Zero Trust in Practice

December 1, 2022
Introduction

Shane Dwyer  
State Chief Information Security Officer  
Iowa

Adam Ford  
State Chief Information Security Officer  
Illinois

Mitch Spaulding  
Senior Solutions Engineer  
Okta
What is Zero Trust?
State of Iowa Chief Information Security Officer (CISO)

- Principal executive reporting into Iowa’s Executive Branch
- Support government operations against foreign and domestic cyber threats
- Promote and foster a cyber culture across Iowa
- Commoditize cyber operations and improve cyber resiliency

- Iowa Code 8B allows the OCIO to serve
  - Executive, Judicial, and Legislative branches
  - Iowa Counties and Cities
  - Iowa Educational Institutions
  - Iowa not-for-profits
Expected Outcomes, Key Points

Shape to your Business
- Sharing the State of Iowa’s practices, one size doesn’t fit all
- Identify opportunities for other states to improve cyber postures
- Shares our approach in addressing/reducing risk of cyber incidents

Defensibility, Liability, and Risk
- Our teams should
  - Pay attention to the environment
  - Have situational awareness
  - Have documented processes and architectures
How Does the State of Iowa Define Cyber?

- **Infrastructure (on-premise and cloud)**
  - Back-up and disaster recovery
  - Network and firewall
  - Platform
    - End-user devices
    - Midrange and distributed
    - Identity and access management

- **Information Security**
  - Governance and security awareness
  - Security operations and risk management
  - Audit and compliance
State of Iowa’s Cyber Incident Response Team

CIRT serves the State of Iowa in responding to Cybersecurity threats to State, Local, Tribal, and Territorial (SLTT) governments.

The CIRT consists of the following organizations

- Department of Management, Office of the Chief Information Officer
- Iowa Department of Public Safety, Division of Criminal Investigation
- Iowa Homeland Security and Emergency Management
- Iowa National Guard, 168th Cyber Operations Squadron
- Iowa Secretary of State
- Iowa State University Board of Regents
The CIRT collaborates with the following organizations:

- Cybersecurity and Infrastructure Security Agency (CISA)
- Iowa Fusion Center
- Federal Bureau of Investigation
- Multi State Information Sharing and Analysis Center (MS-ISAC)
- U.S. Department of Homeland Security
Definitions

• **System Interconnections**
  - Connection between two or more systems

• **Ecosystem (Security Authorization Boundary)**
  - If data is being queried (answer/response)
  - If data is being sent to another information system
  - If data is being reciprocally sent and received (or shared)
# Iowa’s Preliminary Zero Trust Roadmap

<table>
<thead>
<tr>
<th>#</th>
<th>Activity</th>
<th>Government Scope</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Manual inventory information systems and Ecosystems</td>
<td>State</td>
</tr>
<tr>
<td>1.1</td>
<td>Deploy Endpoint Protection and Response (EDR) tool (Prevention Mode)</td>
<td>State</td>
</tr>
<tr>
<td>1.1.1</td>
<td>Enhancement: EDR real-time scanless vulnerability assessment</td>
<td>State</td>
</tr>
<tr>
<td>1.1.2</td>
<td>Enhancement: EDR automated inventory of information systems and software</td>
<td>State</td>
</tr>
<tr>
<td>2</td>
<td>Manual inventory of individual assigned accounts and resource accounts</td>
<td>State</td>
</tr>
<tr>
<td>2.1</td>
<td>Integrate into “Identity as a Service” and apply multifactor authentication</td>
<td>State</td>
</tr>
<tr>
<td>2.1.1</td>
<td>Enhancement: Evaluate accounts based on Authenticator Assurance Levels (AAL)</td>
<td>State</td>
</tr>
<tr>
<td>2.1.2</td>
<td>Enhancement: Evaluate accounts based on Identity Assurance Levels (IAL)</td>
<td>State</td>
</tr>
</tbody>
</table>
# Iowa’s Preliminary Zero Trust Roadmap

<table>
<thead>
<tr>
<th>#</th>
<th>Activity</th>
<th>Government Scope</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>Manual inventory of interconnections (website, API, SaaS, PPS, etc.)</td>
<td>State</td>
</tr>
<tr>
<td>3.1</td>
<td>Integrate interconnections into security boundaries and Identity as a Services</td>
<td>State</td>
</tr>
<tr>
<td>3.1.1</td>
<td>Enhancement: Integrate AAL and IAL into system interconnections</td>
<td>State</td>
</tr>
<tr>
<td>4</td>
<td>Security Analytics Platform</td>
<td>State</td>
</tr>
<tr>
<td>4.1</td>
<td>Integrate interconnection logs into security analytics data lake</td>
<td>State</td>
</tr>
<tr>
<td>4.2</td>
<td>Integrate into Security Orchestration, Automation, and Response (SOAR)</td>
<td>State</td>
</tr>
</tbody>
</table>
Authentication Assurance Level (AAL)

