Utah Cybersecurity Commission

Executive Summary

This year the Utah Cybersecurity Commission completed its second year as a Commission. Following its first year report and recommendations, SB127 was passed during the 2023 legislative session and signed into law. This bill amended the disclosure requirement for system security breaches and requires the Division of Technology Services (DTS) to report certain information regarding the consolidation of networks used by governmental entities. It also codified the Utah Cyber Center (UCC) and defines the center's duties including the intake of breach reporting. Additionally, the bill requires government entities to use authorized domains (.gov) by January 1, 2025.

The Commission held its first meeting for the 2023 session in April. In subsequent meetings, each subcommittee built off their first year recommendations to determine focus areas for the year. In July, the Commission held a second Commission meeting to approve grant recipients for the State and Local Cybersecurity Grant Program (SLCGP). In October at the final Commission meeting, the subcommittees proposed new recommendations for the Commission's annual report. Subcommittee findings include recommendations to hold an annual table top exercise and conference, focus efforts on assisting Utah Government entities adoption of best practices, fund the match requirement for the SLCGP, and develop a UCC Incident Response Team.

2023 Accomplishments:

Following the passage of SB 127, some noteworthy items the UCC accomplished based on the recommendations of the Commission were:

- The formalization and expansion of the UCC.
- Approval of a Utah Cybersecurity Plan that identified key statewide projects to be implemented using the SLCGP funds, with the projects managed and administered by the UCC.
- Creation of a UCC website to serve as an intake point for breach reporting pursuant to UC 13-44-202.
- The development of an application process for local agency subrecipients, and the distribution of funds associated with the SLCGP.

State & Local Cybersecurity Grant Program (SLCGP):

The Cybersecurity Commission continues to have a crucial role in determining what cybersecurity projects Utah will provide under the SLCGP. DTS manages the grant application. Following the first year's approval for the allocation of grant funds, DTS opened applications for UT entities to apply for funding of cybersecurity projects.This year the Cybersecurity Commission assisted with the review of SLCGP applications and voted to approve applicants. The Commission approved multiple statewide projects aimed at improving cybersecurity throughout local governments within Utah. These included: an endpoint protection platform, endpoint vulnerability management, security awareness training for all government employees, and the development of security professionals by providing access to training and certifications.

Assessment of Cyber Threats to Utah:

The Cybersecurity Commission also received an assessment of cyber threats to Utah. In that report some of the major concerns include:

- Cryptocurrency crimes continue to increase in Utah, with scams involving cryptocurrency increasing from $10 million in losses in 2021 to over $28 million in 2022.
- Phishing and spear phishing continue to be a problem, especially for Utah businesses. Utah victims lost over $26 million in 2022 due to Business Email Compromise alone (a cyber attack where attackers target businesses with phishing emails in an attempt to defraud them).
- Ransomware is still prevalent and impacting Utah government and businesses.
- Cyber criminals, hacktivists, and nation state actors continue to target critical infrastructure in Utah, including the energy, defense industrial base, healthcare, food and agriculture, and government facilities sectors.
- Cyber threats, including the number of victims, reported losses, and damage and disruption to businesses will continue to increase.
- While there is no specific threat to Utah currently, Advanced Persistent Threat (APT) groups also continue to be a concern for Utah as geopolitical tensions rise in the Middle East, Russia, Taiwan, and China.

Public/Private Partnership Engagement & Outreach Subcommittee Recommendations:

1. We recommend the development of a contact management platform, maintained by the State and updated by local municipalities and essential critical infrastructure entities.
    a. The platform will contain a designated information technology (IT)/cybersecurity contact for each municipality, county, and essential critical infrastructure, to keep their information updated annually.
        i. Information required: entity name, contact name, phone number, and email address.
        ii. The purpose of this platform is to facilitate communication between entities and expedite dissemination of critical cybersecurity information.
        iii. This information should not be publicly accessible.
        iv. Considerations should be made to ensure registration compliance does not cause undue burden.
    b. We recommend considering the amendment of existing legislation (67-1a-15) which created an Entity Registry (https://entityregistry.utah.gov/s/search-entity) that is similar in function to the recommended database, but currently serves other purposes. The Entity Registry and its underlying legislation could be examined for expansion to include the above-mentioned government and essential critical infrastructure contacts in the State.
        i. Alternatively, should it be determined that amending this legislation in such a manner is inappropriate, we would propose using the existing registry to point entities to another location, where this data could be maintained as previously recommended.
2. We recommend that an annual table-top exercise be conducted.
    a. It should include representation from the following entities:
        i. State and Local Government
        ii. Department of Homeland Security (DHS) Cybersecurity & Infrastructure Security Agency (CISA)
        iii. Private Critical Infrastructure (specifically with essential critical infrastructure sectors).
    b. This exercise should focus on topics related to cybersecurity and promote collaboration between the represented entities.
3. We recommend that an annual gathering (conference/meeting/working group) be held which would serve to bring together State, Local, Federal, and Private Critical Infrastructure cybersecurity representatives, for the purposes of fostering unity, creating working relationships, sharing information, and the improvement of inter entity cooperation.
    a. We recommend considering existing forums that could be expanded to accommodate these gatherings. For example, the Utah Digital Government Summit could be expanded to include such gatherings.

