    - Three software development teams to support each business unit
    - In-House software application development

Office of the Minnesota
Secretary of State

Federal Partnerships

- FBI
- Department of Homeland Security (DHS) - Office of Intelligence and Analysis (I&A)
- Cybersecurity & Infrastructure Security Agency (CISA)
  - Catalog of Services
    - Available at no cost to critical infrastructure
    - Risk and Vulnerability Assessment
    - Remote Penetration Test
    - Vulnerability Scanning
    - Web Application Scanning
    - Validated Architecture Design and Review

State Partnerships

- **MN.IT**
  - Security Operations Center (SOC) daily briefs
  - Leverage additional MN.IT offerings where beneficial and cost effective
    - Office365 security features
    - Data Center
    - Forensics
    - Data flow analysis
    - Offsite log retention
    - Vulnerability scanning
    - Domain registration monitoring
    - Phishing Tool
- **MN Fusion Center**
  - Intelligence and situational awareness

Office of the Minnesota
Secretary of State

Non-Governmental Organization Partnerships

- **National Association of Secretaries of State (NASS)**
  - Tech Talks
  - Collaboration with other Secretary States IT offices across the country for best practices and solutions
- **Multi State/ Elections Infrastructure – Information Sharing and Analysis Center (MS/EI-ISAC)**
  - Managed by Center for Internet Security and Funded in part by DHS
  - Available member services
    - Malicious Code Analysis Platform (MCAP)
    - Vulnerability Management Program (VMP)
    - CIS SecureSuite Membership
    - Nationwide Cybersecurity Review (NCSR)
    - Malicious Domain Blocking and Reporting (MDBR)
    - Albert Sensors
    - 24x7 SOC

Office of the Minnesota
Secretary of State

Office Cybersecurity Objectives

following the National Institute of Standards and Technology (NIST) Cybersecurity Framework

Credit: N. Hanacek/NIST

Office of the Minnesota
Secretary of State

Identify

Develop organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.

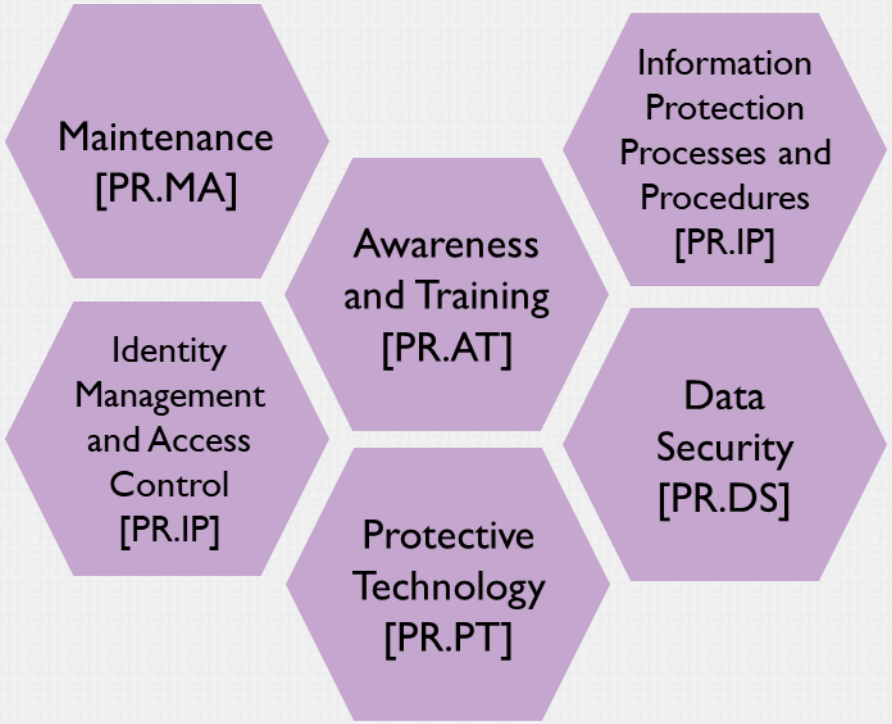
- Business Environment [ID.BE]
- Asset Management [ID.AM]
- Governance [ID.GV]
- Risk Assessment [ID.RA]

- Identify critical business processes
- Participate in yearly Nationwide Cybersecurity Review (NCSR)
- Establish policies for cybersecurity that includes roles and responsibilities
- Maintain hardware and software inventory

Office of the Minnesota
Secretary of State

Protect

Develop and implement the appropriate safeguards to ensure availability of services.