**AAL 1**
- **Limited Impact**
- **Low Risk**
  - Unprotected data
  - Open data
- **Identity Validation**
  - Identity Assurance 1
    - No requirement to validate to a real-life identity
- **Authentication**
  - Single Factor
    - Memorized Secret
    - One Time Password

**AAL 2**
- **Serious Impact**
- **Moderate Risk**
  - PII/PHI data
  - Protected data
- **Identity Validation**
  - Identity Assurance 2
    - Remote of physical validation with real-life identity
- **Authentication**
  - 2 Factors
    - Memorized Secret
    - OTP Device
    - Crypto Software
    - Crypto device

**AAL 3**
- **Catastrophic Impact**
- **High Risk**
  - PII/PHI data
  - Protected data
- **Identity Validation**
  - Identity Assurance 3
    - Physical validation with real-life identity by authorized and trained personnel
- **Authentication**
  - Templated Factors
    - Memorized Secret
    - OTP Device
    - Crypto Software
    - Crypto device
Introduction: State of Illinois CISO

Statewide Chief Information Security Officer (CISO)

• Established in Statute in 2018
• Report directly to State CIO (cabinet-level official)
• Strategic planning, facilitation, and coordination office for information technology security in IL
• Lead and central coordinating entity to guide and oversee the information security functions of State agencies
• Oversight for elections cybersecurity outreach program
• Operation of cyber liaison program for local government in Illinois
Legacy Resident Digital Interaction

• Legacy applications were purpose-built for specific programs
  • Unemployment Insurance
  • Food security
  • Energy assistance
  • Hunting permits

• Interoperability between programs not a design requirement
• Outward-facing approach – Resident interaction is designed around the program instead of program being designed around resident interaction
• Account service frequently requires call to agents/help desk
Legacy Resident Challenges

• Residents often have multiple user accounts for State systems
  • Duplicate accounts within a program not uncommon
  • Each program a resident engages with has a unique login

• User identity verification is often unsophisticated
  • Utilizes information about resident such as SSN, DLN, etc
  • Lacks modern approach to risk evaluation

• Implementing modern security features is difficult and piecemeal
  • Multiple complex passwords, multiple MFA implementations

• Frequent calls to help desk for password reset
  • Resident frustration
  • Difficult for help desk agent to identify correct account
ILogin – Resident Single Sign-On

• Single user access method available across multiple resident services
• Built on commercially available Software as a Service (SaaS) platform
• Identity Security is built-in
  • Multi-factor authentication methods enrolled during account creation
  • Identity verification using commercial methods required prior to establishing access to systems containing sensitive information
• User Self-Service methods are configured during account creation
• User interaction with State digital services feels familiar to banking, ecommerce and digital entertainment
Identity Verification

• Identity Assurance Level (IAL)
  • IAL Level 1 – correlation to a real identity is not required
    • Public information only
    • Self-verification provided by the user
  • IAL Level 2 - requires correlation to a real identity is required
    • Sensitive Information (PII, PHI, account information)
    • Digital support for identity is acceptable (Identity-proofing technologies)
    • In-person verification is acceptable (Presentation of documents such as driver's license)
  • IAL Level 3
    • In person validation required
    • Generally unapplicable to public State services
    • Employee is an example

• Represents a culture shift for agency interaction with the public
  • Resistance to friction for digital transactions is common

• Risks from identity breach can seem very unlikely to agency program staff
ILogin is the new State of Illinois sign-in site that allows you to securely access state services using a single ILogin account. This means you can sign in once on the ILogin page to access the state programs you use.

Get Started
User Enrollment

Create Account

- Email *
- Password *
- First name *
- Last name *
- Middle name
- Suffix

* indicates required field

Register

Back to sign in
Account Self-Service

Reset Password

Enter your ILogin Email address

SMS or Voice Call can only be used if a mobile phone number has been configured.

- Reset via SMS
- Reset via Voice Call
- Reset via Email

Back to sign in

Unlock account

Enter your ILogin Email address

SMS or Voice Call can only be used if a mobile phone number has been configured.

- Send SMS
- Voice Call
- Send Email

Back to sign in
Fireside Chat Questions
Audience Q&A
Thank You

For questions, additional resources, or to be put in contact with any of our speakers, please contact:

**Casey Dolen**
Senior Policy Analyst, Cybersecurity
National Governors Association

cdolen@nga.org

Please visit [https://www.nga.org/statecyber/](https://www.nga.org/statecyber/) for more updates from NGA’s cybersecurity division