Many of these recommendations fall in line with the duties assigned to the UCC, and therefore recommend that any accepted recommendations should be implemented through their

operations and the resources necessary, namely funding and personnel, should be allocated in order for these recommendations to be successfully adopted.

Cybersecurity Assets & Resources Recommendations:

1. We recommend funding the match requirement for the SLCGP for years 2-4, in order for Utah to take full advantage of the federal program and help approved projects be successful over the next 4+ years.
    a. Year 2 (Federal FY2023) - $1,337,092
    b. Year 3 (Federal FY2024) - $1,683,591
    c. Year 4 (Federal FY2025) - $872,937
2. In keeping with last year's recommendation, we have found the need to find long term funding for cybersecurity improvements for State and Local government, the UCC, and staffing. Therefore, we recommend sustained long term funding for the State and local government entities to implement best practices and projects as identified by the commission.
    a. Along with the recommendations for funding, the proposed solutions should also include:
        i. Standards and specifications to which these systems should be implemented
        ii. Expert advice related to the implementation of these systems
        iii. Priority given to implementations that support a shared service model or Whole-of-State approach, leveraging a unified solution

Cyber Incident & Disruption Response Recommendations:

1. S.B. 127 amended UC 63A-16-510, and assigned to the UCC the duty of coordinating cybersecurity incident response, the duty to serve as the state cybersecurity incident response hotline, and the duty to develop incident response plans to coordinate federal, state, local, and private sector activities.
    a. We recommend sustained funding for software, hardware, and personnel that can be used by the UCC to develop an Incident Response team that will be used for incident response of cybersecurity breaches for State and local government entities, and assist where appropriate with critical infrastructure, and hold harmless agreements for entities reporting or requesting assistance.
2. We have identified the need for local government entities to create and implement their own internal incident response plans.
    a. We recommend funding and personnel to assist local government entities with evaluating their environments through a business impact analysis, then building and implementation of incident response plans.

Cybersecurity Best Practices and Recommendations:

1. We recommend that the following items are presented and promoted to State and local governments:
    a. Promote the UCC website for reporting security breaches related to Utah residents.
    b. Promote participation in CISA free services - develop cybersecurity resilience and maturity by participating in CISA's voluntary no-cost cybersecurity resources.
    c. Require/Promote participation in MS-ISAC NCSR (for government entities) or other yearly assessment program.
    d. Promote the adoption of the CIS Critical Security Controls and Cyber Hygiene guide, or the National Institute Standards and Technology (NIST) Cybersecurity Framework, dependant on the maturity of the organization.
    e. Promote the adoption and implementation of a Business Continuity Plan that includes:
        i. Business Impact Analysis
        ii. Incident Response plan
        iii. Disaster Recovery Plan
        iv. Continuity of Operations Plan

    We believe that additional resources, including funding and personnel, are needed in order for many Utah Government entities to be able to achieve these goals, and we believe that funding should be allocated for that purpose.

2. We recommend that additional efforts should be focused on assisting Utah Government entities in the adoption of the following key best practices that are highlighted by CISA through guidance given in the Infrastructure Investment Jobs Act (IIJA) and are key controls outlined in NIST Cybersecurity Standards.
    a. The key best practices are:
        i. Implementation of multi-factor authentication
        ii. Implementation of enhanced logging
        iii. Data encryption for data at rest and in transit
        iv. Prohibiting the use of known/fixed/default passwords and credentials
        v. Ensuring the ability to reconstitute systems (backups)
    b. We recommend that these additional efforts should include:
        i. Securing funding sources for implementation to promote adoption of these key best practices
        ii. Identifying standards to which these best practices should be implemented
        iii. Providing expert advice related to the implementation of these best practices
        iv. Evaluation of the efficacy of meeting these best practices through a Whole-of-State solution
3. We recommend monitoring of cybersecurity issues with regards to efforts of Utah state entities to enhance data transparency, define data use, promote data privacy, and define Utahn's data management rights.

