Cyber Strategy

Cyber is **not** just an IT issue

People, Process, and Technology

Interdependency

- Infrastructure
- Communications
- Third Parties (Vendors/Business Partners)
Cyber Strategy

• People - Build Relationships

• Process
  • Formalize Cyber Security
  • Define Roles/Responsibilities
  • Train
  • Exercise

• Technology - Test Systems
Cybersecurity Overview & Industry Trends

2023 Global Cyber Status Report
Malicious activity Experienced in the last 24 months.
Ransomware

21 DAYS
Average downtime due to ransomware attacks² (Coveware)

287 DAYS
Average days it takes a business to fully recover from an attack³ (Emsisoft)

$350 MILLION
Victims paid in ransom in 2020 — a 311% increase over the prior year⁴ (Chainalysis)

$312,493
The average payment in 2020 — a 171% increase compared to 2019⁵ (Palo Alto Networks)

In 2020, nearly 2,400 U.S.-based governments, healthcare facilities, and schools were victims of ransomware

Source: Institute for Security and Technology
PROTECT AGAINST RANSOMWARE

- Maintain offline backups.
- Automate software patching and updates.
- Learn how to identify phishing emails.
- Use multi-factor authentication.
- Ensure antivirus/antimalware software is up to date.

Learn more: CISA.gov/ransomware
Take Action

IF YOU EXPERIENCE AN ATTACK

- Identify and isolate affected systems.
- Only if you are unable to disconnect devices from the network, power them down to avoid further spread of the ransomware infection.
- Triage impacted systems for restoration and recovery.
- Notify the FBI/U.S. Secret Service and CISA.
- CISA does not recommend paying ransom since there is not any guarantee cybercriminals will restore your data.

Learn more: CISA.gov/ransomware
Implement most impactful security measures:

**FIRST**
1. Implement multifactor authentication (MFA)
2. Prioritize patch management
3. Perform and test backups
4. Minimize exposure to common attacks
5. Develop and exercise a cyber incident response plan
6. Create a training and awareness campaign at all levels

**SECOND**
- Prioritize further near-term investments in alignment with the full list of GSA's Cybersecurity Performance Goals (CPGs)

**THIRD**
- Develop a unique cybersecurity plan that leverages the NIST Cybersecurity Framework (CSF)
<table>
<thead>
<tr>
<th>Service</th>
<th>State</th>
<th>Federal</th>
<th>Dual Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proactive</td>
<td>Office of Emergency Management (OEM)</td>
<td>Multistate Information Sharing &amp; Analysis Center (MSISAC)</td>
<td>Oregon National Guard</td>
</tr>
<tr>
<td>Advisories/Threat Notification</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
</tr>
<tr>
<td>CIS SecureSuite Membership Consulting</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
</tr>
<tr>
<td>Continuity Planning</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
</tr>
<tr>
<td>Cyber Assessments</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
</tr>
<tr>
<td>Cyber Exercise Planning</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
</tr>
<tr>
<td>Cyber Training/Education Resources</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
</tr>
<tr>
<td>Cyber Vendor Contracts</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
</tr>
<tr>
<td>Malicious Domain Blocking</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
</tr>
<tr>
<td>Managed Security Services</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
</tr>
<tr>
<td>Network Monitoring</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
</tr>
<tr>
<td>Penetration Testing</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
</tr>
<tr>
<td>Phishing Campaign Assessments</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
</tr>
<tr>
<td>Risk &amp; Vulnerability Assessment</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
</tr>
<tr>
<td>Validated Architecture Design</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
</tr>
<tr>
<td>Vulnerability Scanning</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
</tr>
<tr>
<td>Web Application Scanning</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
</tr>
<tr>
<td>Reactive</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Alerts</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
</tr>
<tr>
<td>Emergency Declaration</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
</tr>
<tr>
<td>Incident Response Assistance</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
</tr>
<tr>
<td>Malicious Code Analysis Platform</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
</tr>
<tr>
<td>Malware Analysis</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
</tr>
<tr>
<td>Vulnerability Assessment</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
</tr>
<tr>
<td>Vulnerability Management Program</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
</tr>
</tbody>
</table>
Cyber Disruption Response and Recovery Plan

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

security.oregon.gov/cyberdisruption
# CISA Cyber Services

(all offered at no charge)

<table>
<thead>
<tr>
<th>Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vulnerability &amp; Web Application Scanning</td>
</tr>
<tr>
<td>Phishing Exercise</td>
</tr>
<tr>
<td>Remote Pen Testing</td>
</tr>
<tr>
<td>Risk &amp; Vulnerability Assessment</td>
</tr>
<tr>
<td>Malware Analysis</td>
</tr>
<tr>
<td>Various cyber assessments – virtual/onsite or self-assessments</td>
</tr>
<tr>
<td>Cyber Table-Top Exercise</td>
</tr>
</tbody>
</table>

Lots of other CISA resources at [https://www.cisa.gov](https://www.cisa.gov)
Funding – State and Local Cyber Grant Program

Who is eligible to apply:

The State Administrative Agency (SAA)’s for states and territories are the only eligible applicants. In addition, two or more eligible entities may apply jointly for assistance as a multi-entity group. Under SLCGP, that means two or more SAAs may apply for joint projects, but they still must submit separate applications.

Role of the SAA:

The SAA is responsible for managing the grant application and award. Working with the Cybersecurity Planning Committee, the SAA must ensure at least 80% of the federal funds awarded under the SLCGP are passed-through to local entities. Leaving 20% for state entities. In addition, at least 25% of the total funds made available under the grant must be passed through to rural communities.
First Year:

In the first year, the focus is on establishing a strong foundation on which to build a sustainable cybersecurity program. Initial priorities include the following, all of which are statutory conditions for receiving a grant:

- Establish a Cybersecurity Planning Committee that can lead entity-wide efforts.
- Develop a Cybersecurity Plan that addresses the entire jurisdiction and incorporates cybersecurity best practices.
- Conduct assessments and evaluations to identify gaps that can be mitigated by individual projects throughout the life of the grant program.

- SLCGP_INFO@DAS.OREGON.GOV
SLCGP Cybersecurity Plan

- Statewide Cybersecurity Plan Template and the plan development effort estimate.

- 16 Key Elements must be on the plan.
Cyber Security Services Catalog Approach

Tier 1: Basic Cyber Hygiene
- Security awareness training program that includes phishing service
- Centralized cybersecurity workforce development – Online training services

Tier 2: Tactical
- MFA implementation assistance program
- Patch management
- Tenable scans service

Tier 3: Strategic
- Cybersecurity Strategic planning assistance
- Security assessment of government information assets in Oregon
Contact

Sherri Yoakum
Cyber Security Services (CSS), Enterprise Information Services
Email: sherri.m.yoakum@das.Oregon.gov

Mariah O’Seanecy
Cyber Security Services (CSS), Enterprise Information Services
Email: mariah.oseanecy@das.Oregon.gov
Thank you