- Conduct regular backups and validate backups
- Protect sensitive data
  - Network segmentation
  - Identity management
  - Multifactor authentication
- Patch operating systems and applications using more aggressive schedule as laid out in CISA 's Known Exploited Vulnerability Catalog
- Create response and recovery plans
- Vulnerability scans
- Ongoing phishing training and testing for Staff
- Yearly penetration testing

Office of the Minnesota
Secretary of State

Detect

Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.

Anomalies and Events [DE.AE]

Continuous Monitoring [DE.CM]

- Implemented endpoint detection and response (EDR) Solution
- Monitor data flows for abnormalities
- Maintain and monitor logs

Office of the Minnesota Secretary of State

Respond

Develop and implement the appropriate activities to act regarding a detected cybersecurity event.

Response Planning [RS.RP]

Communications [RS.CO]

- Coordinate with internal and external partners
- Tabletop Exercises
- Ensure response plans are updated

Office of the Minnesota Secretary of State

Recover

Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

Recovery Planning [RC.RP]

Communications [RC.CO]

- Manage public relations and company reputation
- Communicate with internal and external stakeholders
- Disaster Recovery Testing

Office of the Minnesota Secretary of State

Challenges and Initiatives

- Expanded collaboration with federal and state partners to combat foreign actors
- Application Modernization
- Vulnerability Disclosure Program
- IT Talent Recruitment and Retention to maintain in-house applications
- Increased automation in detection and response
- High-profile physical events create opportunities for cyber events
- Continuous Cybersecurity process improvements based on NIST Cybersecurity Framework
- Expanded Cyber Navigator program for county coordination and information sharing

Office of the Minnesota
Secretary of State

Election Security Cyber Navigator Program

- **Established late-2019 in advance of 2020 election year**
- **Initial focus: build statewide network of Elections *and* IT leaders in all 87 counties**
  - Cyber threat and vulnerability information sharing
  - Awareness of available state, federal, non-profit and academic election cybersecurity resources
  - Collaboration; shared situational awareness and best-practices
- **2020 Election Year Cybersecurity Assessment**
  - Third-party vendor partnership resourced by OSS
- **2022 HAVA Grants Program to Counties**
  - Comprehensive cybersecurity prerequisites
- **Expanding program capacity in 2022**
  - Additional team member; enhanced partner collaboration

Office of the Minnesota
Secretary of State

References

- NIST CyberSecurityFramework
  - https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf (Version 1.1)
- CISA Service Catalog
  - https://www.cisa.gov/sites/default/files/publications/FINAL_PDFEPUB_CISA%20Services%20Catalog%202.0.pdf
- MS-ISAC Service Catalog
  - https://www.cisecurity.org/ms-isac/services
- EI-ISAC Service Catalog
  - https://www.cisecurity.org/ei-isac/ei-isac-services/
- CISA Directive on Reducing the Significant Risk of Known Exploited Vulnerabilities
  - https://www.cisa.gov/known-exploited-vulnerabilities-catalog
  - https://www.cisa.gov/news/2021/11/03/cisa-releases-directive-reducing-significant-risk-known-exploited-vulnerabilities
- CISA Binding Operational Directive 20-01 - Develop and Publish a Vulnerability Disclosure Policy
  - https://www.cisa.gov/binding-operational-directive-20-01
- CISA Zero Trust Maturity Model
  - https://www.cisa.gov/sites/default/files/publications/CISA%20Zero%20Trust%20Maturity%20Model_Draft.pdf

Office of the Minnesota
Secretary of State

Questions

Office of the Minnesota
Secretary of State