ENTERPRISE
information services

Cyber Security Services (CSS)

Annual Report on Information Security

May 28, 2021

ENTERPRISE information services

Background: Information Security in Oregon

Since entering office in February 2015, Governor Brown has focused on improving state information security. In 2017, the Legislature approved and Governor Brown signed Senate Bill 90 (SB-90), which transferred information technology security functions to the Office of the State Chief Information Office (OSCIO) now known as Enterprise Information Services (EIS). SB-90 (2017) required state agencies to adhere to the statewide information security program within EIS.

SB-90 (2017) formalized a shift in the state's approach to information security to a whole-of-state government approach based on common priorities, policies, and safeguards. This approach recognizes that the connections among state systems and networks mean that a risk to one agency can create risks for all. In short, a unified information security program is required to manage a shared risk.

Implementing a unified program involves coordinated action by EIS and state agencies. The State CIO, through Cyber Security Services (CSS), manages a risk-based, enterprise security program based on common security policies and standards. State agencies remain responsible for managing their information and systems, for reducing risk exposure and for ensuring agency activities do not introduce undue risk to the enterprise.

Progress Made

Service Catalog

While cyber security has been unified for nearly four years, there ambiguity remained around what agencies are still responsible for executing. As such, the 2019 Legislature requested that CSS create a RACI to address those questions. CSS engaged Gartner to assist in defining the RACI *(Exhibit 1)* and developing the necessary inputs to create a service catalog *(Exhibit 2).*

Exhibit 1

Capability	CSS				DCS	Shared Services	Strategy & Design	Data Governance and Transparency	Agencies
	CISO	GRC*	SOC	Operations					
Program Management (policy)	A, R, C	I	I	I	C, I	C, I	C, I	C, I	C, I
Governance, Risk, Compliance (requirements, guidelines, awareness)	A, C	I	I	I	R, C	R, C	C, I	C, I	A, R, C
Security Architecture (standards)	A, C	I	I	I	R, C	R, C	C, I	C, I	R, C
Infrastructure and Data Protection (includes platforms, applications, data, vulnerability management)	A, C	R	C	R, I	R, C	R, C	C, I	C, I	R, C
Identity and Access Management	A, C	R	C	I	R, C	R, C	C, I	C, I	R, C
Security Operations Center (including incident response and vulnerability assessment)	A*	I	R	C, I	C, I	C, I	I	I	C, I
Security Administration (patching, system admin., change management, operational user provisioning)	C	R	C	R	R, C	R, C	I	I	A, R, C
Systems Integration	C	R	I	C, I	R, C	R, C	C, I	I	A, R, C
Vendor Management	C	R	I	I	R, C	R, C	I	I	A, R, C
Security Consulting	A	R	R	R	R, C	R, C	C, I	C, I	I

ENTERPRISE information services

Exhibit 2

CSS Catalog – Future-state Capabilities and Services*

37 centralized service offerings across 10 primary programmatic capabilities

Program Management
- Security Policy-Setting + Advisory
- Statewide Security Management Plan
- Security Program and Resource Management

Identity and Access Management (IAM)
- Identity Lifecycle Management + Advisory

Governance Risk & Compliance (GRC)
- Working Group(s) Sponsorship
- CISO Roadshow
- Requirements-setting + Advisory
- General Security Awareness Training

Security Administration
- Release Management Requirements + Advisory
- Change Management Requirements + Advisory

Security Architecture
- Standards-setting

Systems Integration
- Secure Technology Transformation Guidance

Vendor Management
- Vendor Contract Review
- Vendor Security Evaluation + Advisory

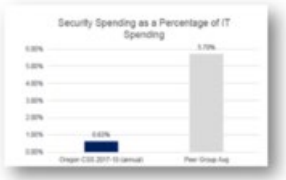
Security Consulting
- Security Risk Assessment
- Business Enablement + Advisory
- Business Case Security Consulting
- SOC Advisory (reference SOC capabilities)
- Configuration and Security Review

Data and Infrastructure and Operations (I&O)
- Endpoint Security Baseline Guidance
- SDLC Process Framework + Advisory
- Data Protection Configuration Guidance
- Network Operations Consulting

