



OREGON
STATE
TREASURY

OREGON STATE TREASURER ELIZABETH STEINER

INFORMATION SECURITY OVERVIEW

Joint Legislative Committee
On Information Management
And Technology



MISSION AND VISION

Treasury Mission

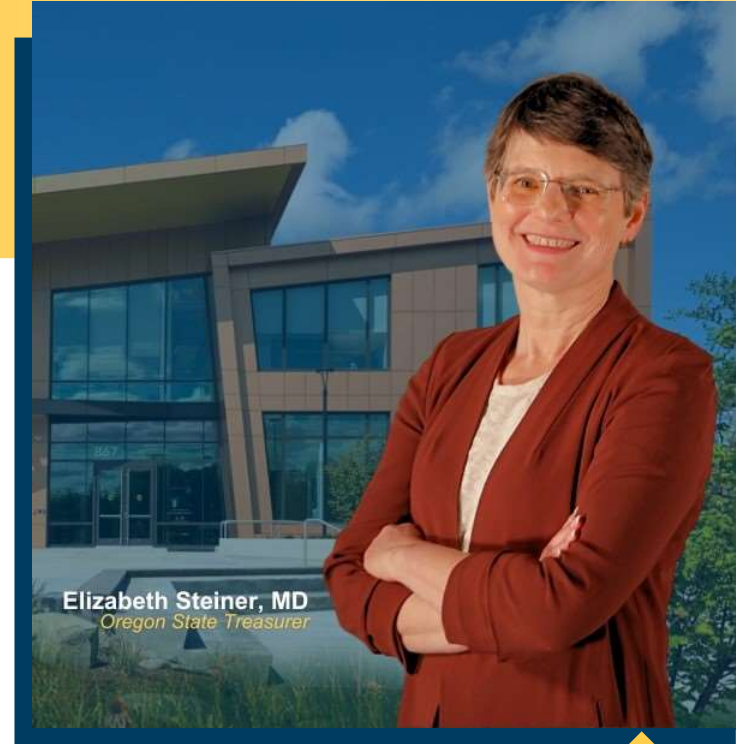
To Provide Financial Stewardship For Oregon.

Treasury Vision

Leading The Way For Oregonians To Achieve Long-Term Financial Security.

Information Technology (IT) Mission

Improving Oregon Governments' And Citizens' Financial Capabilities Through Collaborative, Resilient, Innovative, And Secure Technology Solutions.





OREGON
STATE
TREASURY

INFORMATION SECURITY OVERVIEW

TREASURY'S CYBER SECURITY PROFILE



Provide Resilient Enterprise Infrastructure And Expertise Needed To Conduct Business Securely And Reliably

TREASURY 2024 OPERATIONAL SNAPSHOT



Issued \$5.2 Billion In State & Local Debt To Support Oregon Communities



\$140 Billion Investment Assets Managed On Behalf Of Public Employees, Governments, & Public Universities



18.4 Million Banking Transactions Processed Totaling \$419 Billion



OREGON
STATE
TREASURY

INFORMATION SECURITY OVERVIEW

CYBER ATTACKS IN THE FINANCIAL SERVICES INDUSTRY

The Financial Industry Is 300 Times More Likely To Face An Attack

- The Cost Of A Data Breach In The United States Averaged 9.36 Million USD In 2024
- The Average Time To Contain A Data Breach Was 64 Days In 2024

The Effect: More Money Is Being Dedicated Within The Financial Industry To Address And Contain Cyber Attacks

