Information Security Report

2019

June 6, 2019

Joint Legislative Committee on Information Management and Technology

OREGON STATE TREASURY

Our Way is Forward

Vision Statement

Leading the way for Oregonians to achieve long-term financial security

Mission Statement

Improving Oregon governments' and citizens' financial capabilities

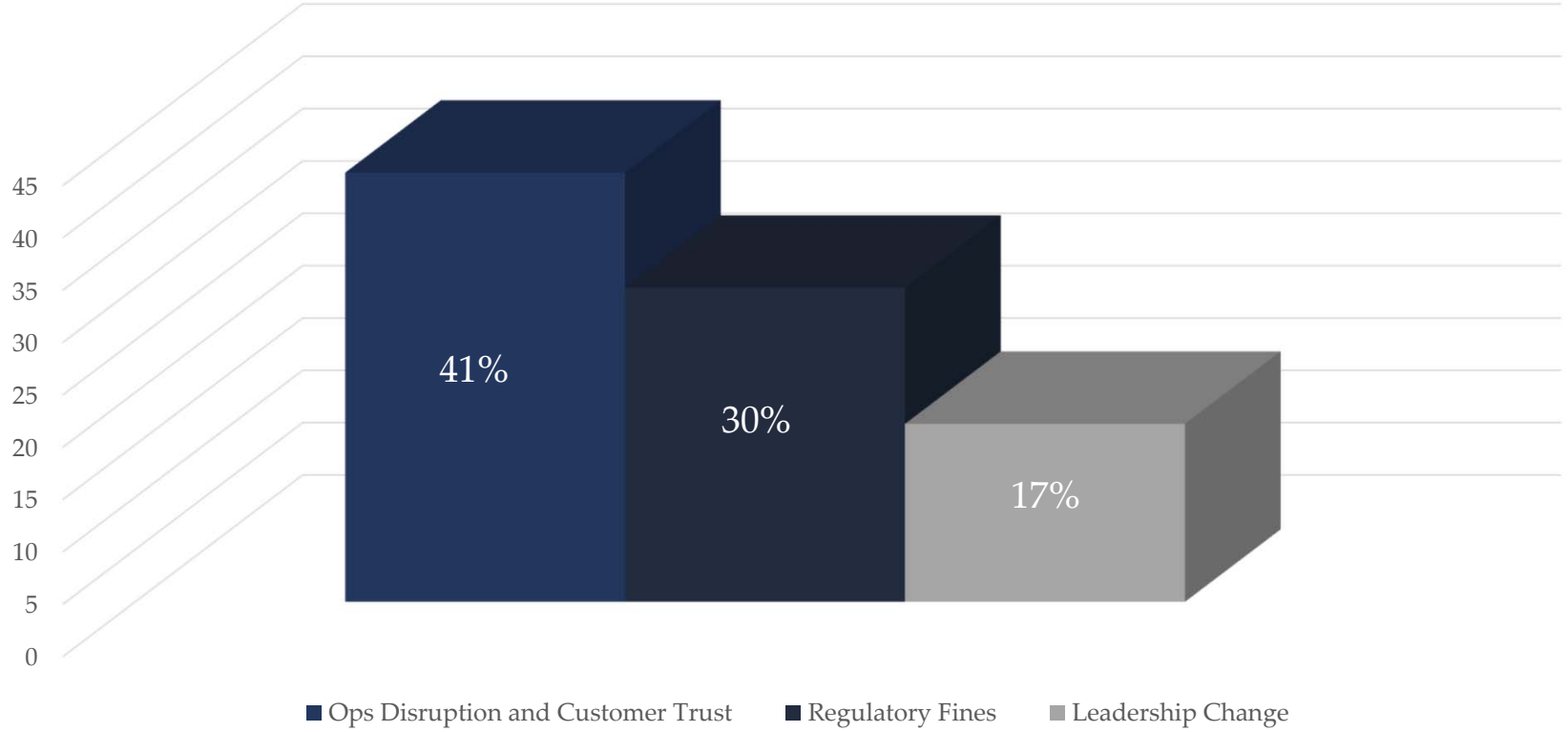
Our IT Mission

Improving Oregon governments' and citizens' financial capabilities *through collaborative, resilient, innovative, and secure technology solutions*.

