State of Utah
Division of Technology Services
Cyber Center

Cybersecurity
SecureUT: A Whole-of-State Cyber Collaboration

January 1, 2023 - Ongoing

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

In 2023, the State of Utah Division of Technology Services (DTS) created a program to support local government jurisdictions with cybersecurity tools, resources, and expertise. The SecureUT: A Whole-of-State Cyber Collaboration kicked off with the creation of the Local Government Cybersecurity Outreach Team and the Utah Cyber Center.

This effort focused on enhancing information sharing, providing critical cybersecurity resources and education, developing a comprehensive statewide approach to cybersecurity, mitigating cyber attack risks, improving preparedness, and strengthening incident response capabilities. By forming strategic partnerships and sharing resources, the project aimed to create a proactive security culture, elevate cybersecurity maturity, and build a resilient foundation across all levels of government in Utah, ultimately addressing the challenges of limited resources and expertise faced by local entities through the provision of security products, services, and implementation support.

Vision:

> Create a security culture of proactive collaboration and information sharing through strategic partnerships and shared resources, with the aim of fostering trust, resilience, and building a strong foundation to elevate the cybersecurity maturity across all levels of government within Utah.

Mission:

> Support local government entities in their efforts to protect communities through secure IT services and effective cybersecurity measures.

Idea

What problem or opportunity does the project address?

Local governments often face cybersecurity challenges due to limited resources and expertise. This poses a particular challenge as it forces local entities to make decisions based on funding or personnel, thus leading to a compromise in key areas of IT security. As outlined in NIST cybersecurity standards and CIS controls there are many security safeguards that should be implemented in order to properly secure an IT environment and in turn protect citizen data. When faced with these budget and personal constraints, there is not much that local entities can do but fall short on security essentials. Coupled with the vast array of sophisticated and technologically capable bad actors from nation states, hacktivists, financially motivated criminals etc., waiting and ready to exploit these vulnerabilities, it makes for the perfect environment for exploitation and cybersecurity problems.

Using existing data from cybersecurity audits, assessments, surveys, as well as having independent and additional assessments and surveys done, the vulnerabilities with local entities can be seen below. The findings are measured against NIST cybersecurity standards. Lower scores in red, oranges, yellows show where local governments lacked sufficient capabilities.

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			1.9	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

Why does it matter?

Protecting local government systems in Utah is of paramount importance as these systems support essential public services and hold sensitive citizen data. Local governments often face budgetary and personnel constraints, forcing compromises on critical IT security measures, as noted in NIST cybersecurity standards and CIS controls. This vulnerability creates an environment ripe for exploitation by sophisticated threat actors, ranging from nation-states to financially motivated criminals.

Looking across Utah and taking into account only county, city, and special district governments, the State of Utah has around 510 local government entities providing differing services covering all Utah citizens. Given the size of the constituent group served by these local governments—every resident of the state—and the potential cost of recovering from a significant cyberattack at different levels, investing in robust cybersecurity prevention measures is not just prudent but essential for the well-being and security of all Utah citizens.

What makes it different?

This project is different in its comprehensive approach of providing both security products/services *and* implementation support to local governments. Many cybersecurity initiatives might focus on one or the other or none, but this project addresses the complete lifecycle, from acquiring necessary tools to ensuring they are effectively deployed and utilized. Also, we are taking the approach of trying to help all government entities within the county, city, and special district space. By using common tools and software across all levels of government, larger government entities can assist smaller entities with cyber events without having to learn new toolsets.

Also, this is innovative and distinct as it recognizes that simply providing resources isn't enough for entities with limited expertise and staffing. By offering hands-on implementation support, the project ensures that local governments can actually leverage the security solutions effectively. This "whole-of-state package" approach, coupled with the emphasis on shared services and economies of scale, allows even smaller jurisdictions to access and benefit from top-tier cybersecurity measures that they might not otherwise be able to afford or manage. This makes the project particularly impactful and potentially sets it apart from other cyber initiatives that may not offer such a holistic level of support.

What makes it universal?

This project is universal in that it addresses several key cybersecurity challenges that are common to *all* states and local governments. Specifically:

- **Cybersecurity is a universal concern:** Every state and local government faces the threat of cyberattacks, regardless of size or location. The need to protect sensitive data and maintain critical services is not unique to Utah.
- **NIST cybersecurity standards and CIS controls:** These industry-standard frameworks are applicable and recommended for *all* government entities across the United States. Adhering to these standards is a universal best practice for cybersecurity.
- **Limited resources and expertise:** Many state and local governments struggle with budget and staffing constraints when it comes to cybersecurity. This is a widespread issue, not just isolated to Utah. The project's model of providing shared services and support could be adopted by other states facing similar challenges.
- **Threat actors:** The document mentions the variety of sophisticated threat actors, including nation-states, hacktivists, and financially motivated criminals. These threats are not limited to Utah and target governments across the country.
- **State CIO Ten Priorities:** Several of the State CIO Ten Priorities align with this project, such as:
    - **Cybersecurity:** This is a top priority for all state CIOs, and this project directly addresses this.
    - **Digital Government/Citizen Experience:** By protecting citizen data and ensuring the continuity of government services, this project contributes to a better digital government and citizen experience.
    - **Workforce Development:** The training and education components of the project help develop a more skilled cybersecurity workforce, which is a priority for many states.