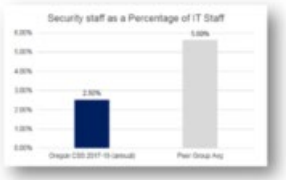
Security Operations Center (SOC)
- NIDS Monitoring
- Firewall Log Monitoring
- Platform Log Monitoring
- Security Advisories
- Incident Recording
- Incident Consulting
- Incident Response
- IT Forensics
- Internal Vulnerability Scanning
- External Vulnerability Scanning
- Penetration Testing
- Threat Hunting
- Red/Blue Teaming

As part of the effort, Gartner also compared Oregon's staffing and spend for security with other states and evaluated the maturity level of Oregon's security program *(Exhibit 3).*

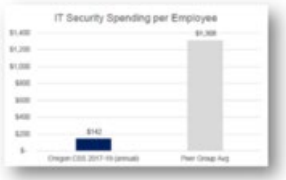
Exhibit 3



- **Security as a % of Overall IT Spending.** *"CSS spending on security operations **[0.63%]** as a percentage of the overall IT budget is **significantly lower** than other State and Local Government Organizations **[5.7%]**"*



- **Security Staff as a % of IT Staff.** *"CSS's proportion of security staff **[2.5%]** as a percentage of total IT employees is **lower** than peers **[5.6%]**"*



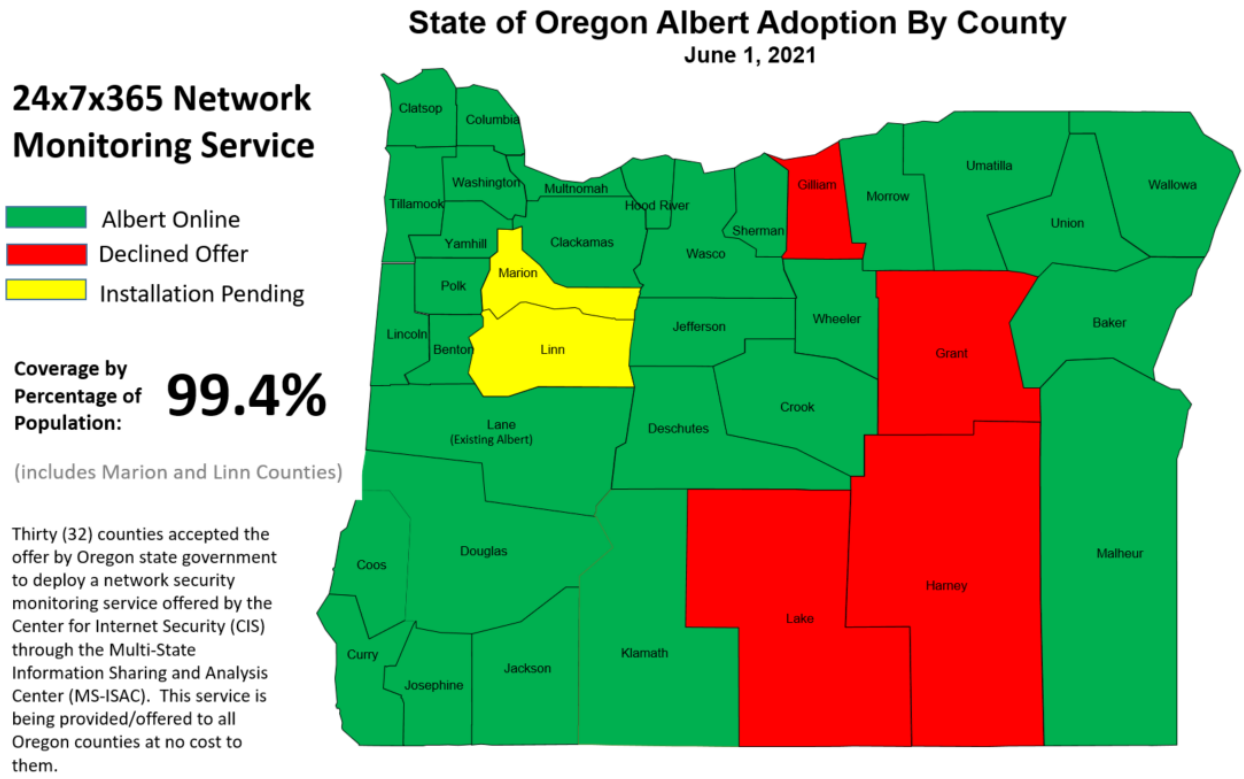
- **Security Spending per Employee.** *"CSS security spending per employee **[$142]** is **significantly lower** than the peer group average **[$1,308]**"*