Cyber Attacks in the Financial Services Industry

- Financial industry is **300 times more likely** to face an attack
- Attacks have **tripled** in the last five years
- **More money** to address and contain
  - **$18 million** average firm recovery (vs $12 million in others)
- **87 %** of cost is business disruption and info loss

Biggest Impacts of Cyber Events



Top Threats to Financial Services Organizations

1. Phishing/Malware
2. Technical Vulnerabilities
3. Third-Party
4. Data Leak/Data Integrity
5. Unauthorized Access

Treasury's Cyber Security Profile

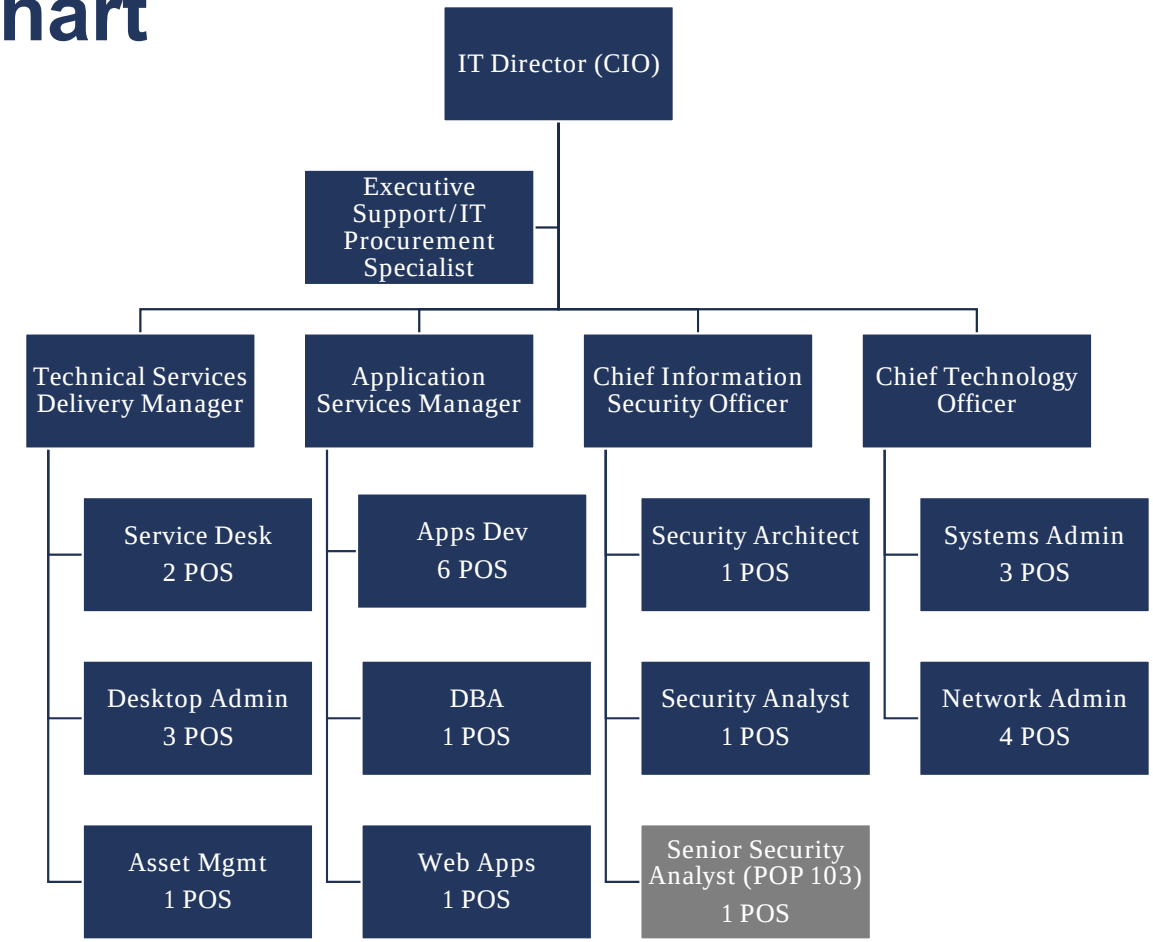
- Bottom line: Millions of annual transactions, hundreds of billions of dollars
- Complex integrated systems providing critical financial transactions
- Provide the computing infrastructure and expertise needed to conduct business securely and reliably
- Three connected locations (Salem, Capitol, Tigard)
- Design and manage solutions that meet business needs through a combination of cloud-based, purchased, and custom in-house developed applications
- Process and organizational maturity