Implementation

What was the roadmap?

This Whole of State cybersecurity initiative followed a straightforward process of evaluation/assessment, local engagement and buy-in, planning, legislation, identification and evaluation of resources, implementation, and finally sustainment and advanced support and review.

After first formalizing the local government outreach team, we started with a strong understanding of the need that exists. Since DTS serves the State of Utah Executive branch agencies, it has been positioned well to help local governments during past breaches and attacks. Armed with that knowledge, we started by looking at existing cybersecurity audits and assessments. We supplemented that by doing additional professionally backed assessments and surveys of local governments of current cybersecurity needs and baseline capabilities. Provided with information from this data and comparing that with best practices from NIST, CIS controls, and our own internal experience, we identified several key areas of need. We then evaluated the model to best deliver and where we could provide the most impact and security given different financial, personnel, geographic, and technological challenges that existed.

Upon creation of our Cybersecurity Commission we met and presented first the data collected and then later a plan of what resources to pursue. We then built a cybersecurity plan and had them approve it. As part of that and in conjunction the Commission supported legislation formally creating the Utah Cyber Center and requesting needed funding for the initiative.

Once we had approval of the plan and our individual projects to pursue, we built a process around evaluation of products involving locals for testing once we got to a certain evaluation stage. Each service was then built into a project in order to best plan for and manage the full lifecycle, from purchase to implementation and sustainment at the local level.

We measure or assess the success of the program through several different avenues such as, projected savings to local entities and tax payers, adoption of the different projects/programs, how many entities and users have been served, proportion of citizens covered, the number of trainings provided, how many attacks have been blocked or thwarted, and finally feedback from those using the system, getting that qualitative information of what they think about it. We have planned for the capability to get these protections in place for all county, municipality and special districts and so far have covered around seventy five percent of the counties and municipalities with much more work to be done with the special districts.

Taking into account the number of entities crossreferenced with the apparent needs in a variety of areas, the cost would be substantial if each entity pursued or was given individual funding to meet all of the needs. Knowing this, we continued with further independent evaluations to see where we might be able to leverage resources from the State level and identify which types of services would have the most impact and could be sensibly deployed given the wide range of needs and geography. Below is an example of that analysis.

Analysis Based on Feasibility/Functionality

Gartner selected 4 criteria for analyzing the feasibility/ functionality of offering a service to Entities:

- **Outsource feasibility**, based on whether a service should be outsourced or kept in-house (typically aligned to operational and governance tasks, respectively)
- Whether access to a **common network is required**, e.g., UETN
- **Relative ease of providing service**, based on the complexity of the tasks required to provide the service
- The level of **DTS CSS resource requirements** based on whether personnel or software licenses are required, and the rough estimate of time required to provided the service.

Service Type (EISS Bundled Security Services)	Outsource Feasibility	Common Network Required	Relative Ease of Providing Service	DTS CSS Resource Requirements	Service Type (EISS Optional Services)	Outsource Feasibility	Common Network Required	Relative Ease of Providing Service	DTS CSS Resource Requirements
Application Security Testing	Y	N	H	M	Asset Procurement	P	N	H	L
Continuous Monitoring/SIEM	Y	Y	H	M	Risk Assessment Scans (ARCHER GRC)	Y	N	M	M
Forensics	Y	N	H	L	Server Administration	P	N	M	M
Information Security Management	P	N	M	H	Web URL Filtering	Y	Y	H	L
Proactive Ops - Penetration Testing	Y	N	M	H	Cloud Hosting & Storage	P	N	M	L
Proactive Ops - Phishing campaigns	Y	N	M	L	Data Centre (Rack Space)	Y	N	H	M
Proactive Ops - Threat Hunting	Y	N	L	M	Desktop-as-a-Service (DaaS)	P	N	H	M
Quality Assurance and Compliance	Y	N	M	M	Backup Data Centre Facilities (Richfield)	Y	N	M	L
Security Awareness Training & Education	P	N	M	L	Security Advisory/Consulting	Y	N	H	M
Security Incident Response Management	P	N	H	M	Application Hosting (Wordpress in AWS)	Y	N	M	L
Security Operations and Maintenance	Y	Y	L	M	Security Assessments (custom)	N	N	L	M
Security Review/Assessment	Y	N	L	M	Authentication Services (UtahID)	Y	N	M	L
Strategic Planning & Management	N	N	M	M	Authentication Services (2FA)	Y	N	H	L
System and Application Security	P	N	L	H	Transition to Cloud (Advisory/Consulting)	Y	N	H	L
Vulnerability Management	Y	Y	H	M		Y = Yes	Y = Yes	L = Low	L = Low
PCI-Data Security Standard (DSS) Compliance	Y	N	H	L		P = Partial	N = No	M = Moderate	M = Moderate
Security Risk Management	P	N	L	M		N = No		H = High	H = High

Findings were that if we established a shared services model acquiring software contracts, providing personnel, and working with locals, we could protect major vulnerabilities with limited costs and a strong central team to support. Thus saving money and time in personnel and technology costs, taking advantage of economies of scale on software licensing and a strong central core to help with implementation and deployment of these services.

