Division of Technology Services

State of Utah

Division of Technology Services

Cybersecurity

Utah's Whole-of-State Cybersecurity Model: A unified front against threats

March 2025

Alan Fuller - alanfuller@utah.gov
Stephanie Weteling - stephanie@utah.gov

Executive Summary

The Whole-of-State Defense Strategy

Over the past decade, the Utah Division of Technology Services (DTS) Enterprise Security has witnessed the escalating frequency and sophistication of cyber attacks against local jurisdictions. Recognizing that a vulnerability in a local municipality is a systemic risk to the entire state, DTS launched a strategic initiative to bolster cybersecurity resilience across all levels of government. This Whole-of-State model officially commenced with the formation of the **Local Government Cybersecurity Outreach Team** and the legislative establishment of the **Utah Cyber Center**.

Strategic Objectives

The program is built on a proactive security culture designed to bridge the gap for jurisdictions with limited resources. By fostering collaboration, the initiative focuses on:

- **Information Sharing:** Cultivating a statewide network for real-time threat intelligence.
- **Resource Provisioning:** Delivering enterprise-grade security products and implementation support.
- **Maturity Elevation:** Increasing the cybersecurity posture of all State, Local, Tribal, and Territorial (SLTT) entities through risk-based projects.

Vision and Mission

- **Vision:** To foster a culture of proactive collaboration and trust through strategic partnerships. By sharing resources and intelligence, we aim to build a resilient foundation that elevates cybersecurity maturity across every level of government in Utah.
- **Mission:** Improve access to and awareness of cybersecurity resources, develop a facilitated whole-of-state model, and raise the security posture of all SLTTs through risk-based projects, information sharing, and education.

The Idea – Addressing the Resource Gap

The Problem: A Perfect Environment for Exploitation

Local governments are primary targets for sophisticated threat actors, ranging from nation-states and hacktivists to financially motivated cybercriminals. However, these local entities are often forced to make critical security trade-offs due to severe budget constraints and a chronic shortage of specialized personnel. While industry frameworks like NIST and CIS provide a roadmap for essential safeguards, many jurisdictions simply lack the financial and human capital to implement them, leaving citizen data and critical infrastructure vulnerable.

The Strategic Opportunity: Shared Services

This project solves the execution gap by centralizing expertise and procurement at the state level. Through this model, Utah can:

- **Capitalize on Economies of Scale:** Provide enterprise-grade tools at a fraction of the cost available to individual organizations, ensuring responsible stewardship of taxpayer funds.
- **Democratize Expertise:** Offer smaller jurisdictions access to top-tier cybersecurity specialists they could not otherwise afford to hire, acting as a force multiplier for overtaxed local IT teams.

Business Process and Operational Impact

The initiative transforms local operations from a reactive, resource-strained state to a proactive, supported posture. By providing direct implementation support, the state reduces the burden on local staff, ensuring that enhanced security products are effectively deployed rather than just purchased. This standardization ensures continuity of vital services—water, power, and emergency response—while protecting the integrity and privacy of citizen information.

The Case for Statewide Resilience

The Domino Effect of Local Vulnerability

Protecting Utah's local government systems is a matter of public safety. Local entities manage the "last mile" of essential services. Because the state and local jurisdictions share interconnected networks and software dependencies, a crisis in a non-state-controlled asset can rapidly escalate into a statewide emergency, as seen in the Colonial Pipeline incident. By securing local entities, the state proactively mitigates risks that would otherwise inevitably become its own problem.

The Scale of the Challenge

Utah is home to approximately **510 local government entities**, including counties, cities, and special districts. Collectively, these organizations serve every resident in the state.

- **Data-Driven Analysis:** Statewide audits measured against the NIST Cybersecurity Framework revealed significant maturity gaps, particularly in jurisdictions with limited technical staff.

