RFA: Utah Cyber Center - Local Government Cybersecurity Support

Representative Carl Albrecht

What is the Utah Cyber Center?

Utah Cyber Center

Director: Philip Bates, State CISO

- Department of Public Safety
  - State Bureau of Investigation
  - Division of Emergency Management
  - Statewide Information and Analysis Center
- Division of Technology Services
  - Enterprise Security Services
  - Local Government Outreach

Cybersecurity Commission

Federal Bureau of Investigation

Utah Office of the Attorney General

Utah Education and Telehealth Network

CISA

Local Entities

All NIST CSF Function and Category Scores

Relative NIST Maturity Level

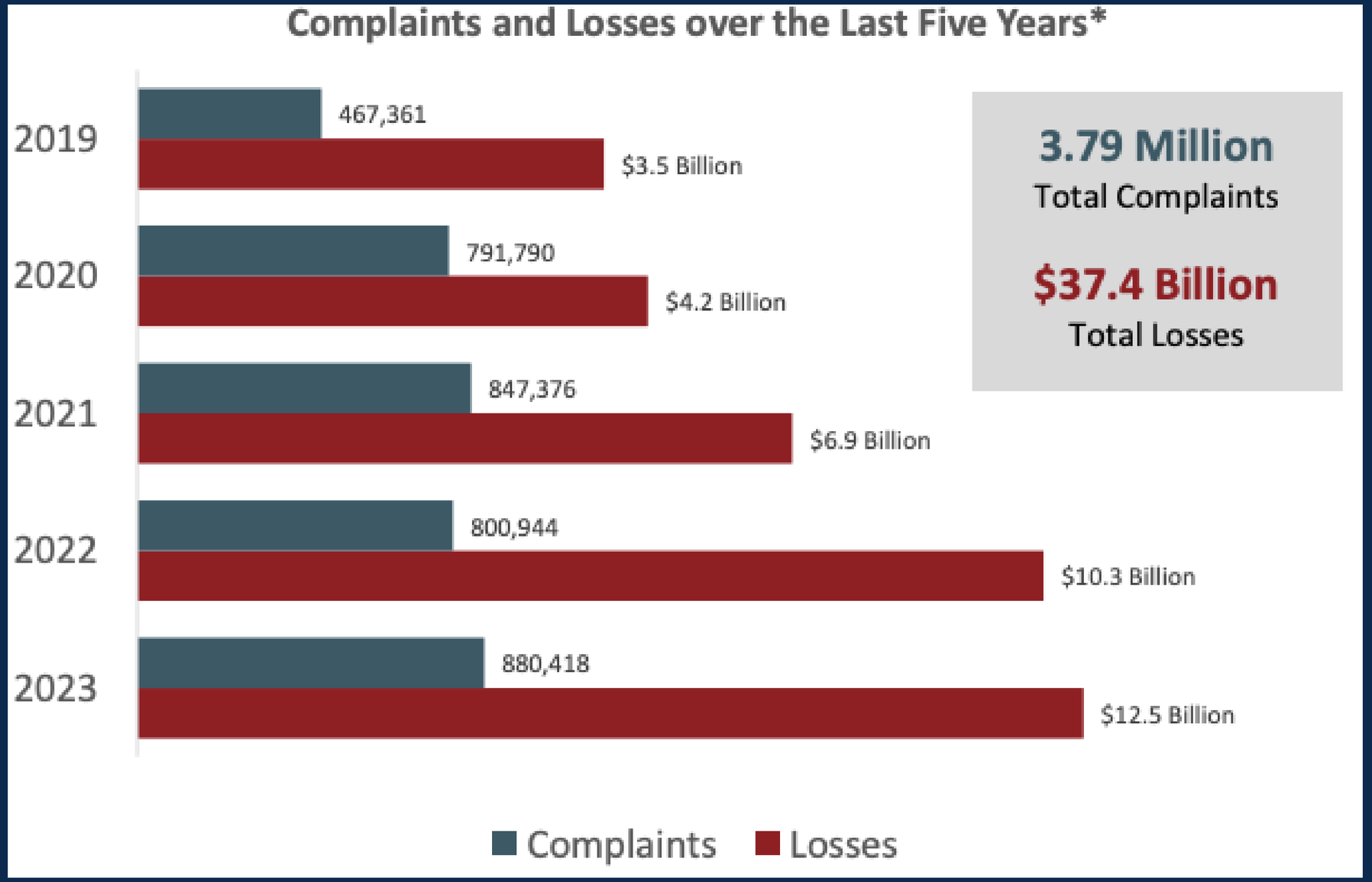
Low — High

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

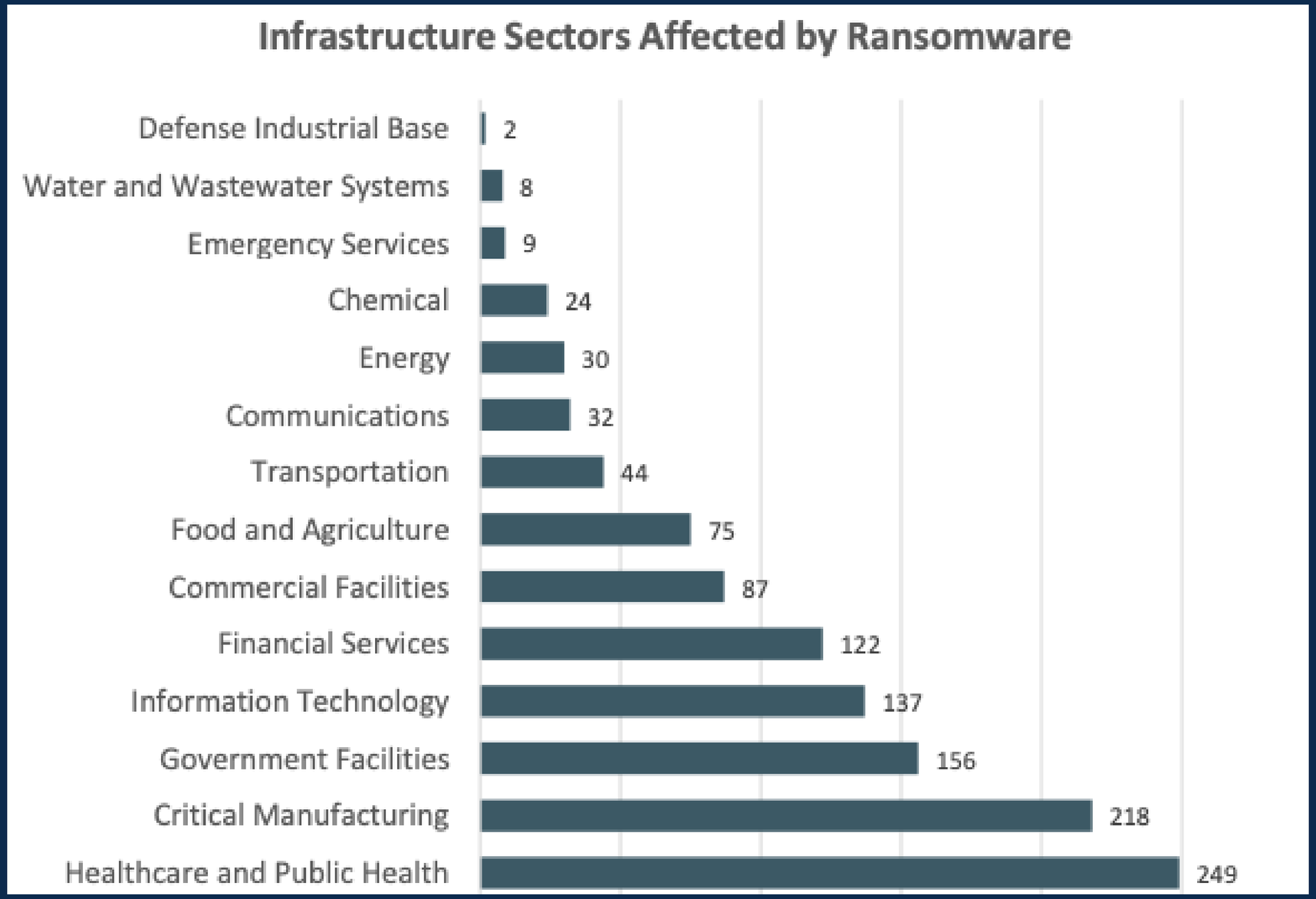
Perimeter Blocking - Geo Blocking

- 2020 – 1.2 Billion per day
- 2021 – 1.7 Billion per day
- 2022 - 1.5 Billion per day
- 2023 - 1.5 Billion per day
- 2024 - 1.5 Billion per day

FBI – Internet Crime Complaint Center Statistics



Ransomware by Sector



Results to date (1 year)**:**

Endpoint Protection:

- Onboarded:
  - Counties - 23
  - Cities - 94
  - Special Districts - 23
  - Total Accounts - 140
  - Total Endpoints - 26,824

True positive incidents: 9,255

Prevented 4 major incidents

Security Awareness Training:

- Onboarded:
  - Counties - 22
  - Cities - 104
  - Special Districts - 31
  - Total Accounts - 157
  - Total Seats- 31,090

9 newsletters, 4 quarterly trainings, 2 phishing campaigns

IT Professional Cybersecurity Training/Certification:

- 8 classes completed
- 200 Local IT professionals trained

*Expectation was to achieve 10,000 endpoints and 30-50 entities in year 1.

Request for Appropriation:

$5,000,000 ongoing FY 2028

Breakdown:

Category	Amounts	Details
Personnel	$1,058,190	6 FTEs to administer and support the City/County/Special District program, including assessing and addressing cyber risk, implementing cybersecurity programs, conducting threat hunting, assisting with data breaches, incident response, consultation, and assisting local entities with improving cybersecurity.
Licenses	$3,628,333	Endpoint (computer/server) protection and vulnerability scanning licenses, vulnerability patching software, email security, network security software licensing (SIEM, SOAR, firewalls, and network logging software)
Employee - Cybersecurity Training	$125,477	Cybersecurity awareness and compliance training for all localentity personnel.
Professional IT - Cybersecurity Training	$80,000	Professional IT cybersecurity training and certification for localgovernment IT staff.
.gov Requirement	$108,000	Assistance with .gov requirements for website and email services for entities with populations of 10,000 or less.