Who was involved?

Entities involved in the project were:

- Utah Cybersecurity Commission
- Division of Technology Services - Cyber Center - Enterprise Security, Local Outreach Team
- Department of Public Safety - State Information Analysis Center, State Bureau of Investigations, Division of Emergency Management
- Federal partners - CISA, FBI
- Utah Attorney General's Office

- City and County representatives

How did you do it?

From a technical architecture perspective we focused all of the projects and actual software deliverables around cloud based vendor solutions that could be implemented on a wide scale and into varied technical environments locally with a wide array of maturity levels in cybersecurity. From that perspective we would also have the greatest ability to help implement, respond for assistance, and review. Beyond that we have the technical background and support of the existing State of Utah Division of Technology Services to lend help and provide other needed tools here and there to support the effort. This includes one off software like remote tools, or planning and project software to keep everything moving in a productive manner.

Impact

What did the project make better?

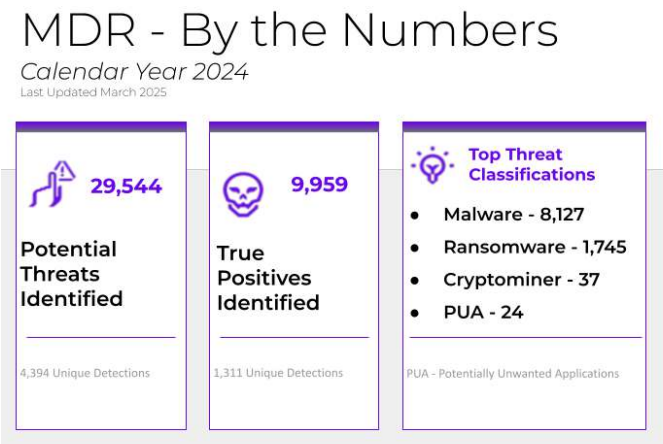
Overall the project has been a success in that it is helping to build a stronger security community in Utah through cooperation and common platforms, leading to a large group that is used to communicating and that can aid each other during incidents in the future while also meeting the objective of saving tax pay dollars and providing high end toolsets that were not accessible to everyone previously. We have increased security in key areas across the board either for those that did not have endpoint, vulnerability management/patching, and training of IT and government employees or by amplifying those services.

How do you know?

We know that this has been effective from a cooperation standpoint because anecdotally we are seeing more of that cooperation through discussions and meetings, and from a numbers standpoint reporting of attacks across all sectors has increased. We have also been called to lend more aid during these attacks.

From those directly participating in the program and receiving security services, we have participation numbers and numbers from attacks. For instance, with our endpoint protection we know what services were being used before or not at all versus now. We have also seen them replaced with this better service and have numbers for deployment. We have deployed to over 144 local government entities which results in over 27, 900 endpoints being deployed.

As noted in the following graphic we can track the number of thwarted attacks against participants and over a one year span thwarted a significant number of attacks that would have led to many different incidents and issues.



Before implementation of our training services, most entities were not providing security awareness training to their employees. To date we have 161 total accounts with over 33,000 total seats being utilized.

What now?

Our plan long term is to continue to evaluate the success of the program and the overall increase in security by performing a yearly survey of baseline capabilities versus improved security of all of the local government entities. We also intend to use this data to supply new services to local government entities where possible. We have not yet completed the push out to all of the entities we are focused on for our current services and will continue to do that through this year, with the goal to have onboarded all entities that wish to participate by the end of 2025. The plan from there is to move into more of a sustainment stance and less of an onboarding stance. The sustainment aspect will entail us doing health checks of the systems and how they are operating, where the software policies are set and the like. We also intend on moving to more of an active role of identification and notification, where we threat hunt across the environment and send any findings on to entities to remediate.

We have funding to maintain this program until 2028 and are actively working with our locals, through our Commission and with legislators to obtain ongoing and sustained funding. In any other identified need or gap areas, we are pursuing new technologies and processes for expanding the program to address the other needs. We hope to assist in as many areas as reasonable to help entities long term with cybersecurity without taking over their environments, thus focusing as more of force multiplier. We already have plans to add to our current offerings and program in the SIEM space and in assessments and evaluations.

As outlined throughout, we believe the initial and long-term investment in time, personnel, and funding towards this program is a net positive for Utah at the local government level, State level and just in general. The program has proved successful so far and the Whole of State model is the way forward as cybersecurity and the challenges of manpower and funding will always be a challenge going forward. It is important for the State to help improve cybersecurity throughout Utah as an attack on one of our government entities or downstream partners can easily spread to others or back to the State in the form of similar attacks due to connected systems, user accounts, or in the form of new targeting through phishing and other similar types of attacks. DTS and the State of Utah see that the only way forward in combating cyber threats is through a combined effort at all levels which is exactly what our program is all about.