STATE PRIVACY OFFICER

Dr. Whitney Phillips
wphillips@Utah.gov
April 2022
Remember

Don’t Panic
Don’t Wait
Get Help
Why is the state government an attractive target?

- Technology adoption
- Very low security
- Lots of data
Cost of 1 Terabyte of Data

2000: $17,000
2020: $3
THE RISKS

out of the
70 MILLION devices
lost or stolen each year
ONLY 7% recovered

- 15% of employees have accessed sensitive data from non-work-sanctioned devices
- 54% of organizations don’t include employee-owned devices in their backup plans
- 65% of companies cannot wipe devices remotely
- 76% of companies do not encrypt mobile devices
Privacy and Security Fanatic

By Mrs. Smith, CSD  Oct 3, 2017 8:45 AM PT

News

Dark Overlord hacks schools across U.S., threats against kids to parents

Schools in Iowa, Montana, Texas and Alabama were hacked, and threats of violence and kids were texted to parents.

Telephone Terrorism

‘Dark Overlord’ Hackers Text Death Threats to Students, Then Dump Voicemails From Victims

The same hackers who tried to extort Netflix have moved onto another

Des Moines Register

Education Department warns of new hacker threat as ‘Dark Overlord’ claims credit for attacks on school districts

By Valerie Strauss and Mariah Railing  October 26 25
The secret police: Cops built a shadowy surveillance machine in Minnesota after George Floyd’s murder

An investigation by MIT Technology Review reveals a sprawling, technologically sophisticated system in Minnesota designed for closely monitoring protesters.

By Tate Ryan-Mosley & Sam Richards
March 3, 2022
2021 HB 243: Privacy Protection Amendments

Personal Privacy Oversight Commission (PPOC)
- Investigates complaints
- Develops standards and best practices
- Recommends legislation

Two state privacy positions
- Government Operations Privacy Officer
- State Privacy Officer

Creates a reporting requirement
- Annually, on or before Oct 1, the commission shall report to the Judiciary Interim Committee
State Privacy Officer Responsibilities

1. Analyze and report on government privacy practices
2. Provide educational and training materials
3. Identify privacy practices that pose the greatest risk to individual privacy and prioritize those privacy practices for review
4. Respond to requests from individuals to review a designated government entity’s privacy practice
5. Make privacy recommendations to the State Legislature
Scope

1,147 government entities:
- Local and Special Service District 391
- Local Education Agency 152
- City 146
- Town and townships 108
- Redevelopment /Project Area 89
- State of Utah (depts/comp, units) 67
- Interlocal 62
- Conservation District 38
- County 29
- Housing 19
- Institution of Higher Education 18
- Misc. 28

262,860 employees
My Plan: 2022

Measure Baseline
Deliver Resources

Build Relationships
Privacy Maturity Survey

- All Local Education Agencies, 153
- All Counties, 29
- All other designated government entities with 50 or more employees, 168