Information Security Program

Frameworks

- ISO 27001:2013
- National Institute of Standards and Technology (NIST)
- Cybersecurity Framework v1
- Center for Internet Security (CIS) Critical Security Controls v7.1
- Oregon Statewide Information Security Standards (2017)
- Oregon Statewide Information Security Plan (2018)

IT Org Chart


IT Director (CIO)
Executive Support/IT Procurement Specialist
Technical Services Delivery Manager
Application Services Manager
Chief Information Security Officer
Chief Technology Officer
Service Desk 2 POS
Desktop Admin 3 POS
Asset Mgmt 1 POS
Apps Dev 6 POS
DBA 1 POS
Web Apps 1 POS
Security Architect 1 POS
Security Analyst 1 POS
Senior Security Analyst (POP 103) 1 POS
Systems Admin 3 POS
Network Admin 4 POS

IT Program/Embedded Security Model

Technical Services Delivery

Service Desk
- ITIL Call Center
- Tier 1 Triage
- Ticket Tracking and Escalation
- Knowledgebase
- Mobile Device Management

Asset Management
- Hardware/Software Inventory
- Warranty Management
- Lifecycle Management
- Issue monitoring and reporting

Desktop Support
- Patching
- Tier 2 Troubleshooting
- End-User support

Application Services

Application Development
- Application Development and Maintenance
- COTS/SaaS Evaluation and Implementation
- COTS Updates
- Integration
- Web Design

