utah govops

UTAH DEPARTMENT OF GOVERNMENT OPERATIONS

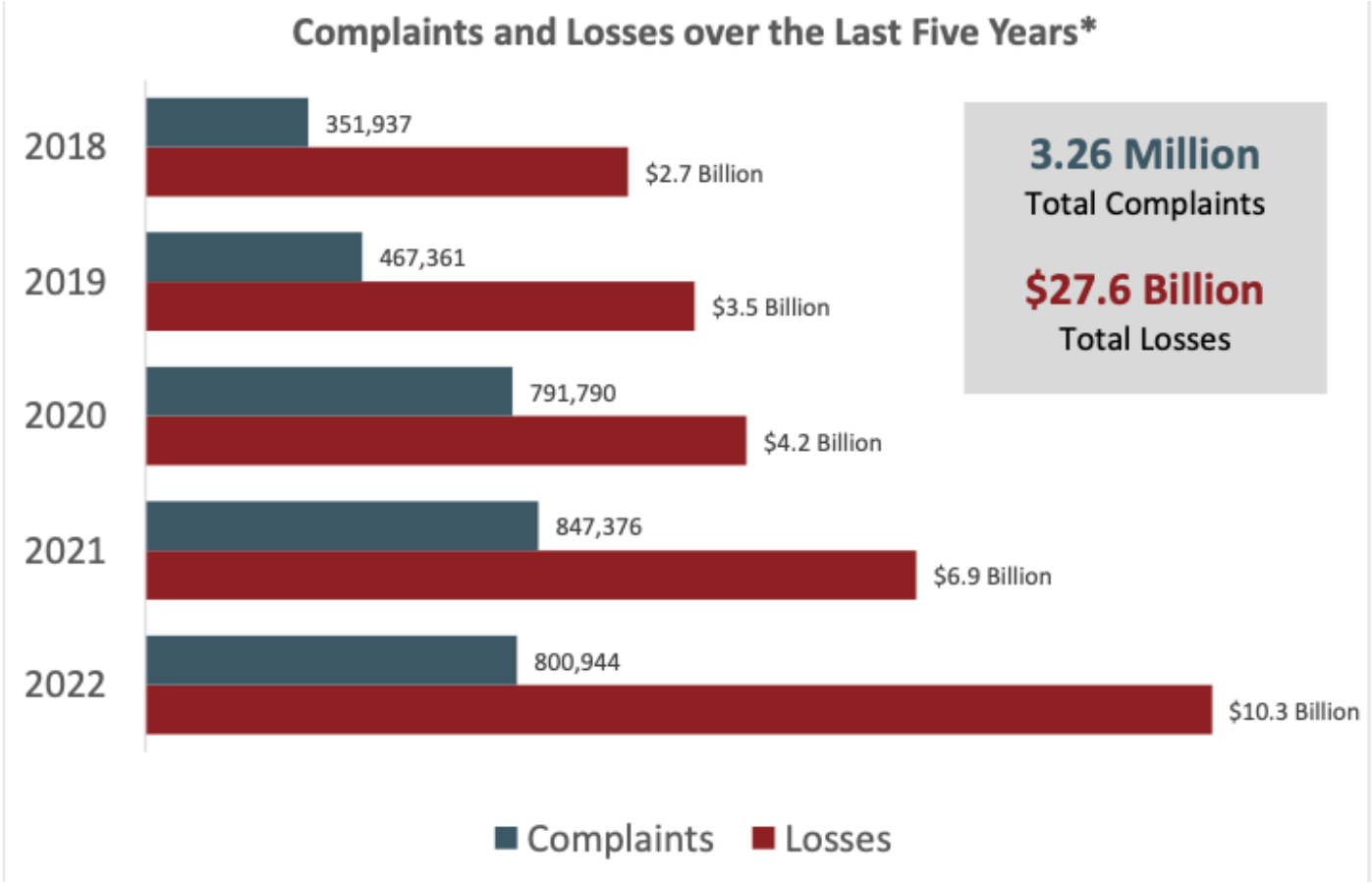
Division of Technology Services

Alan Fuller

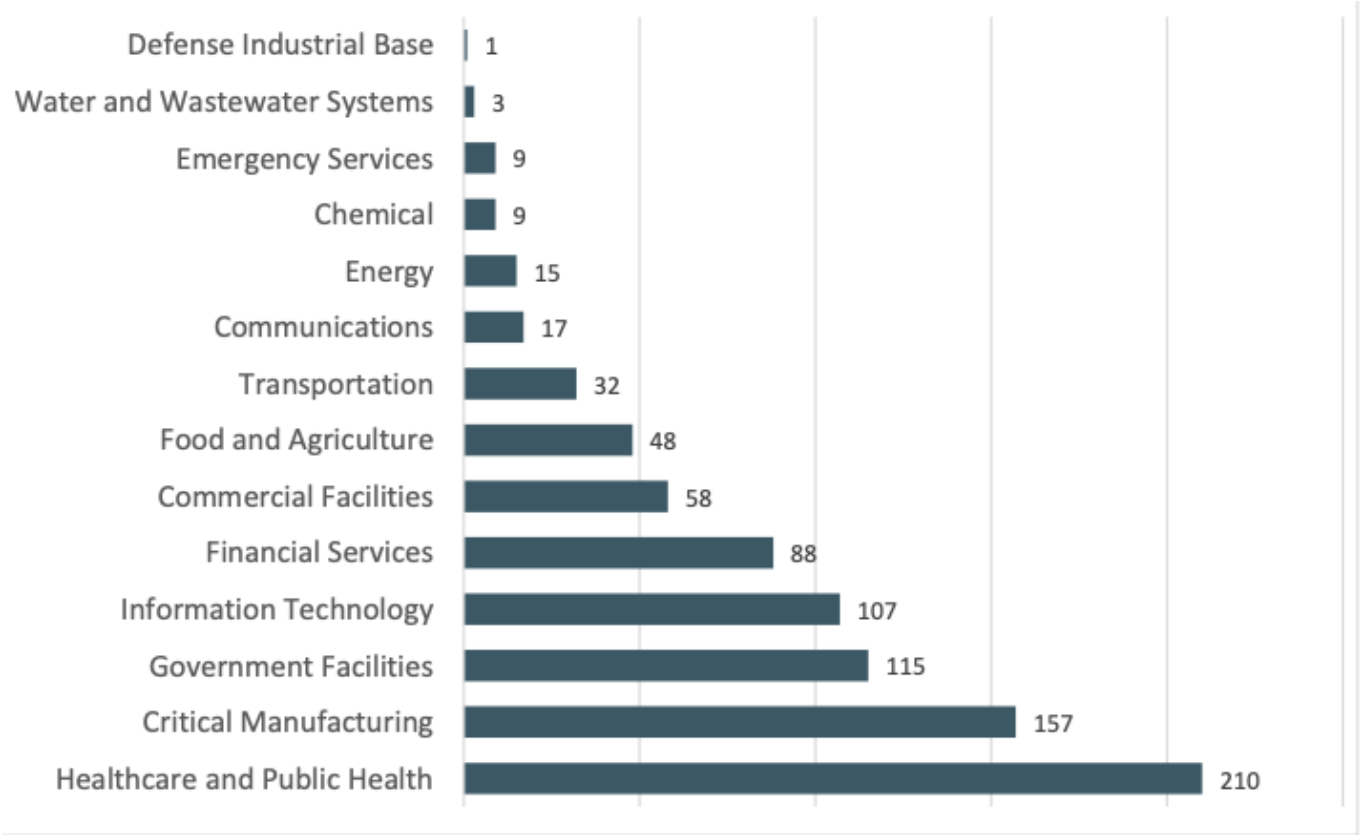
Information Security Officer

Statistics

FBI – IC3 Statistics



Ransomware by Sector



Cyber Center

What is the Utah Cyber Center?

Utah Cyber Center

Director: Philip Bates, State CISO

- Cybersecurity Commission
- Federal Bureau of Investigation
- Utah Office of the Attorney General

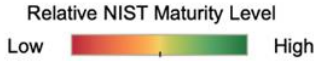
- Department of Public Safety
  - State Bureau of Investigation
  - Division of Emergency Management
  - Statewide Information and Analysis Center
- Division of Technology Services
  - Enterprise Security Services
  - City/County Cybersecurity Outreach

- Utah Education and Telehealth Network
- CISA
- ULCT & UAC

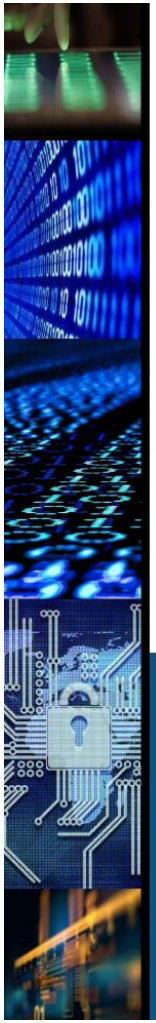
Cybersecurity Assessments and Surveys

1. Independent firm Gartner (2 separate assessment completed)
2. Legislative Cybersecurity Audit (2023)
3. State Cybersecurity Audit
4. Cybersecurity needs survey - conducted by UVU Emerging Technology Policy Lab

