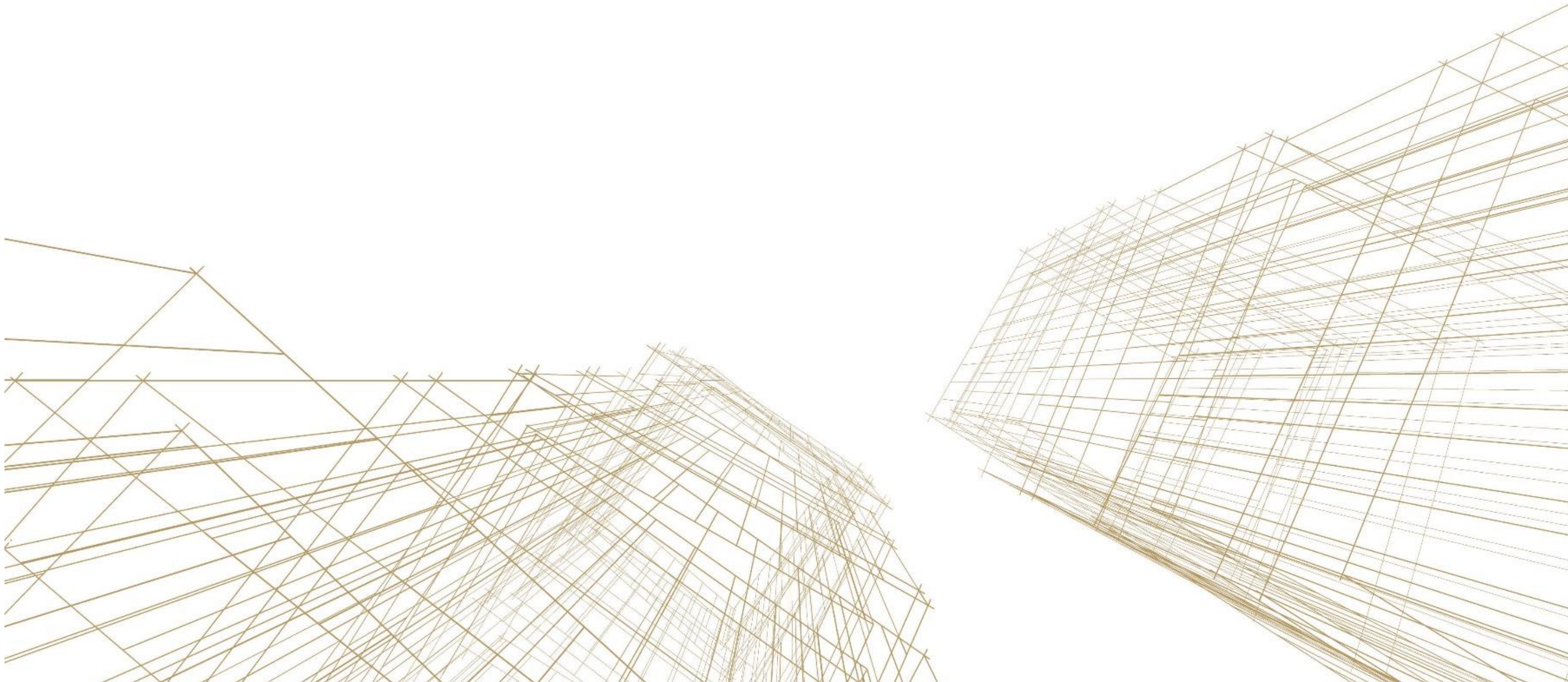
OREGON STATE LOTTERY

BIENNIAL SECURITY REVIEW 2024

OCTOBER 2024



1 ABOUT SYGNIA

Sygnia is a cyber technology and services company, providing high-end consulting and incident response support for organizations worldwide. Sygnia collaborates with companies to build their cyber resilience and defeat attacks within their networks. It has managed numerous high-profile cyber breach events and has become the trusted advisor of executive management and technology and security leadership of leading organizations worldwide, including Fortune 100 companies.

2 SCOPE AND OBJECTIVES

The cyber posture revisit and red teaming assessment was designed to assess Oregon Lottery (OSL)'s cyber security posture, and further enhance its overall cyber resilience. Conducted by Sygnia between August 19th 2024 and October 14th 2024, the engagement focused on reviewing the progress and changes made since the previous posture assessment engagement. Sygnia reassessed security capabilities across OSL's environment, and simulated real life attack scenarios, mirroring the tactics, techniques, and procedures (TTPs) used by real world adversaries, with the following objectives:

- Provide OSL with a high-level strategic perspective of its security posture, and the security alignment with the evolving security threats.
- Identify strengths, gaps, and opportunities for high impact improvements.
- Address specific challenges, dilemmas, and priorities in relation to implementation of OSL's Cyber Security Roadmap and Strategy.
- Address how to better utilize existing security stack within OSL's environment and suggest recommendations for new capabilities and processes if needed.

3 ENGAGEMENT PHASES

The assessment included five main phases:

1. **Information Gathering**: Numerous information-gathering sessions were conducted on network, infrastructure, systems, and security technologies and processes.
2. **Adversary Simulation**: In this phase, Sygnia's Adversarial Tactics team executed hands-on adversary simulations against OSL infrastructure, assessing attackers' ability to penetrate the environment, to move laterally, and accessing sensitive data.
3. **Analysis:** After completing the information gathering sessions and hands-on activities, Sygnia consolidated insights, identified strengths and areas for improvement and review changes since the last posture assessment.
4. **Initiatives Development**: This phase involved developing resilience-enhancing initiatives, prioritizing them based on their expected impact on security and feasibility.
5. **Validation and Presentation**: The final phase of the engagement involved presenting and validating the draft report, followed by delivering the final report.

4 FINDINGS & CONCLUSIONS

Based on the assessment, it was determined that OSL's cyber posture has continued to mature, with notable improvements made in Network and Security Governance in comparison to the 2023 assessment.

Cyber security processes are closely tracked, strong interfaces exist within the security organization, demonstrating increased awareness, knowledge, and commitment to further security improvement.
No critical vulnerabilities were identified that would enable an attacker to breach OSL's perimeter, indicating that OSL's external and physical attack surfaces are minimal.
Additional strengths were identified in terms of detection and response, alerting on most of the hands-on activities conducted by Sygnia.

Sygnia did identify areas in which cyber security could be further enhanced. As a result, new detailed and prioritized resilience-enhancing initiatives were provided to OSL to mitigate the identified risks. These initiatives are pragmatic, actionable, and impact driven.

The specific recommendations provided could reveal or otherwise identify security measures, or weaknesses or potential weaknesses in security measures, taken or recommended to be taken to protect OSL.

Therefore, in accordance with ORS 461.180(6) and ORS 192.345(23)(d), due to the sensitive nature of these recommendations and mitigation efforts, the specific findings are not provided in this public report.