Data Management
- Database Administration
- Data Analysis
- Data Management

Banking Operations
- Transaction Processing
- Job Scheduling

Information Security

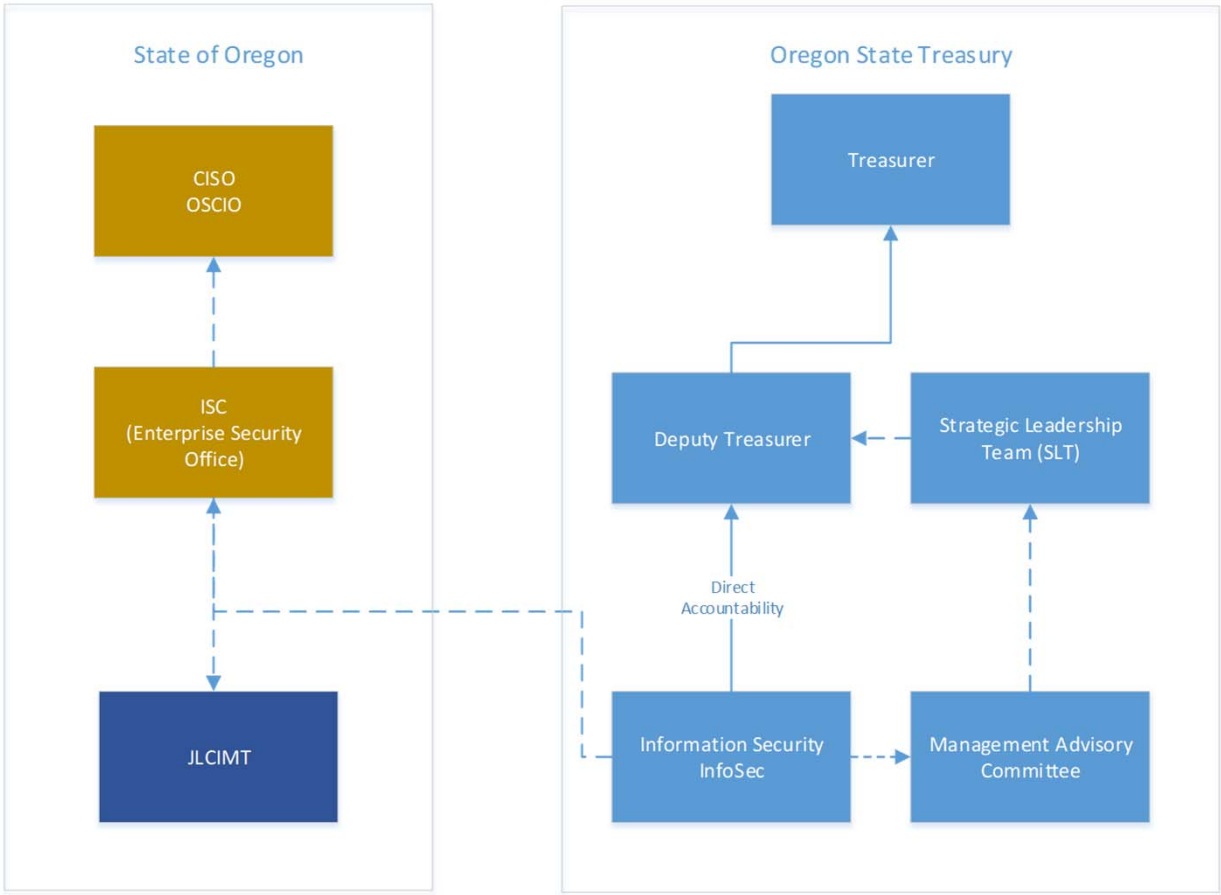
- Agency-wide Information Security Program
- Information Security Risk Management
- Application Security
- Information Security Policy
- Network & Systems Security
- Third-party Due Diligence
- Security Awareness
- Incident Response
- Threat and Vulnerability Management
- Continuous Monitoring
- Identity and Access Management
- Data Security

Infrastructure Services

Systems
- Server and Desktop Infrastructure
- Office and Collaboration Tools
- Patching and Compliance
- Remote Access
- Secure Data Transmission

Network
- Network Infrastructure
- Network Management and Monitoring
- Virtual Infrastructure
- Backup and Recovery
- Physical Infrastructure