Level in Hierarchy	Control Abbreviation	Control Description	Entity F	Entity G	Entity H	Entity I	Entity J	Entity K	Entity L	Entity M	Entity N	Entity O	Entity P	Entity Q	Entity R
Overall			1.3	1.4	1.6	2.2	2.3	2.9	2.4	1.5	1.6	2.0	1.7	2.5	2.4
Function	ID	IDENTIFY	1.4	1.4	1.3	1.8	2.5	2.9	2.4	1.6	2.1	2.1	1.7	2.3	2.8
	PR	PROTECT	1.6	1.8	1.9	2.1	2.6	3.1	2.6	1.8	1.9	2.2	1.9	2.6	2.8
	DE	DETECT	1.3	1.7	2.0	3.0	1.9	3.3	2.5	1.5	1.4	2.0	1.4	2.0	1.9
	RS	RESPOND	1.1	1.3	1.7	2.8	2.4	3.0	2.4	1.6	1.4	2.2	1.7	2.3	2.0
	RC	RECOVER	1.1	1.0	1.0	1.2	2.1	2.0	2.1	1.2	1.2	1.7	1.6	3.2	2.6
Category	ID.AM	Asset Management	1.9	1.7	2.0	2.4	3.0	3.2	2.5	1.5	2.3	2.1	2.0	3.0	3.0
	ID.BE	Business Environment	1.3	1.2	1.1	1.7	2.7	2.5	2.3	1.5	2.3	2.2	1.5	2.4	3.0
	ID.GV	Governance	1.4	1.4	1.1	2.0	2.7	3.4	2.3	1.4	2.6	2.4	1.7	2.5	2.8
	ID.RA	Risk Assessment	1.2	1.7	1.5	2.2	2.3	3.5	2.3	1.7	2.0	2.0	1.6	2.0	2.5
	ID.RM	Risk Management Strategy	1.2	1.1	1.1	1.2	2.2	3.0	2.4	2.1	2.4	2.1	1.7	2.0	3.1
	ID.SC	Supply Chain Risk Management	1.1	1.1	1.1	1.1	2.1	1.8	2.8	1.3	1.3	1.8	1.5	2.1	2.4
	PR.AC	Identity Management, Authentication and Access Control	1.9	2.1	2.5	2.8	2.5	3.3	2.9	2.3	2.2	2.4	2.3	2.8	2.9
	PR.AT	Awareness and Training	1.3	1.8	1.2	1.5	2.9	3.7	3.2	1.7	1.9	2.3	1.6	3.0	3.3
	PR.DS	Data Security	1.4	1.7	2.1	1.6	2.4	2.4	2.4	1.5	1.6	1.8	2.0	2.1	2.3
	PR.IP	Information Protection Processes and Procedures	1.6	1.6	1.7	2.2	2.3	3.2	2.4	1.7	2.1	2.1	2.0	2.5	2.8
	PR.MA	Maintenance	1.7	2.3	1.8	2.1	3.2	3.3	2.6	2.1	2.0	2.3	2.0	3.1	3.4
	PR.PT	Protective Technology	1.4	1.6	2.1	2.4	2.5	2.9	2.4	1.7	1.7	2.1	1.7	2.4	2.3
	DE.AE	Anomalies and Events	1.3	1.7	2.0	3.3	2.2	3.3	2.5	1.3	1.4	2.2	1.4	1.9	1.8
	DE.CM	Security Continuous Monitoring	1.4	2.1	2.4	2.9	1.7	3.4	2.8	1.8	1.5	2.3	1.6	2.3	2.2
	DE.DP	Detection Processes	1.2	1.4	1.5	2.8	1.8	3.1	2.3	1.3	1.5	1.7	1.4	1.8	1.6
	RS.RP	Response Planning	1.0	1.2	2.1	3.0	2.6	2.6	2.5	1.6	1.3	2.3	1.8	2.3	1.8
	RS.CO	Communications	1.3	1.3	1.7	2.8	2.4	3.2	2.4	1.6	1.6	2.2	1.5	2.4	2.1
	RS.AN	Analysis	1.1	1.4	1.6	2.9	2.3	3.2	2.2	1.4	1.4	2.2	1.6	2.1	2.0
	RS.MI	Mitigation	1.0	1.2	1.6	2.3	2.4	3.0	2.3	1.8	1.5	2.2	1.5	1.9	2.1
	RS.IM	Improvements	1.0	1.1	1.6	2.8	2.4	3.2	2.6	1.4	1.1	2.0	1.9	2.9	2.2
	RC.RP	Recovery Planning	1.0	1.0	1.0	1.0	2.7	2.3	2.0	1.0	1.0	1.7	1.3	3.7	3.0
	RC.IM	Improvements	1.0	1.0	1.0	1.0	1.6	1.6	2.3	1.1	1.0	1.4	1.5	3.1	2.5
	RC.CO	Communications	1.4	1.0	1.0	1.7	1.9	2.1	1.9	1.5	1.6	1.9	2.0	2.9	2.3

- **The Cost of Fragmentation:** Analysis confirmed that if each of the 510 entities sought individual funding to meet NIST standards, the total cost to Utah taxpayers would be astronomical. Inefficient use of specialized talent would result in a fragmented, weak defense.

