Cybersecurity

John Quinn, Secretary and State CIO

January 6, 2022

Cybersecurity Preparedness

User awareness training

- Helps prevent and mitigate user-based risks
- Educates users on topics like privacy, phishing, and equipment security
- Short, meaningful lessons spread out over the entire year
- Increases retention and engagement both proven to reduce risk

Incident response exercises

- Familiarize cyber response personnel with process
- Exercises checklists and procedures to refine response actions
- Integrates employees from affected Agencies forming partnerships with cyber personnel
- Increased complexity improves response capability and communication

Cybersecurity Landscape

Over 7 million attempted intrusions on State networks in 2021

- Almost 700 incidents
- No incidents significantly impacted enterprise operations
- New endpoint security reduces detection and response times
- Security Operations Center puts more personnel on detection and remediation
- Ransomware will continue to be a driving concern moving through 2022
- Supply chain compromise is an expanding threat
 - Recent issues at large companies:
 - SolarWinds, Microsoft, Target, Maersk, FedEx

Projects to Continue Cybersecurity Improvement

In-progress

- Unified multi-factor authentication (MFA)
- Data center security architecture upgrades
- System-wide vulnerability scanning and reporting
- Risk assessment governance and reporting

Anticipated

- Increased segmentation, detection, and prevention of network threats
- Increased visibility of systems logs and data movement within State systems