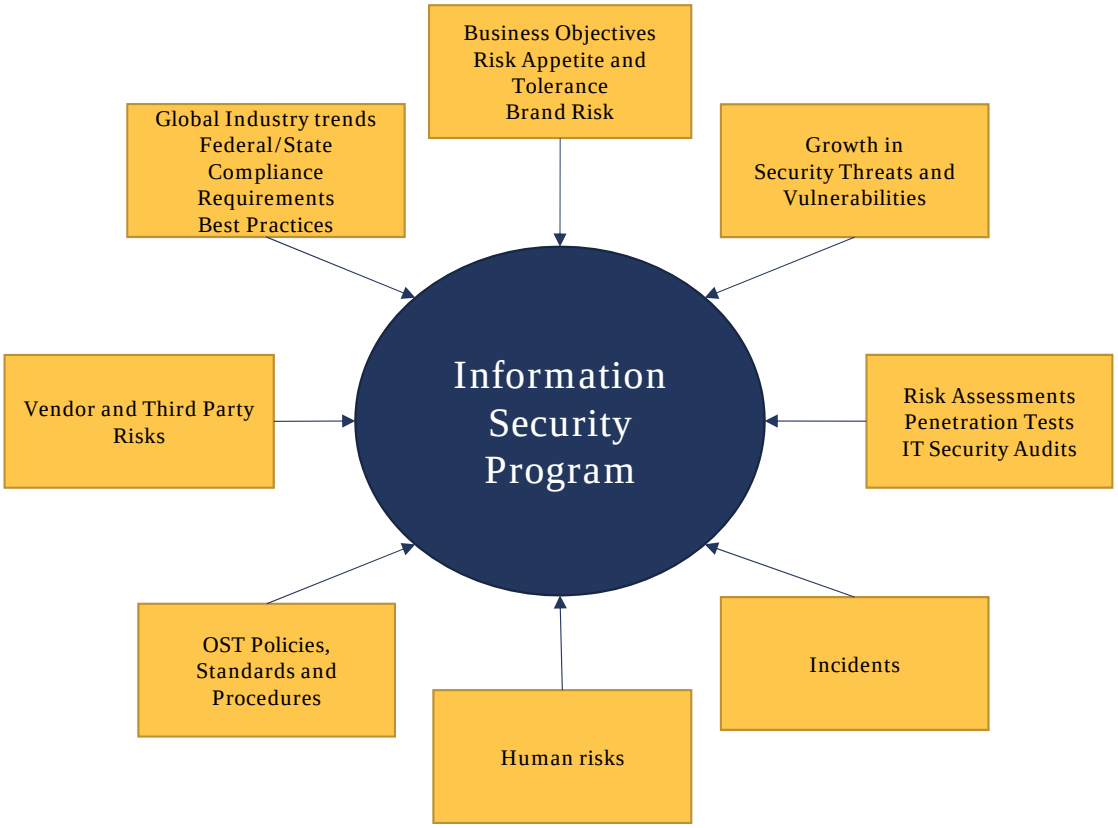
Security Governance



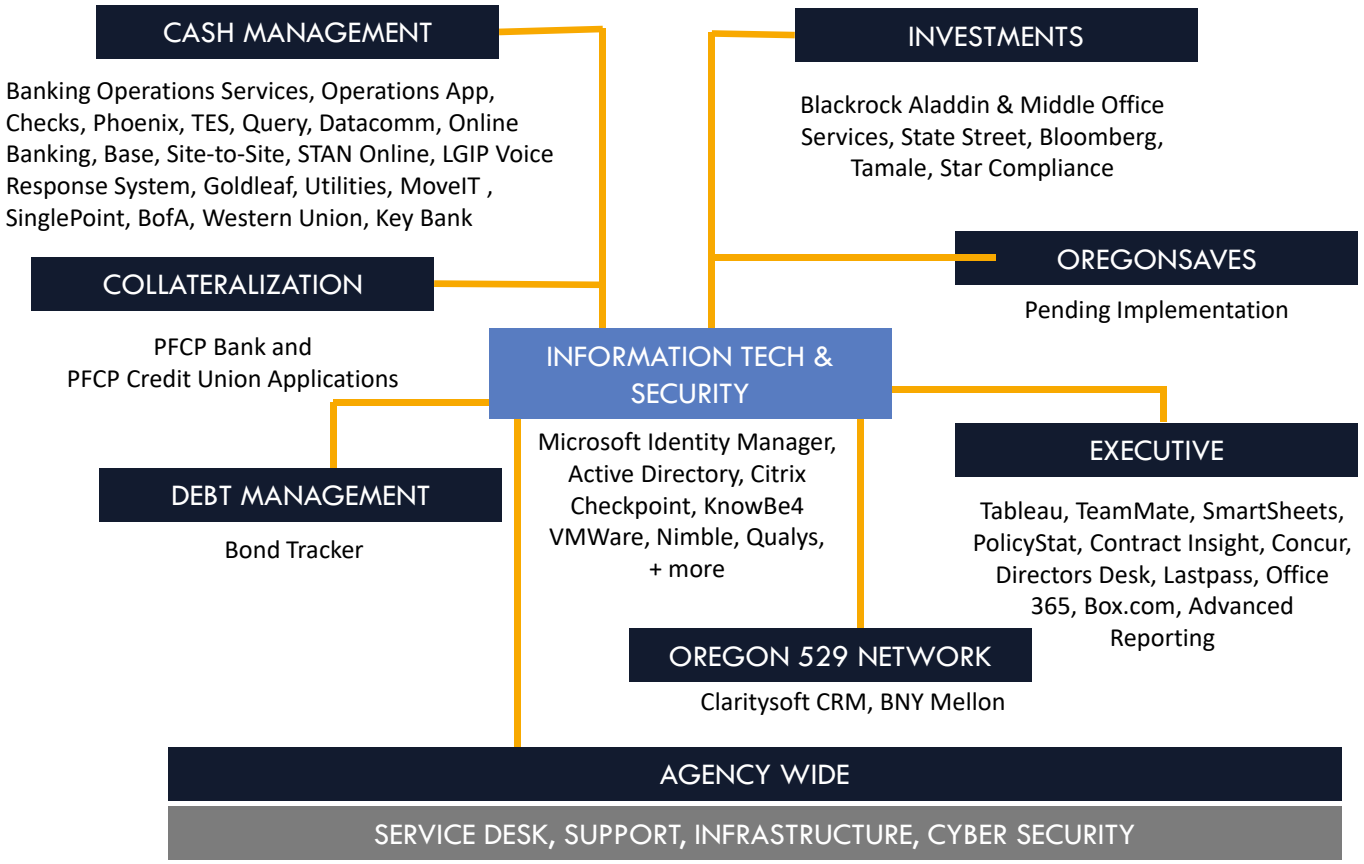
Security Collaboration

- Enterprise Security Office (ESO)
- Enterprise Security Strategy 5-year
- ESO/OST Joint Incident response
- Independent Agency Security
- Info-Tech
- Financial Services – Information Sharing and Analysis Center (FS-ISAC)