*2024 IBM Security- Cost Of A Data Breach Report 2024



Top Threats To Financial Services Organizations

Phishing

Denial of Service DDoS

Ransomware

Malware Spam

Smishing

**2025 FS-ISAC- Annual Threat Trend Report*



**OREGON
STATE
TREASURY**

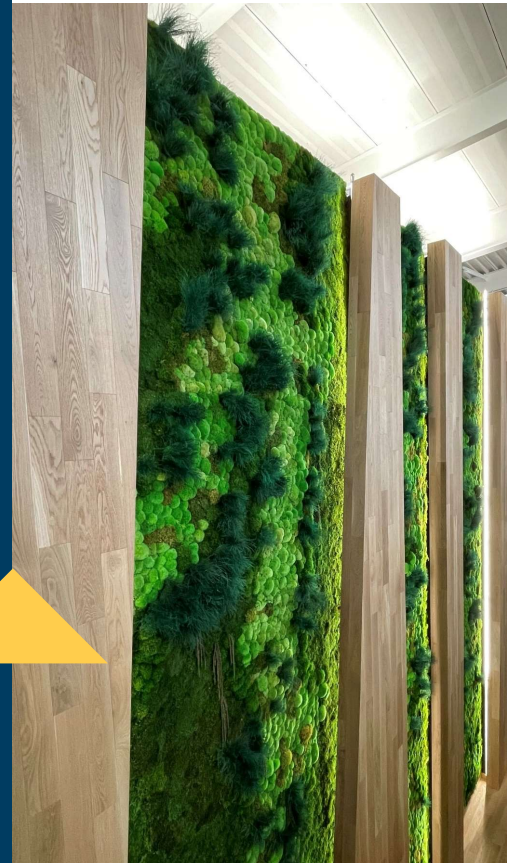


OREGON
STATE
TREASURY

INFORMATION SECURITY OVERVIEW

BIGGEST IMPACTS OF CYBER EVENTS

- Financial Loss
- Data Theft/ Data Leak
- Customer Trust And Reputational Damage
- Disruption Of Operations
- Regulatory And Legal Consequences
- Increased Cybersecurity Costs





OREGON
STATE
TREASURY

INFORMATION SECURITY OVERVIEW

INFORMATION SECURITY PROGRAM OVERVIEW

Frameworks: NIST Cybersecurity Framework, NIST 800-53 Rev. 5, OR Statewide Information Technology (IT) Control Standards (2024), & OR Statewide Information Security Plan (2023)

Security Operations Center

Event Monitoring

Incident Response

IT Disaster Recovery

Metrics Effectiveness

Architecture & Engineering

Security Strategy

Project Consulting

New Product Reviews

IT Escalation

Zero Trust

Threat & Vulnerability Mgmt.

Vulnerability Management

Security Configuration
Management

Application Security

Access Management

Endpoint Protection

Risk & Compliance

Policy Management

Risk Management

NIST Compliance

Security Governance

Regulatory Inquiries

Vendor Risk
Management



OREGON
STATE
TREASURY

INFORMATION SECURITY OVERVIEW

CYBERSECURITY KEY OBJECTIVES

Objective

Description

Govern

Develop Cybersecurity Risk Management Strategy, Expectations, And Policy Are Established, Communicated, And Monitored.

Identify

Develop Organizational Understanding To Manage Cybersecurity Risks To Systems, Assets, Data, And Capabilities.

Protect

Develop And Implement Appropriate Safeguards To Ensure The Protection Of Oregon State Treasury Assets.

Detect

Develop And Implement The Appropriate Activities To Identify The Occurrence Of A Cybersecurity Event.

Respond

Develop And Implement The Appropriate Activities To Take Action Regarding A Detected Cybersecurity Events.

Recover

Develop And Implement The Appropriate Activities To Maintain Plans For Resilience And To Restore Any Capabilities Or Services That Were Impaired Due To A Cybersecurity Event.



OREGON
STATE
TREASURY

INFORMATION SECURITY OVERVIEW

CYBERSECURITY ROADMAP

2025

2026

GOVERN

- Align Security Program And Policies With NIST CSF
- Enhance GRC Platform

Update Policies

Enhance GRC Platform

Improve Data Governance Program

IDENTIFY

- Ensure Current Cybersecurity Risks Are Understood
- Third-party Risk Assessment