All NIST CSF Function and Category Scores



Level in Hierarchy	Control Abbreviation	Control Description	Central Security Services	Entity A	Entity B	Entity C	Entity D	Entity E	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	Average
Overall			3.62	2.4	2.3	1.6	1.9	2.4	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	2.1
Function	ID	IDENTIFY	3.69	2.5	2.0	1.8	2.2	2.7	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	2.1
	PR	PROTECT	3.82	3.0	2.3	2.0	2.3	2.8	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	2.3
	DE	DETECT	3.60	2.3	3.0	1.6	2.1	2.2	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	2.1
	RS	RESPOND	4.18	2.2	2.7	1.4	2.0	2.3	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	2.0
	RC	RECOVER	2.83	1.9	1.7	1.3	1.1	1.9	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	1.7
Category	ID.AM	Asset Management	4.19	3.1	2.1	1.9	2.9	3.4	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	2.5
	ID.BE	Business Environment	3.92	2.4	1.9	1.6	1.9	2.5	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	2.0
	ID.GV	Governance	4.20	2.5	2.0	1.7	2.3	2.7	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	2.2
	ID.RA	Risk Assessment	3.68	2.6	2.3	1.7	2.3	2.6	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	2.1
	ID.RM	Risk Management Strategy	3.77	2.1	1.6	2.0	2.2	2.6	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	2.0
	ID.SC	Supply Chain Risk Management	2.37	2.0	1.9	1.8	1.6	2.4	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	1.7
	PR.AC	Identity Management, Authentication and Access Control	4.49	3.6	2.6	2.5	2.9	3.0	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	2.6
	PR.AT	Awareness and Training	3.68	2.5	3.0	2.2	1.8	3.0	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	2.3
	PR.DS	Data Security	3.74	2.8	1.5	1.7	1.7	2.5	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	2.0
	PR.IP	Information Protection Processes and Procedures	3.61	2.8	2.2	1.8	2.0	2.6	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	2.2
	PR.MA	Maintenance	3.52	3.3	2.3	2.2	3.0	2.9	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	2.5
	PR.PT	Protective Technology	3.89	3.2	2.0	1.8	2.4	2.6	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	2.2
	DE.AE	Anomalies and Events	3.94	2.2	3.2	1.5	1.9	2.3	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	2.1
	DE.CM	Security Continuous Monitoring	3.44	2.7	2.9	1.9	2.2	2.5	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	2.2
	DE.DP	Detection Processes	3.43	2.1	2.9	1.5	2.2	1.8	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	1.9
	RS.RP	Response Planning	4.92	2.0	2.7	1.2	2.1	2.2	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	2.0
	RS.CO	Communications	4.14	2.5	2.9	1.7	1.9	2.6	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	2.1
	RS.AN	Analysis	3.70	2.1	2.9	1.5	1.7	2.3	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	2.0
	RS.MI	Mitigation	3.81	2.1	2.5	1.5	1.9	2.4	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	2.0
	RS.IM	Improvements	4.33	2.3	2.6	1.1	2.3	1.8	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	2.0
	RC.RP	Recovery Planning	3.00	2.3	1.7	1.0	1.0	1.7	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	1.7
	RC.IM	Improvements	2.42	1.6	1.1	1.1	1.0	1.9	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	1.5
	RC.CO	Communications	3.07	1.7	2.3	1.7	1.3	2.2	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	1.8



State of Utah Cybersecurity Plan

April 2023

Security Service Recommendations Summary

Using the earlier work Gartner performed with DTS as a basis, and corroborated with the analysis of prior security assessments of municipal entities, Gartner recommends the following Security Services be offered to the municipal entities across the State to improve the security posture of the entire State:

Security Service
Endpoint Detection & Response (EDR)/Managed Detection & Response (MDR)
Security Awareness Training
Cloud-based Backup Storage
Continuous Monitoring (SIEM)
Vulnerability Management – Scanning
Vulnerability Management – Patching
Security Incident Response Management

Cybersecurity Assets & Resources

1. We request funding the match requirement for the State and Local Cybersecurity Grant Program (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

Request Total: $3,893,621 (One time funding)
Federal Funding - $13,205,072 - From the SLCGP

Local Governments Program Adoption

118 different entities signed up for services and are in various states of onboarding

Endpoint Protection Platform to date:

65 unique Accounts created

13,100 installed endpoints