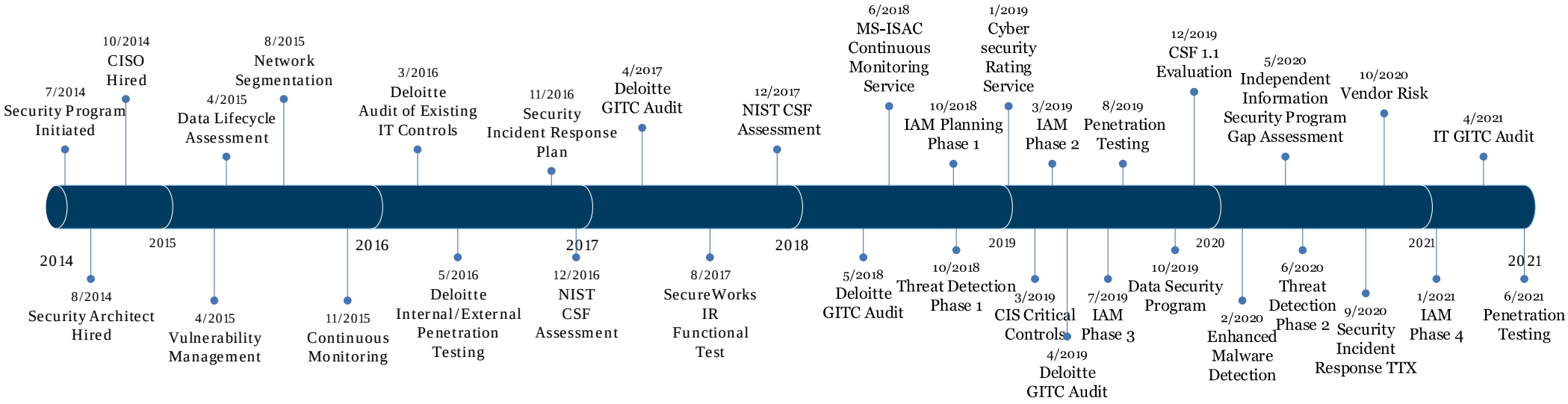
InfoSec Key Drivers



IT and Cyber Security

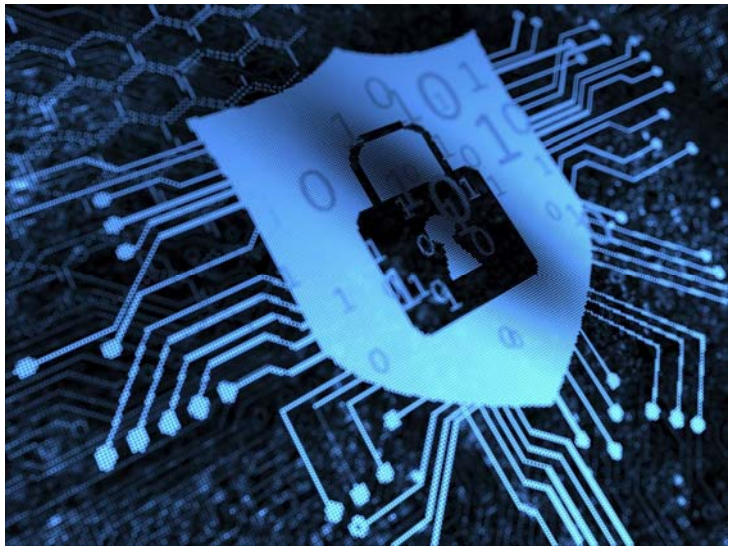


Information Security Program Activities



Security Assessments

- General IT Controls – Logical Access Audit by Deloitte. (March 2017)
- General IT Controls – Change Management Audit by Deloitte. (May 2018)
- General IT Controls – Network Operation and Physical Security audit by Deloitte. (March 2019)
- Comprehensive Penetration Test – (2019)
- Security Program Gap Assessment – (2020)
- IT General Controls – (2020)
- Application Penetration Testing – (2021)



General IT Controls Assessment Results

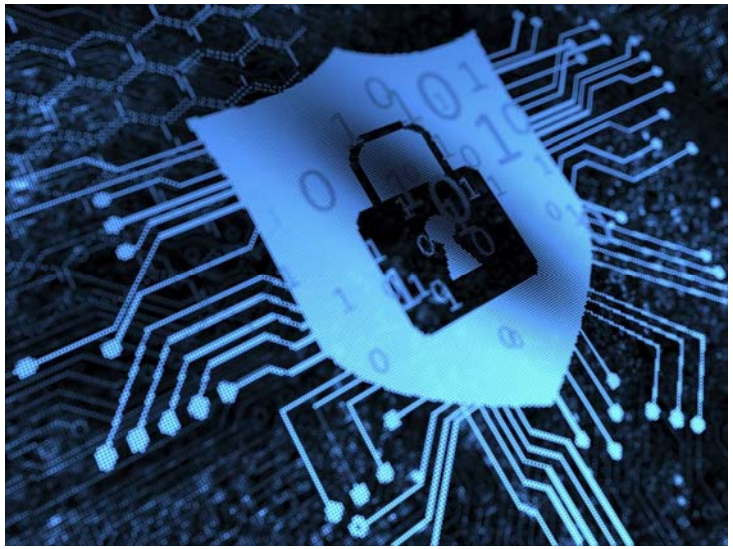
- Change Management Maturity
- Formalize Vendor Management
- Identity and Access Management Program
- Expansion of Application Development Security

