OREGON | Office of the State

Chief Information Officer

Enterprise IT Security Update

August 2018

OREGON
Enterprise Security Office

Enterprise IT Security Update

Senate Bill 90 Update

- Unified IT Security Strategy & Execution
- Oregon Cybersecurity Advisory Council
- Oregon Cybersecurity Center for Excellence

Unified Strategy

Unify *– Know Our Environment – Master the Basics – Build Culture –* ***Govern by Risk***

MISSION

Lead Oregon in safeguarding the State's information resources

VISION

A unified approach to cybersecurity that improves customer service for Oregonians while ensuring systems and data are secure, resilient and ready for the future

STRATEGIC PILLARS

Open, Empowered Culture of Security

Proactive, Holistic Risk Management

Resilient IT Infrastructure

Rapid Detection, Response & Recovery

IMPERATIVES

- Raise employee awareness
- Increase security expertise
- Build in the basics

- Know our IT ecosystem
- Understand weaknesses
- Govern by risk

- Harden & maintain security architecture
- Foster enterprise standards
- Protect the user & perimeter

- Consistent logging & monitoring
- Unified expert-level security response
- Reduce & shorten events

Revised: 09 July 2018

OREGON Enterprise Security Office

Strategic Objectives

*2017-19 Enterprise Security "**Big 3**" objectives*

Unify IT security

- Unified security team & program that enables state business

Establish security risk management & governance

- Security risk program & IT lifecycle aligned with business leadership & enterprise IT governance

Implement security basics at all agencies

- Drive highest priority security controls at all agencies

OREGON
Enterprise Security Office

Roadmap & Execution

2017-19 Biennium

2017

Form new ESO, Ops review, Start on governance

- ✓ Positions (35) moved by HR to DAS/ESO
- ✓ All existing staff (15) moved to new roles in ESO
- ✓ Vacancies prepared for recruitment
- ✓ Deputy CISO hired
- ✓ Security risk governance foundation defined

2018

Establish shared services, publish enterprise plan, staff team

- ✓ ESO shared security services catalog
- ✓ Published plan for unified execution
- ✓ Agency minimum security requirements
- ✓ Comprehensive unified enterprise security plan
- ✓ System security requirements for IT governance/stage gate
- ✓ Key vacancies filled (10)

Rule & Policy updates, metrics & reporting, 5-year planning

- Refresh security policy
- IT security rule making (update of OAR 125-800)
- Publish quarterly report cards
- Initiate 5-year planning
- Establish enterprise security board under ELT/EITG
- Vacancies filled (9), remaining to fill (4)

2019

Evaluate, course correct as needed, 2019-21 planning

- Independent review of enterprise security program against best practice
- Independent technical security assessment of State network
- Survey agency leaders on program quality & effectiveness
- Establish 2019-21 objectives
- Publish 5-year plan

OREGON
Enterprise Security Office

Results

Delivered results since passage of SB90

Unify IT security

- Annual enterprise security training completed (September 2017)
- **Unified security team** established (January 2018)
- **Unified security services** defined & published (June 2018)
- **Enterprise 5-year plan** working group chartered (August 2018)
- ESO staffed to **90% of headcount** (September 2018)
- Annual enterprise security training deployed (July 2018)
- Quarterly **security scorecard** established (September 2018)

OREGON
Enterprise Security Office

Accountability

Quarterly Enterprise Security Score Card

First score card will be delivered in September 2018

Unification	40	↑
Maturity	44	-
Risk	75	↓
Operations Effectiveness	58	↑
Culture	75	-

Top Risks

1. *Theft & abuse of user passwords through social engineering (phishing)*
2. *Data theft through application vulnerabilities in older applications*
3. *Data breach through user action (deliberate & accidental)*

Significant Security Events

State email reputation loss due to compromised email accounts (phishing)

Impact: lost ability to deliver email to some citizens, mentioned in press

Resolution: restored ability to deliver email, trained staff on phishing, investigating technical solutions

Results

Delivered results *since passage of SB90*

Establish security risk management & governance

- Enterprise security **risk policy** drafted (December 2017)
- Internal risk assessment calendar established (June 2018)
- **Cloud security standards** drafted (July 2018)
- **Unified Enterprise Security Plan** published (August 2018)
- System security plan expectations published (August 2018)
- **Enterprise Information Security Board** charter draft (August 2018)
- External Assessment – State Network (start late 2018)
- External Assessment – Unified Security Program (start early 2019)

Results

Delivered results *since passage of SB90*

Implement IT security basics at all agencies

- Network encryption hardware brought current (October 2017)
- **Malicious Helpdesk** for all agencies established (June 2018)
- Agency **top security priorities** published (June 2018)
- Program to address agency top security priorities set (July 2018)
- **Breach protocol** for all agencies established (July 2018)
- First agency move to centralized detection service (August 2018)
- **Unified agency security planning** initiated (August 2018)
- Central network security services documented & technical standards published (August 2018)

