Information Technology Ecosystem/Security, including Risk Management Report

BACKGROUND

The Executive & Audit Committee annually reviews with university leadership the top risks that may impact Oregon State University's ability to meet its mission and objectives. Each of the top risks identified are assigned to the various Board committees based on alignment with each committee's charter and workload. Through this process, the university identified OSU's *information technology ecosystem and security* as a top risk for the university. The Executive & Audit Committee provides oversight of the university's action plan for mitigating this risk.

STATUS UPDATE

Management of the university's information technology ecosystem and security is guided by OSU's IT strategic plan, which is now in its second year and on track. The 2023 IT Strategic Plan's vision is that OSU's community members will lead vibrant, digitally empowered lives, enabling their transformative impact at OSU and beyond. This aspirational vision is then translated into the 2023 plan's strategies and a second document, the IT Roadmap, which is a rolling 18-month set of actionable plans. The IT Roadmap describes, prioritizes and outlines the resourcing required to implement the strategies in the IT Strategic Plan. Through pursuit of the strategies of the IT Strategic Plan and completion of the Roadmap, OSU works to mitigate Information Technology ecosystem and security risks. This report addresses OSU's work in three areas: building the data ecosystem, strengthening the information security program, and implementing an identity and smart access environment.

BUILDING THE DATA ECOSYSTEM

Central to realizing the IT Strategic Plan's vision is the ability to manage and effectively use data about the university, its missions, and its impact. OSU's shorthand for this ability is that the university must "Free the Data" OSU community members need while maintaining security and privacy. A modern organization runs on continuously updated information, and staff must create a data ecosystem within which OSU managers and others can use information to deliver effective teaching and learning, research, and extension and engagement, and adapt to the current and future demands of students, faculty, and communities. IT ecosystem risk is elevated at OSU due to its historical approach of viewing data collected by the university in silos and only in the context of the individual functions being performed. Data connections among the different functions are not automatic, and data are often trapped within computer systems, needing to be re-entered again and again for each system that needs it, or they may be excluded entirely.

OSU is now intentionally designing the data ecosystem needed to run a modern university. This requires considering data collection, storage, analysis, and access comprehensively, so that leaders can make decisions based on better information:

- Staff in IT are deeply engaged in the design of this environment. Initially, a consulting group was engaged to define OSU's approach and critical path. Following the consultant's advice, OSU re-established a data governance approach that ensures the IT work addressed the needs of the university and considered the responsibility to treat data securely and protect privacy.

- OSU is partnering with HelioCampus, a higher education data analytics firm, to deploy new data sets for enrollment management and student success. The resulting data environment is on track for release in summer 2022.
- The university's next step is to design a new data hub, which will connect the needs of OSU's administrative, academic, research and extension units to the information and technology tools that create insights for effective decision-making and help enforce data governance. By managing this data intentionally, staff can quickly integrate separate systems and migrate to new digital systems as needed, while maintaining the integrity and privacy of OSU's data.

Objective 1 in the Attachment 1 table lists the associated actions and their status.

STRENGTHENING THE INFORMATION SECURITY PROGRAM

In October, 2020, the university released a three-to-five year plan to continuously improve OSU's cyber maturity and reduce information security risk (the "Information Security Resilience Plan and Roadmap"). The plan uses the NIST Cybersecurity Framework (CSF)) as the measure for OSU's Cyber Maturity level. The CSF provides a means of assessing an organization's capacity to identify, protect, detect, respond, and recover from a cybersecurity attack. Maturity assessments were conducted in February 2021 and November 2021, demonstrating that the university has made improvements in all five categories of the NIST CSF. Overall, the program increased in assessed maturity by 16%. Functional area increases are included in the Performance Metrics Table within Attachment 1, and specific achievements justifying these increases are provided here:

- OSU's Information Security Advisory Committee (ISAC) received an updated charter, and refreshed membership to better represent the full spectrum of the OSU mission. ISAC is charged with advising the Chief Information Security Officer (CISO) on how best to balance information security risks with the broad mission of an R1 research-intensive land-grant institution, and to build understanding and improved communication of risks to the OSU community.
- Six information security rules were published or updated during 2021. A major change was updating the university password policy to make OSU account credentials more resilient. One new rule established revised password expectations for people in the OSU community who have elevated permissions to use applications and systems.
- OSU expanded its investment in Microsoft tools, which protect Linux and Apple devices in addition to computers using Windows operating systems, dramatically increasing visibility into the security of the university's IT ecosystem. With this action, OSU gained an enhanced cyber security capability that addresses many common cyber threats in an automated fashion. The OSU Security Operations Center is using this resource to continuously improve cyber-threat detection and response. This work has resulted in reduced risk through proactive and continuous monitoring of the university's IT ecosystem, with a very large number of cyber incidents being addressed before they impact the OSU community.
- Through the use of third-party risk identification tools, OSU achieved a 90% reduction in critical and high exposure vulnerabilities, compared to February 2021. The risk tools allowed for a focused coordination campaign across OSU IT staff to mitigate and remediate risks. The tools monitor over 100 vendors, including credit card processors, cloud services, core instructional applications and others. Coupled with improved security reviews of large cloud-based procurements, OSU has gained improved understanding of risks posed by third parties.

Objective 2 it the Attachment 1 table lists the associated actions and their status.

IDENTITY AND SMART ACCESS

The ability to lead vibrant, digitally-empowered lives at OSU in support of instructional, research, extension, and service missions requires OSU community members to have secure access to the right information whenever they need it, whatever role they hold, and with any device they use. The IT Strategic Plan has a strategy that is intended to make this possible.

The IT Roadmap sets out the work needed to achieve this strategy over the short-term. It seeks to address an immediate risk: currently OSU cannot ensure that individuals have access to only the data, systems, and services they need, and no more. The university's ability to grant permissions to specific systems or roles based on identities is limited. Further risk is created by OSU's insufficient ability to manage and protect the devices ("end points") through which individuals gain access to OSU IT systems and data.

To address these risks, the IT Strategic Plan and Roadmap provide for a "smart access" program that will deliver a "zero trust" data environment with stronger systems for managing identities and granting permissions. With smart access, OSU will simultaneously strengthen security for end point devices. This program includes the following activities:

- An Identity Task Force was formed to understand university identity requirements.
- The IT advisory firm, InfoTech, was consulted on identity and smart access strategies.
- Design of an approach to identity that supports business outcomes and institutional objectives is underway.
- Following design, the university wll acquire an identity tool to implement OSU's desired approach to identity management.
- Development of policies that simplify granting access to services and applications, based on the new identity management system is underway.

Objective 3 in the table in Attachment 1 lists the associated actions and their status.

NEXT STEPS

At its April 7 meeting, the Executive and Audit Committee will review the risk management report with staff and may identify additional follow-up actions, as needed.

Oregon State University
Enterprise Risk Management
2022 Priorities
Information Technology Ecosystem/Security

Risk Topic Oversight Summary						
Board Oversight Committee	**Risk Topic**	**University Goal**	**Type(s) of Risks to be Prevented**	**Risk Owner(s)**	**Primary Risk Mitigation Strategy(ies)[1]**	**Risk Mitigation Team**
Executive & Audit Committee	Information Technology (IT) Ecosystem/Security	Effectively implement the OSU IT Strategic Plan; provide for a data driven enterprise; and safeguard IT resources against loss of research, operational or student data; safeguard network services to prevent disruptions of service, financial loss, or negative perceptions of operational controls and maintain compliance with national security laws	Operational, Compliance, Financial, Reputational	Provost, Vice Provost for Information Technology and Chief Information Officer (CIO)	Accept, Reduce, Share/Insure	Chief Information Security Officer; Executive Director, Technical Solutions Architecture; IT Security Advisory Council

[1] Definitions of mitigation strategies:
Avoid: Discontinue the activities that present unacceptable risk
Reduce: Implement controls, practices, programs to lessen the risk
Share/Insure: Transfer the risk through insurance programs or 3rd party
Accept: Proceed with the activity because the benefit outweighs the risk