Security Assessment Remediation Process

- Each security audit finding is analyzed and prioritized based on risk – likelihood and impact, cost of remediation, complexity etc.
- Items that require budget and comprehensive planning are incorporated into the Information Security Plan and, in some case are included in POP requests – i.e. IAM project, data security, and enhanced malware detection
- Assigned to the appropriate IT team
- Resolution due dates are set
- Bi-monthly status and follow-up
- Remediation activities are documented
- Internal review of remediation is performed

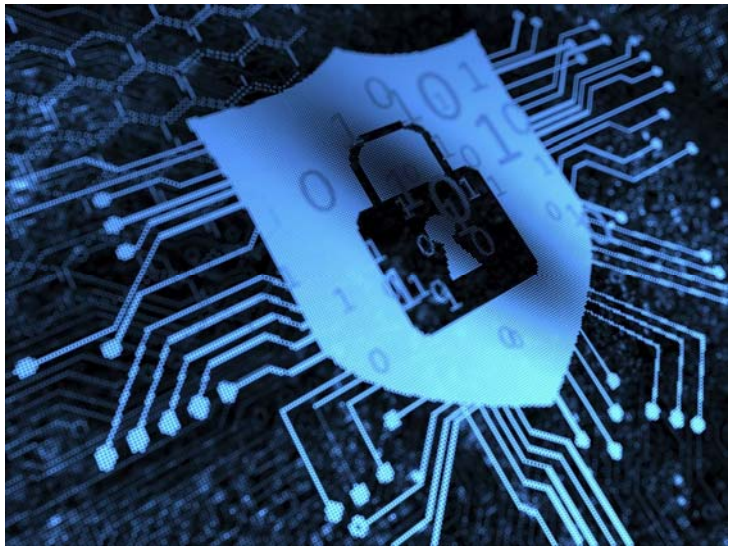
Information Security Investments

- Threat and anomaly detection
- Continuous monitoring
- Information security research and advisory services
- Identity and Access Management service provider (Current RFP)
- Cybersecurity rating service



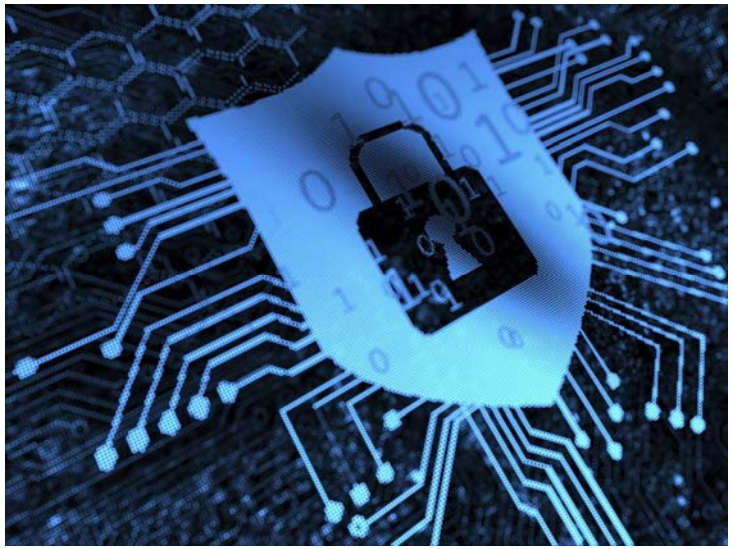
Recent Key Improvements

- Next Generation firewall technology (2017-2018)
- Security Hygiene (2018)
- Third-party security risk management (April 2018)
- Continuous Security Monitoring Service Migration (June 2018)
- Security awareness (September 2018)
- Implementation of Security Threat and Anomaly Detection Capabilities (November 2018)



Staff Training

- Security boot camp
- Microsoft Conference
- Security Conferences
  - Annual FS-ISAC Security Conferences
  - Annual RSA Conference
  - Gartner Information Security Summit
- Banking Security Conference
  - US Bank
- SANS Security Training



OREGON STATE TREASURY

Tobias Read
Oregon State Treasurer

350 Winter St NE, Suite 100
Salem, OR 97301-3896

oregon.gov/treasury