Developed in partnership with **Gartner; source: Gartner IT Key Metrics Data 2020: IT Security Measures - Analysis*

Albert Sensors

CSS partnered with the Secretary of State to implement intrusion detection at the county level with the use of Albert sensors which are provided by and monitored 24/7 by the Multi-State Information Sharing and Analysis Center (MS-ISAC). Albert is a network security monitoring service offered by the Center for Internet Security (CIS) through the Multi-State Information Sharing and Analysis Center (MS-ISAC). The service is free to the counties with the first year paid for by the Secretary of State and subsequent years paid for by CSS *(Exhibit 4).* The next generation of the Department of Homeland Security's "Einstein Project" Albert identifies malicious or potentially harmful network activity based upon known signatures.

Exhibit 4



With this service, counties can expect to be notified directly by MS-ISAC in less than 6 minutes upon detection of malicious activity on their network. Additionally, the State of Oregon SOC will analyze alerts from all 31 monitored counties and provide threat intelligence, specific to our state, to allow state-wide collaboration in the event of an incident.

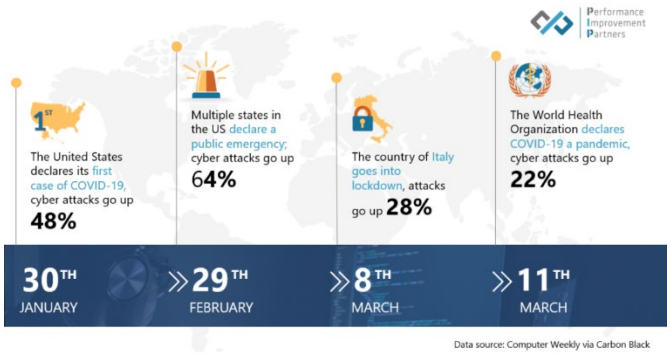
It was critical and necessary to have this implemented prior to the 2020 National elections. Of the 36 Oregon counties, 31 chose to take advantage of this free service and all but two were implemented prior to the election. Those counties have since scheduled their implementations.

Data Breach Mitigation

In an effort to help reduce the likelihood of a data breach due to a phishing email, CSS implemented Malicious Domain Blocking and Reporting (MDBR), a service also provided by MS-ISAC. MDBR technology prevents IT systems from connecting to harmful web domains, helping limit infections related to known malware, ransomware, phishing, and other cyber threats. This capability can block the vast majority of ransomware infections just by preventing the initial outreach to a ransomware delivery domain.

Remote Work Security

During the initial response to the COVID-19 Pandemic, CSS took several steps to improve both the ability of the network to handle the sudden numbers of full-time remote workers and the security of the network - by increasing VPN capacity and requiring multifactor authentication (MFA).



Information Risk Management

The Enterprise Governance, Risk and Compliance Tool, also referred to as Information Risk Management (IRM), is in the process of being procured. Due to a failed procurement the implementation will occur during the 21-23 biennium. This tool will allow CSS and Agencies to record and monitor risks and compliance across the state, making it possible to prioritize security remediation efforts at both the enterprise and agency level.

Intrusion Detection, Threat Prevention and Incident Response

- CSS implemented basic Network Intrusion Detection and Prevention to increase the state's ability to find and address attacks in real time. An intrusion detection system is a device\software application that monitors our network and systems for malicious activity or policy violation. Any intrusion activity or violation is reported to the centralized IBM Qradar security information and event management system (SIEM).
- Compliance Logging (formerly known as Logging Critical Infrastructure) is planned to be implemented by the end of the biennium. This first phase will allow CSS to improve the state's ability to respond to detected incidents and potential threats while addressing several federal regulatory requirements for agencies that use the state data center.
- A complete firewall migration was needed for a variety of reasons but primarily because hardware had reached end-of-life and was not keeping up with evolving security needs.