OBJECTIVE 1: Build a robust and unified university data/information ecosystem that delivers data as a strategic working asset	
Actions to Satisfy Objective	**Status Report**
Enterprise Data Ecosystem a. Re-establish data governance through a new data governance Council, Steering Committee and working groups to inventory and categorize data based on value to institution b. Partner with an external higher education data analytics firm (HelioCampus) to deliver data products for Enrollment Management and Student Success c. Ensure integration with new identity system and access control approach	**Completed and Planned Activities** a. Building out a new virtual data warehouse environment starting with student data from HelioCampus is on track for summer 2022. b. Subsequent data products will be incorporated into this new environment for reporting and analytics in FY23. c. To create a resilient and adaptive data ecosystem, a Data Hub will be the next step for the “free the data” efforts.

OBJECTIVE 2: Strengthening OSU’s Information Security Program	
Actions to Satisfy Objective	**Status Report**
Information Security Program a. Develop Information Security Plan and Roadmap based on the National Institute of Standards and Technology (NIST) cybersecurity framework (CSF) to guide maturation of program b. Update Information Security Advisory Committee (ISAC) charter and membership c. Published or updated information security rules d. Obtain Microsoft risk tools to improve insight into systems and continually update threats. **Identify** e. Implemented a third-party risk assessment tool **Protect** f. Implement a tiered security architecture and a three-security zone network with new firewall systems g. Revitalize awareness and training program h. Implement centralized logging policy and practice	**Completed and Planned Activities:** a. The Plan and Roadmap are complete and regularly updated. b. ISAC has been rechartered and has new membership c. 6 rules have been updated based on the advice of the ISAC and additional policy updates and improvements are in progress d. Microsoft tools in use to protect devices and to identify, detect and respond to threats **Identify** e. Third-party risk assessment tools in use **Protect** f. A tiered security architecture, new network security zones, and new firewalls are in place. Additional tiers will be added to meet other requirements. g. Information Security Critical Training updated; new OSU security resources on web site, and tabletop exercises conducted for staff, further improvements to training continue to be made h. Centralized logging is in place

Detect i. Centralize network, application, and endpoint anomaly detection j. Implement and maintain continuous monitoring k. Detection processes in place and constantly improved and refined **Respond** l. Mature the incident management system m. Implemented automated analysis and mitigation functions	**Detect** i. Anomaly detection has been centralized j. Continuous monitoring and detection processes in place with constantly being improved. **Respond** k. Incident response documentation updated, and incident commander qualification process is in place l. Vulnerability management program is being implemented m. Mature OSU's security incident management system n. Improve the OSU vulnerability management program to better tracks, prioritize, and manage vulnerabilities on an institution-wide basis o. Revise and update an ongoing OSU security training and awareness security program

OBJECTIVE 3: Protect Oregon State University information assets and stakeholder privacy in line with university values	
Actions to Satisfy Objective	**Status Report**
Identity and Smart Access Program a. Commission program b. Gather requirements c. Issue RFP for Identity tool	**Completed and Planned Activities:** a. External experts consulted on identity management b. Program team created c. Requirements gathered d. RFP for Identity tool to be issued March 2022

Performance Metrics		
OSU CSF Risk Profile for Personally Identifiable Information (PII) and Controlled Unclassified Information (CUI) systems and data		
Goal	**FY2022 Results**	**Comments**
Identify: 3 Protect: 4 Detect: 3 Respond: 3 Recover: 4	Identity: 1.87 (+14%) Protect: 1.83 (+12%) Detect: 2.18 (+26%) Respond: 2.21 (+21%) Recover: 2.33 (+5%)	Higher numbers better. OSU CSF Risk profile—Briefed to CEC in September 2019 and March 2021. Reassessed in November 2021. Percentage increase reflects change from March 2021 brief-out to CEC to November 2021 assessment.
Deliver training and resources to employees		
Goal	**FY2022 Results**	**Comments**
100% participation in employee and student worker training. Awareness and Training is a key element of the Protect functional area.	Delivered information security awareness training to 95% of faculty and staff and 70% of graduate employees, student Workers and post-doctoral scholars.	Metrics from 2021. OSU Critical Training Program has reset training as of February 2022, with a new approach to assure higher compliance in a short time.