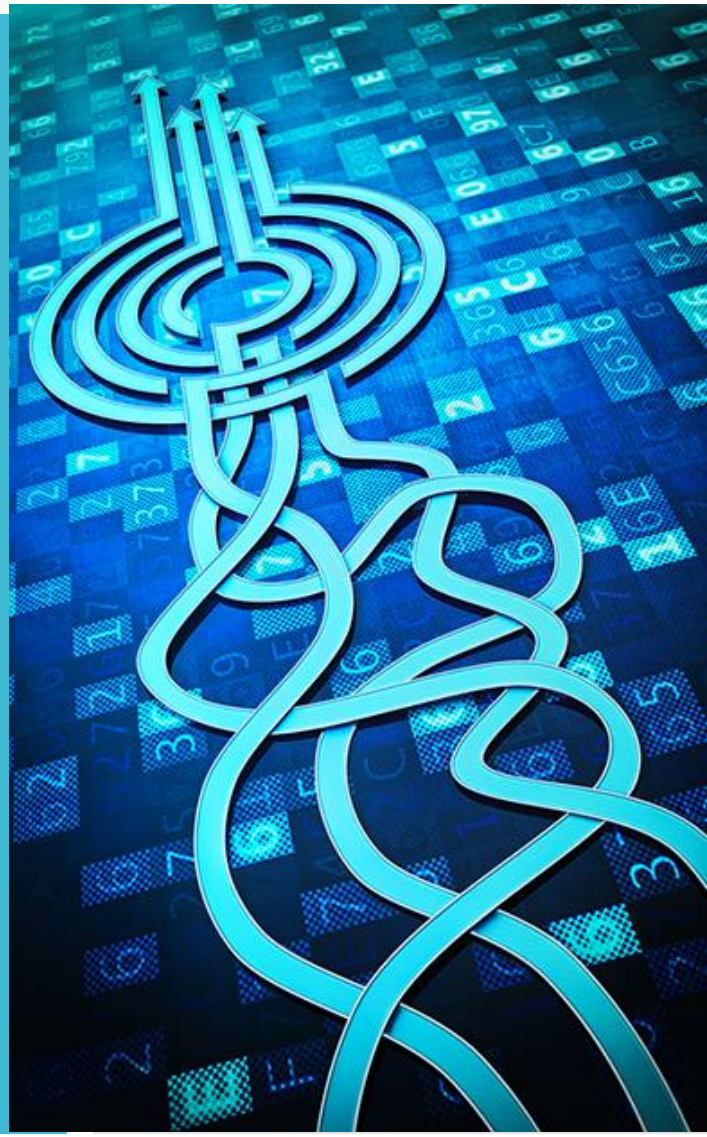
Oregon Summit Cyber

Theresa Masse

US Department of Homeland Security -Cybersecurity and Infrastructure Security Agency (CISA)

Cinnamon Albin

State of Oregon – Cyber Security Services (CSS), Enterprise Information Services



All Hazards Approach

- Cyber is **not** just an IT/Security issue – it's a *Risk* issue
- People, Process, and Technology
- Interdependency:
  - Infrastructure
  - Communications
  - Third Parties (Vendors/Business Partners)
  - Supply Chain

Current State

- Automation
  - Systems
    - Cloud
    - On-Prem
    - Hybrid
- Mix of legacy and new systems and equipment
- Mobile devices - provide immediate access to sensitive information from any location.
  - Corporate
  - Personal

Prepare

- Build Relationships – People
  - Business Leadership
  - CIO/IT Manager
  - Emergency Manager
- Coordination - Process
  - Define Roles and responsibilities
  - Train
  - Exercise
- Test Systems – Technology
- See something, say something
- Insider Threats

Best Practices Checklist

- ❑ Install software to scan for viruses/malware/vulnerabilities*
- ❑ Install Web application scanning*
- ❑ Segment systems and implement encryption
- ❑ Install strong spam filters to prevent phishing emails from reaching end users

Best Practices Checklist

- ❑ Conduct Security Awareness training on a regular basis for all staff & management
- ❑ Conduct Phishing exercises on a regular basis -review metrics*
- ❑ Conduct Remote Pen Testing*
- ❑ Conduct Risk & Vulnerability Assessments*
- ❑ Don’t allow users administrator access

Best Practices Checklist

- ❑ Create a cyber incident response plan and exercise it regularly*
- ❑ Schedule regular assessments*
- ❑ Due diligence on third parties & vendors and regularly review access*
- ❑ Develop an Information Security Strategic Plan and Architecture
- ❑ Develop and implement Information Security Policies

Best Practices Checklist

- ❑ Implement patches as soon as possible
- ❑ Keep software and operating systems up to date
- ❑ Implement multi-factor authentication
- ❑ Evaluate cyber security insurance

Best Practices Checklist

- ❑ Limit access to resources over networks
  - Restrict Remote Desktop Protocol (RDP) to only those administrators and devices that require that access.
  - Restrict or block Server Message Block (SMB) to those systems that require that protocol. If it is not used or required, block it.
- ❑ Set antivirus/antimalware programs to conduct regular scans
- ❑ Risk-based asset inventory
  - Establish an extensive and complete asset inventory of all resources in IT and OT . Prioritize the assets based on risks and the cost to replace, and the data /information on them.