Improve Asset Management

Third-Party Risk Assessment

PROTECT

- Application Security And Enhancements To Network Security
- MFA Upgrade

Network Security Upgrades

Automate Security In DevOps Pipelines

MFA Upgrades

IAM/PAM Upgrades

Set Performance Goals

Measure Performance

DETECT

- Improve Monitoring
- Integrate SecOps With ITSM
- Copilot For Security

Improve Monitoring

Enhance SecOps With AI & Automation

RESPOND

- Improve The Incident Response Plan
- Tabletop Exercise

Update Response Playbooks

Test Incident Response Plan

RECOVER

- Update The Business Continuity Plan

Conduct Business Impact Analysis

Design Plan To Address Gaps

Test DR Plan



OREGON
STATE
TREASURY

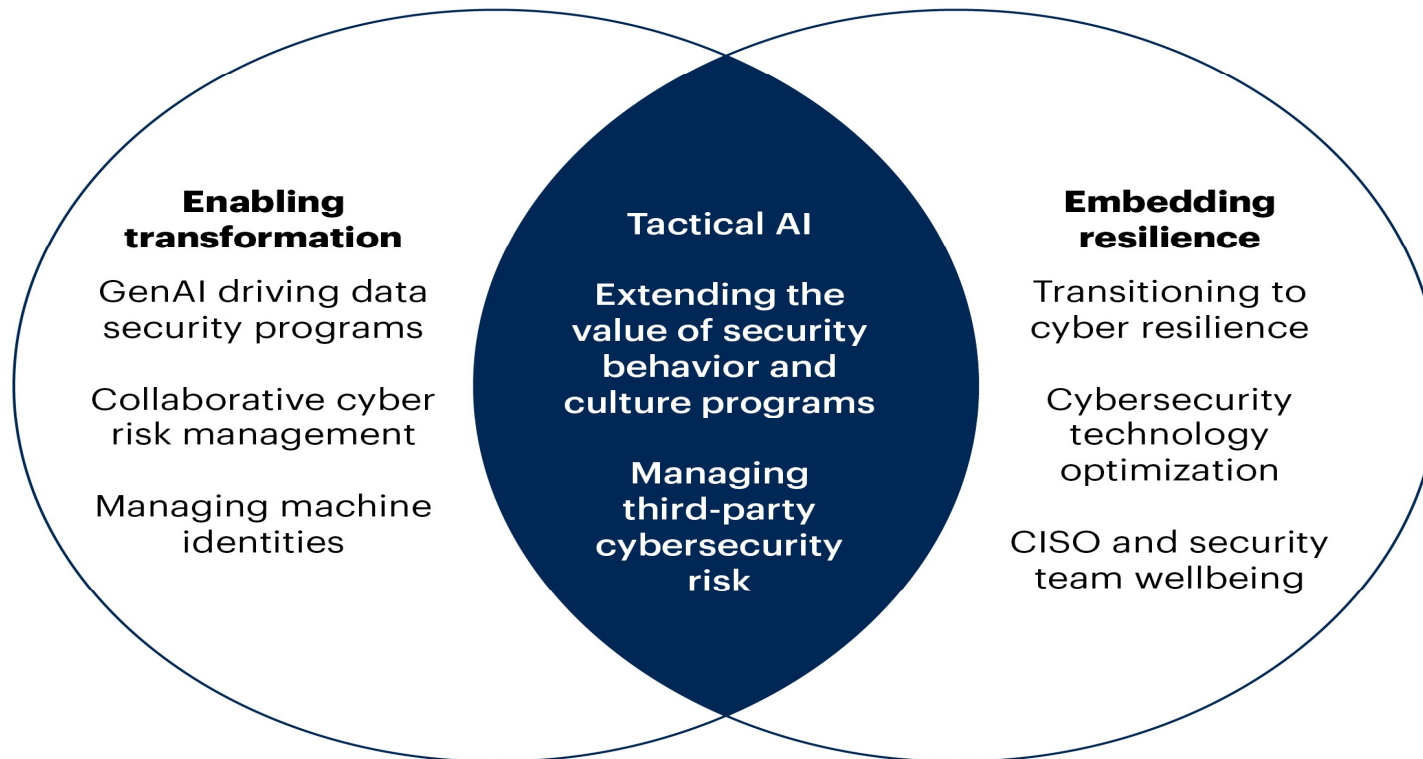
INFORMATION SECURITY OVERVIEW

INFORMATION SECURITY INVESTMENTS



- 24x7 Incident Detections & Response
- Enhance Security Operations With AI And Automation
- Cyber Resilience & Business Continuity
 - Automated Security Integration In DevOps Pipelines
 - MFA Enhancements
- Cloud Security
- Information Security Research And Advisory Services
- Transitioned From A Traditional SIEM To An Extended Detection And Response Platform

Top Trends in Cybersecurity for 2025



Source: Gartner
822766_C



OREGON
STATE
TREASURY

INFORMATION SECURITY OVERVIEW

RECENT ACTIVITIES



Security Assessments

- SoS Cybersecurity Audit Updates (2024)
- Comprehensive Penetration Test (2023)
- Security Program Gap Assessment (2024)



Staff Training

- New Hire Orientation
- Annual Security Awareness Training
- Monthly Security Tips
- Simulated Phishing Test



OREGON
STATE
TREASURY

INFORMATION SECURITY OVERVIEW

SECURITY COLLABORATIONS



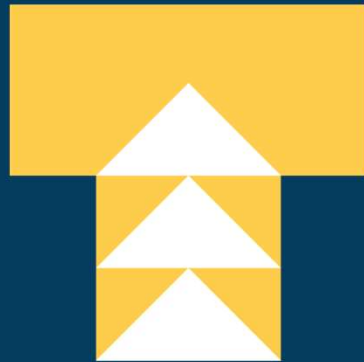
- EIS-Cyber Security Services
- Oregon DOJ Cyber Work Group
- Info-Tech Consultation
- Gartner Consultation
- Multi-State Information Sharing And Analysis Center
- Financial Services – Information Sharing And Analysis Center

INFOSEC STAFF TRAINING

- Cyber Security Conferences
- Cyber Security Webinars
- Security Bootcamps & Certifications
- Information Security Community



Information Security Report



**OREGON
STATE
TREASURY**