Funding Requests:

Many of the Cybersecurity Commission recommendations highlight the need for additional funding to improve the cybersecurity posture of the state to provide ongoing resources.

1. State funding gaps:
    a. We recommend funding the match requirement for the SLCGP for years 2-4, in order for Utah to take full advantage of the federal program and help approved projects be successful over the next 4+ years.
        i. Year 2 (Federal FY2023) - $1,337,092
        ii. Year 3 (Federal FY2024) - $1,683,591
        iii. Year 4 (Federal FY2025) - $872,937
    b. We recommend sustained long term funding for the State and local government entities to implement best practices and projects as identified by the commission. Proposed solutions should include standards and specifications to which these systems should be implemented, expert advice related to the implementation of these systems, and priority given to implementations that support a shared service model or Whole-of-State approach, leveraging a unified solution
    c. We recommend sustained funding for software, hardware, and personnel that can be used by the UCC to develop an Incident Response team that will be used for incident response of cybersecurity breaches for State and local government entities, and assist where appropriate with critical infrastructure.
    d. We recommend funding and personnel to assist local government entities with evaluating their environments through a business impact analysis, then building and implementation of incident response plans.
    e. We recommend funding and personnel to assist with promoting participation in CISA services, promoting/requiring participation in MS-ISAC NCSR program, adoption of cybersecurity frameworks, and assisting with the implementation of Business Continuity Plan.
    f. We recommend funding and personnel to assist with the development of a contact management platform, maintained by the State and updated by the local municipalities and essential critical infrastructure.
    g. We recommend funding and personnel to assist with an annual table-top exercise be conducted and an annual gathering (conference/meeting/working group) be held which would serve to bring together State, Local, Federal, and Private Critical Infrastructure cybersecurity representatives, for the purposes of fostering unity, creating working relationships, sharing information, and the improvement of inter entity cooperation.

Acknowledgements:

The Cybersecurity Commission would like to thank the dedicated members of each of the subcommittees volunteering their time and expertise, as well as the Statewide Information & Analysis Center (SIAC) staff for coordinating and facilitating the Cybersecurity Commission.

Governor Spencer J. Cox, Cybersecurity Commission Chair
DPS Commissioner Jess Anderson, Cybersecurity Commission Co-Chair

Public/Private Partnership Engagement & Outreach	***Cybersecurity Assets and Resources***	***Cybersecurity Best Practices and Recommendations***	***Cyber Incident and Disruption Response***
Chair: Nathan Lee	*Chair: Phil Bates*	*Chair: David Sonnenreich*	*Chair: Mayor Tamara Tran*
Austin Tsosie	*Alan Fuller*	*Ben Mehr*	*Brody Arishita*
Ty Howard	*Patrick Hawkins*	*Bobette Phillips*	*Curtis Mansfield*
Yvonne Hogle	*Stephen Hess*	*Bryan Farnsworth*	*Erick Wiedmeier*
Matthew Beaudry	*Wade Kloos*	*Jerry Gearheart*	*Mark Mitchell*
Dennis Rice	*Rep. Jon Hawkins*	*Matt Ceniceros*	*Rebecca Brown*
Joe Masnica	*Albert Gonzalez*	*Sen. John Johnson*	*Troy Jessup*
Blake Larsen	*John Coker*	*Jason Hoyt*	*Zachary Posner*
Annette Newman	*Julissa Garfias*	*Sean Stalzer*	*Brent Robertson*
Matt Miller			*Michael Pickett*
Tara Thue			*Derrek Spencer*

Thank you to the individuals who contributed to one or more of the subcommittees:

Richard Gardner, Travis Scott, Ken Wheeler, Eric Jensen, Braxton Barker, Brandon Amacher, Captain J. Tanner Jensen, Hanna Bennett, Katherine Chipman, Mallorie Nielsen, Erin Mortensen, Daniel Mealy, Hannah Grayson. & Tyson Jarrett.