*53% response rate*
<table>
<thead>
<tr>
<th>Maturity Level</th>
<th>Contracts with Clients &amp; Partners</th>
<th>Infrastructure &amp; Systems Management</th>
<th>Policy Documentation</th>
<th>Privacy Awareness &amp; Training</th>
<th>Privacy Budget</th>
<th>Privacy Function</th>
<th>Privacy Incident Management</th>
<th>Privacy Personnel</th>
<th>Risk Assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Contracts do not address privacy</td>
<td>Procurement of IT-related products &amp; services do not address privacy</td>
<td>There are no documented privacy policies</td>
<td>Contents of privacy policies are never communicated to personnel</td>
<td>There is no budget specifically allocated to privacy purposes</td>
<td>There is no assigned privacy office or function</td>
<td>There is no way to respond to suspected incidents</td>
<td>No one person with a job description of a privacy officer</td>
<td>Project plans &amp; acquisition of IT-related products do not address privacy</td>
</tr>
<tr>
<td>1</td>
<td>Confidentiality clauses are included, but compliance cannot be monitored</td>
<td>Project and IT managers occasionally address privacy in plans &amp; system development</td>
<td>Multiple, inconsistent policies, or policies that do not address all privacy principles</td>
<td>Some contents of privacy policies are communicated to some personnel</td>
<td>No specific budget, but privacy dollars are spent ad hoc as add-ons to other projects</td>
<td>One person assigned privacy responsibilities serves as the privacy function</td>
<td>Some personnel have knowledge and skills to respond to suspected incidents</td>
<td>At least one person is assigned privacy responsibility, but time commitment exceeds the person’s availability</td>
<td>Policies require acquisition of IT-related products &amp; services address privacy</td>
</tr>
<tr>
<td>2</td>
<td>Personnel review contracts for consistency with privacy policies</td>
<td>Policies require that IT products, services, and system development address privacy</td>
<td>Policies address all privacy principles, and are displayed on relevant websites.</td>
<td>Privacy policies are communicated annually to personnel who encounter PII</td>
<td>Specific budget sufficient to cover basic travel &amp; subscriptions, and modest amount for special projects</td>
<td>Privacy function is identified in org charts, reflecting sustained commitment</td>
<td>Privacy incidents have been effectively resolved, but at most only high-level policy or procedures are documented</td>
<td>At least one person devoted exclusively to privacy, with sufficient staff assistance</td>
<td>Policies require acquisition of IT-related products &amp; services address privacy</td>
</tr>
<tr>
<td>3</td>
<td>Standard contractual clauses are in place, and compliance can be monitored</td>
<td>Policies address all privacy principles, are publicly displayed, and details for implementation are included</td>
<td>Policies address all privacy principles, and are displayed on relevant websites.</td>
<td>Privacy policies are communicated annually to personnel who encounter PII and are provided role-based training</td>
<td>Specific budget that includes enough money to accomplish most privacy objectives</td>
<td>An executive committee member is formally assigned to be privacy champion, and an annual report is presented to board</td>
<td>Personnel have detailed roles and responsibilities, and detailed policies &amp; procedures are maintained</td>
<td>Privacy staff have clearly defined job descriptions that require certification as CIPP, including at least one with a leadership title, and enough staff to meet most privacy objectives</td>
<td>Detailed checklists, procedures, and assigned personnel to ensure all IT-related projects are compliant with privacy policies</td>
</tr>
<tr>
<td>4</td>
<td>Standard privacy &amp; security clauses and internal compliance are measured annually</td>
<td>Compliance with privacy policies of IT products and services are measured and reviewed annually and are updated as needed</td>
<td>Business operations, processes, etc. are reviewed annually and are updated as needed</td>
<td>Personnel comprehension of, and compliance with privacy policies is measured annually</td>
<td>A &quot;Balanced Privacy Scorecard&quot; or other approach used to determine a budget sufficient to cover all objectives</td>
<td>The privacy function is placed in a particular dept to support its strategy, and has direct access to special projects</td>
<td>Suspected incidents are routinely measured &amp; tested for privacy compliance, improvements are made based on this</td>
<td>Privacy staff have clearly defined job descriptions that require certification as CIPP, a Chief Privacy Officer, and enough staff to meet all privacy objectives</td>
<td>Information-related products and services are routinely measured and tested for compliance with privacy policies</td>
</tr>
<tr>
<td>5</td>
<td>Controls in place to prevent adoption of privacy &amp; security commitments that cannot be kept</td>
<td>Controls in place to ensure IT products and services are compliant with policy and procedure</td>
<td>Policies &amp; standards are compared annually to others, and have achieved &quot;best practices&quot; status</td>
<td>Privacy function is exceeded by privacy dollars spent elsewhere in the organization</td>
<td>Privacy function is assessed by privacy dollars spent elsewhere in the organization</td>
<td>The head of the privacy function has direct access to leadership and is a part of business strategy decision-making</td>
<td>All incidents are resolved within 30 days</td>
<td>Privacy objectives are in the job descriptions of all personnel who access PII</td>
<td>Controls in place to prevent new IT-related products and services from being deployed without being compliant with privacy policies</td>
</tr>
</tbody>
</table>
Average Score by Privacy Topic

Infrastructure and Systems Management
Policy Documentation
Privacy Awareness and Training
Risk Assessment
Clients and Partner Contracts
Privacy Incident Management
Privacy Function
Privacy Personnel
Privacy Budget

0 0.5 1 1.5 2 2.5 3
Top 10
8 Local Education Agencies (LEAs)
2 Behavioral Health Facilities

Bottom 10
4 Counties
6 Cities
Government Records Access and Management Act (GRAMA)

- 63G-2-108 **Certification of records officer:** Annual certified Records Officer

- 62G-2-307 Duty to evaluate records and **make designations and classification:** Evaluate, designate, and report record’s series that are used

- 63G-2-601 Rights of individuals on whom data is maintained–Classification statement–Notice to provider of information: Provide **purpose of data collection** to the state archivist, Collection notification
Next Steps

Spring 2022
- Measure privacy maturing of medium and small government entities
- Develop City/Town and County Records Officer Certification Training

Summer 2022
- Train large designated government entities
- Hire additional privacy FTE

Fall 2022
- Legislative Report
- Train at Fall ULCT and UAC conferences
DON’T WAIT!

Certified Records Officer

Certified Information Privacy Manager (CIPM) Training (limited to 10)
- June 21-22    Fall TBD

Security+ training and certification (limited to 10)
- Summer and Fall TBD (5 sessions)
Remember

Don’t Panic

Don’t Wait

Get Help