The Shared Services Solution

Following independent evaluations, the Shared Services Model was identified as the most impactful path. This allowed the state to secure enterprise-grade software contracts at significantly lower per-unit costs and deploy a strong central core of security professionals to handle complex implementation tasks. Ultimately, investing in prevention through a unified model avoids the far greater costs associated with data breaches and the erosion of public trust.

End-to-End Lifecycle Support

Unlike traditional programs that offer either technical software or policy guidance in isolation, Utah's initiative manages the comprehensive lifecycle of cybersecurity defense:

- **Procurement Strategy:** Utilizing state-level purchasing power.
- **Technical Deployment:** Providing professional engineering support to ensure tools are integrated effectively.
- **Operational Mastery:** Empowering local personnel through training to maintain these defense systems.

The Collaborative Ecosystem

Our model maintains inclusivity for all jurisdictions, regardless of their starting maturity. This fosters an ecosystem where smaller entities gain protection from threat data identified in larger metropolitan areas, and standardized platforms enable mutual aid teams to seamlessly assist any jurisdiction during a crisis.

Strategic Scalability: A National Paradigm

The hurdles navigated by Utah's framework represent the systemic obstacles confronting the public sector nationwide. This initiative provides a replicable blueprint designed to bolster cybersecurity maturity for every state by aligning with the **State CIO Top Ten Priorities**:

1. **Cybersecurity:** Mitigating systemic risk across the regional digital ecosystem.
2. **Digital Government/Citizen Experience:** Preserving public trust through data privacy and service continuity.
3. **Workforce Development:** Building a cyber-ready workforce through professional education and statewide training.

By treating the state as a single, unified shield, Utah has established a viable national model for building a resilient, secure digital democracy.

Implementation

The Road to Implementation

The initiative followed a straightforward process of evaluation, engagement, and execution:

- **Assessment:** DTS utilized existing audits and supplemented them with professionally-backed surveys to understand current baseline capabilities.
- **Planning & Buy-in:** Data was presented to the **Cybersecurity Commission**, leading to an approved cybersecurity plan and supporting legislation for the Utah Cyber Center.
- **Testing & Rollout:** A process was built around product evaluation involving local volunteers for testing. Each service was structured as an individual project to manage the lifecycle from purchase to local sustainment.

Collaborative Stakeholders

From concept to fruition, a wide array of players were involved to ensure the program's success:

- **Executive Leadership:** The DTS CIO and CISO, the Governor's Office, and the Department of Public Safety (including SBI, SIAC, and Emergency Management).
- **The Cybersecurity Commission:** A diverse body including federal representatives (CISA, FBI), the Attorney General's Office, State Legislature, and private industry leaders.
- **Technical Architecture:** The program focused on **cloud-based vendor solutions** that could be implemented at scale into varied local environments. This layout allows for global review and response from a central point while providing local entities with state-of-the-art software and support.

Impact

Measurable Outcomes

The project has successfully built a stronger security community in Utah. To date, the initiative has:

- **Deployed protections to over 189 local government entities**, covering approximately 75% of counties and municipalities.
- **Thwarted a significant number of attacks** over a four-year span that would have otherwise led to critical incidents.
- **Increased Security Awareness:** Thousands of local government employees are now receiving professional cybersecurity training where previously none existed.
- **Expanded Mandate:** Due to its success, the State Legislature has added school districts and charter schools to the Utah Cyber Center's portfolio.

The Way Forward

The long-term plan is to transition from an onboarding focus to a **Sustainment Model** by the end of 2026. This phase will include:

- **Active Threat Hunting:** Moving to a proactive role of identification and notification, hunting across the environment to help entities remediate findings.
- **Ongoing Funding:** Collaborative efforts have secured **permanent, ongoing funding** for the local government program and the new education initiatives.
- **Continuous Evolution:** We are currently expanding into SIEM (Security Information and Event Management) and broader assessments to address emerging gaps.

Conclusion

The "Whole-of-State" model is the definitive path forward for Utah. By acting as a force multiplier, the state improves cybersecurity throughout the region, ensuring that an attack on one partner does not become a failure for all. DTS remains committed to a combined effort at all levels to combat the ever-evolving cyber threat landscape.