Detailed planning addressed, current state analysis, vendor and product selection, pre-configuration planning, transition planning and decommissioning of the old hardware.

- Network Threat Detection established the ability to detect anomalous activity on the state network through analysis of network traffic.
- CSS implemented User Behavior Analytics (UBA) for privileged access monitoring at the state data center.
- CSS created an umbrella agreement with Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) for external scanning of state assets facilitating the means by which all agencies can be scanned and also enable a roll-up of all state scanning results.
- CSS Undertook completed several efforts to improve enterprise and agency incident response:
    - Completed a third party Incident Response Readiness Assessment for the state.
    - Updated the State Enterprise Incident Response Plan
    - Created an updated Agency Incident Response (IR) template

Performance Metrics

CSS established and posted new quarterly metrics that are designed to demonstrate the current and ongoing impact of the State of Oregon's unified cyber security approach. These metrics show adoption of key risk-reducing services provided by Cyber Security Service (CSS) along with additional metrics associated with select services.

Maintaining, Modernizing, and Maturing Cybersecurity

While the state has made progress building its cybersecurity capabilities, continued effort and investment is required to establish and maintain an appropriate level of cybersecurity. The state must also ensure compliance with increasingly stringent federal requirements – failure to maintain compliance puts the state at risk of losing access to federal information essential to state business.

Planned Work for 2021-23 Biennium

- As mentioned previously, CSS engaged Gartner for assistance in defining a RACI, developing inputs to create a service catalog, and evaluating our maturity level. As a result of this assessment it became clear that an opportunity exists to improve vulnerability management across the enterprise. Vulnerability Management is more than just patching and most agencies have a very basic, if any, program in place. To help address the need in this area the Governor's Requested Budget includes a Policy Option Package 126, to help CSS and agencies address this need. Included in the POP are CSS positions that will be embedded in seven of the executive branch agencies to assist with creating and documenting vulnerability management programs, in addition to assisting with other cyber security concerns.

- CSS will extend the reach and scope of current vulnerability scanning using a risk-based approach, move to a subscription licensing model, add enhanced vendor support services, and scan for application vulnerabilities—enabling agencies to proactively validate the security of their applications before implementation and/or after major code changes (i.e., "secure by design").
- At the request of the National Governors Association, CSS will continue to work on the Statewide Cyber Disruption Plan over the next year, recognizing that the Pandemic impacted the state's ability to complete this effort.
- In an effort to proactively identify gaps in service, CSS will continue to work on the Service Catalog, aligning the services with the CIS v 7.1 controls and the Statewide Security Plan and Statewide Security Standards (2019) References.
- CSS will continue to mature the Quarterly Security Metrics to ensure a clear picture of the key risk-reducing services and their impact on the overall state of risk for Oregon. To maintain transparency and accountability, CSS will continue to publish metrics on the CSS website.
- Network and Security Modernization Program (NSMP) is the program to modernize the State of Oregon network and associated enterprise network and security services to provide a reliable, secure and scalable foundation in support of business functions for all state agencies. CSS has a major role in this program and will continue to participate heavily next biennium.
- Microsoft 365 is actually two projects. The first, MVP (Minimum Viable Products) is currently underway and is partially staffed by CSS. The second is expected to kick off in the 21-23 biennium and will be focused on service enhancements including multiple *projects and other work efforts to expand the enterprise services and deliver the associated business capabilities and security enhancements. Several components of this project will be security focused - Identity and Access Management (IAM) for the enterprise, MFA (full enterprise service), Microsoft Endpoint Management (MEM), Defender for Endpoint, Cloud Application Security, Privileged Identity Management, Microsoft Information Protection including Unified Labeling, Rights Management and Data Loss Prevention (DLP), Identity Governance and Administration.
- Integrated Risk Management (IRM) is a project from the 19-21 biennium that will continue into the 21-23 biennium when the tool will be configured and implemented for EIS. The use of the tool will be expanded to some agencies as time and resources allow. This tool is necessary for the CSS risk team to record and monitor risks and compliance across the state, drive the security risk governance process, and properly prioritize security remediation efforts.