Best Practices Checklist

- ❑ Prevent unauthorized application execution
  - Disable macro scripts in Office products
  - Implement application allow-listing
- ❑ Monitor and/or block inbound connections
  - Analyze all inbound connections to determine if they meet pre-determined criteria. Some businesses block all inbound connections and allow by exception.

Best Practices Checklist

- ❑ Establish a robust backup program
  - Include 3 things:
    - Frequent backups (full and incremental)
    - Proven method of backing up (E.g. 3-2-1 Method – 3 copies, 2 different media onsite, and one copy offsite)
    - Tested by recovering from backups on a set schedule

CISA Cyber Services

(all offered at *no charge*)

- Vulnerability & Web Application Scanning
- Phishing Exercise
- Remote Pen Testing
- Risk & Vulnerability Assessment
- Malware Analysis
- Various cyber assessments – virtual/onsite or self-assessments
- Cyber Table-Top Exercise
- Lots of other CISA resources at https://www.cisa.gov

State Offering

Oregon Cooperative Procurement Program (ORCPP)

Inter-governmental agreement with partnering entities to provide members with access to:

- Statewide price agreements to purchase goods and services
- Unlimited advertising in the OregonBuys eProcurement System
- Archived solicitations, to help you build new solicitations
- Training opportunities through DAS
- State of Washington Contracts – (Entities must determine whether these contracts meet their own purchasing rules and ORS 279 requirements)
- ORCPP Link - keep you connected with emails concerning trainings, updates to price agreements, specials from DAS Surplus and other resources

State Offering

Oregon Cooperative Procurement Program (ORCPP)

Eligible entities include:

- Local government - cities, counties, school districts, etc.
- Special districts - fire, water, vector control, health, etc.
- Oregon university and community colleges
- Qualified rehabilitation facilities
- American Indian tribes and agencies of American Indian tribes
- Certain qualifying, public benefit corporations
- State agencies

Visit: www.oregon.gov/das/Procurement/Pages/Orcpp.aspx

State Offerings

Basecamp

Brokers high value IT statewide price agreements. Focused on creating win-win relationships for government partners and vendors.

- Government Partner Engagement
- Strategic Sourcing
- IT Catalog
- Vendor Performance Management
- Vendor Relationship Management

Visit: Oregon.gov/basecamp

Community Offering

Cyber Disruption Response and Recovery (CDR) – Voluntary Resource Guide

Provides a common framework for responding to cyber threats impacting Oregon government and enables all levels of Oregon government to rapidly coordinate a cyber disruption response, minimizing the impact in Oregon.

- Whole of Government approach
- Community Driven
- Common Framework
- Voluntary
- Leverage resources
- Communications
- Education

Visit: Security.Oregon.gov

CDR - Resources and Services

Service	State		Federal		Dual Role	
	Cyber Security Services (CSS)	Office of Emergency Manage-ment (OEM)	Cybersecurity Infrastructure Security Agency (CISA)	Multi State-Information Sharing & Analysis Center (MSISAC)	Oregon Titan Fusion Center	Oregon National Guard
Proactive						
Advisories/Threat Notification	✓	✓	✓	✓	✓	
CIS SecureSuite Membership				✓		
Consulting				✓		
Continuity Planning						✓
Cyber Assessments			✓			✓
Cyber Exercise Planning			✓			✓
Cyber Training/Education Resources	✓		✓	✓		
Cyber Vendor Contracts						
Malicious Domain Bloacking				✓		
Managed Security Services				✓		
Network Monitoring				✓		
Penetration Testing			✓			✓
Phishing Campaign Assessments			✓			
Risk & Vulnerability Assessment			✓			
Validated Architecture Design			✓			
Vulnerability Scanning			✓	✓		
Web Application Scanning			✓			
Alerts	✓		✓	✓	✓	
Emergency Declaration		✓				
Incident Response Assistance	✓		✓	✓		
Malicious Code Analysis Platform				✓		
Malware Analysis			✓	✓		
Vulnerability Assessment				✓		
Vulnerability Management Program				✓		

Recommend

- Join an ISAC - www.nationalisacs.org :

  Member-driven organizations, delivering all-hazards threat and mitigation information to asset owners and operators.

- DOTGOV - https://home.dotgov.gov/ :

  Available *solely* to U.S.-based government organizations and publicly controlled entities.

- Cyber awareness - www.stopthinkconnect.org :

  Global online safety awareness campaign. October is National Cyber Security Awareness Month.

Cyber Resources

- Cybersecurity and Infrastructure Security Agency (CISA)
  - https://www.cisa.gov
- Cyber Security Services (CSS), Enterprise Information Services
  - Oregon's Executive Branch cyber leader
  - Oregon Cyber Disruption Response and Recovery
  - Security.Oregon.gov

Contact

Theresa Masse

US Department of Homeland Security, Cybersecurity and Infrastructure Security Agency (CISA)

Email: theresa.masse@cisa.dhs.gov

Web: www.CISA.gov

Cinnamon Albin

Cyber Security Services (CSS), Enterprise Information Services

Email: cinnamon.s.albin@oregon.gov

Web: https://security.oregon.gov