OREGON
Enterprise Security Office

Results

*First unified security service = **more resilient IT infrastructure***

Vulnerability Management

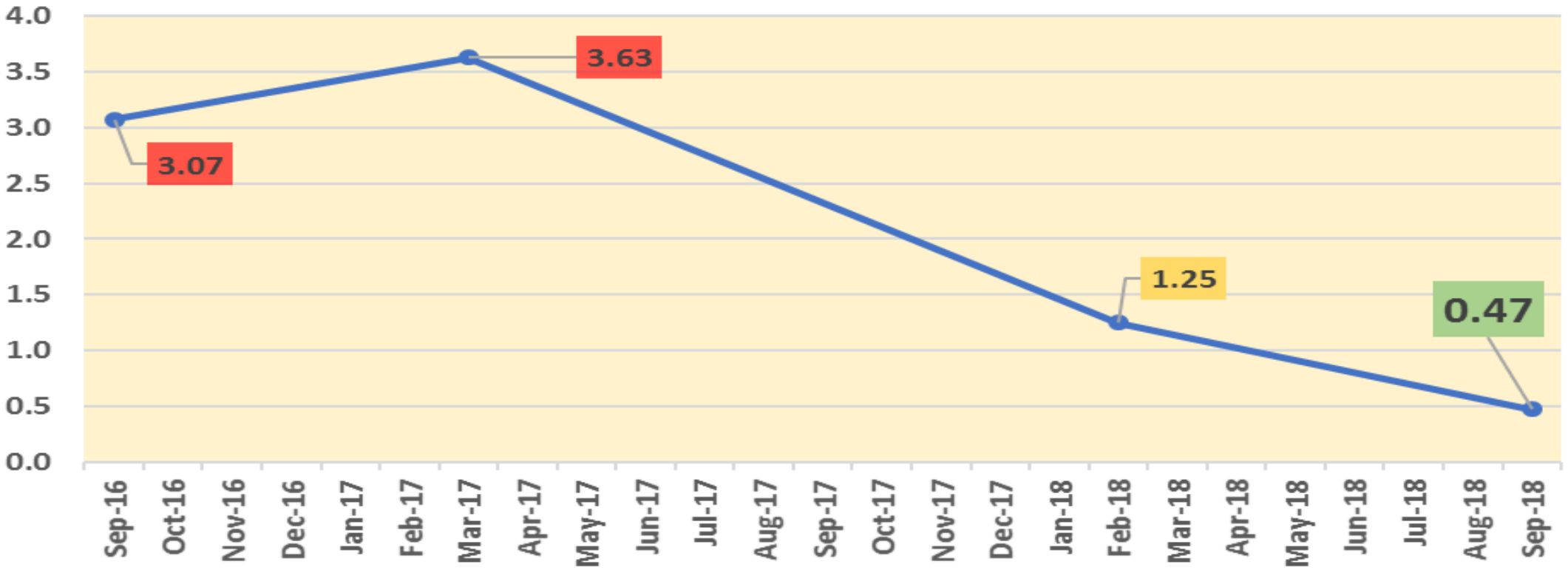
Unified service to regularly scan & report agency vulnerabilities, then partner with agency IT to drive remediation.

Metric	Feb 2018	Today
Agency participation	39	39
Systems scanned	56,000	57,000
Severe vulnerabilities per system	1.25	0.47
Agencies meeting vulnerability targets	13	18

Risk Reduction

*First unified security service + agency partnership = **steady risk reduction***

***Vulnerability Management** – measurable enterprise risk remediation*

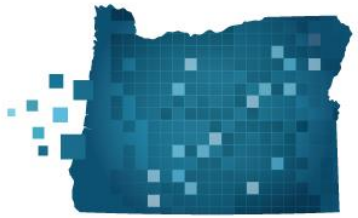


Reduced critical vulnerabilities in IT infrastructure by over 80%!

OREGON
Enterprise Security Office

Statewide Security Leadership

Oregon Cybersecurity Advisory Council (OCAC)



CYBEROREGON

Broad Inclusion

- **Wide, active community**
  - Overwhelming volunteer support from local security practioners
  - Active participation from education (higher ed. & K-12), local government, private sector, law enforcement, & military
- Workgroups focusing on education, workforce development, technology, information sharing & public outreach

Public Engagement

- **Six major community events** across Oregon in 2018
- **Five high school** NW Cyber Camps across Oregon in 2018
- CyberOregon website: **800-850 visitors/month** & growing

OREGON Enterprise Security Office

Statewide Security Leadership

Oregon Cybersecurity Center for Excellence (CCoE)

Center Research

- Top ask from across Oregon:
  - **Cybersecurity workforce development**
- Consistent interest & need for services of a Center for Excellence:
  - **Training, information sharing, risk assessment, & detection/response services**
- Current research: detailed build-out plans from other states to support Oregon CCoE proposals

Center Plan

- **Detailed written plan for Oregon CCoE** in progress (complete in Dec 2018)
- OCAC proposals being finalized for potential policy options (complete in Sept 2018)
- Legislative Concept (LC 550) submitted for 2019 session

OREGON Enterprise Security Office

OREGON | Office of the State

Chief Information Officer

Enterprise IT Security Update

August 2018

OREGON
Enterprise Security Office