Information Technology Ecosystem/Security, including Risk Management Report

BACKGROUND

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

STATUS UPDATE

In January, the Board approved the expansion of the risk item around information technology security to address data governance and privacy initiatives. The broadening of this risk item is consistent with the evolving security landscape and supports the continued maturity of the university's IT strategy.

As part of ongoing efforts to enhance the university's risk assessment process and the overall security program, and in alignment with the recommendations of the 2019 network security audit, a move was made in 2019 by the OSU Cybersecurity Program to begin the transition to a National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) based approach. As the university makes this transition, the initial assessed maturity level for the current program is "medium low." This means that while most functional areas have activity taking place in them, there is work to be done to advance in maturity. Through the efforts outlined in the annual progress report in Attachment 1, the OSU CSF will move the level of maturity of the cybersecurity program to one that has "fully documented policy with minor business related exceptions." Continuing to mature the program will also contribute to university leaders' understanding of what levels of risk remain and the causes in order to advise appropriate mitigation strategies.

NEXT STEPS

The Board will be provided this written report at its April 3, 2020 meeting. Additional discussion of the topic will be scheduled at a future meeting, as determined by the Executive & Audit Committee chair. In addition to Board reports, routine updates on IT ecosystem/security projects will be provided to the Compliance Executive Committee, chaired by the Provost.

Oregon State University
Enterprise Risk Management
2020 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 Ecosystem/ Security	Safeguard IT resources against disruption of research, operational or student data, maintain compliance with national security laws and ensure all employees readily have secure access to the data they need to do their jobs and enable data-informed decisions.	Operational, Compliance, Financial, Reputational	Provost, Vice Provost for Information and Technology	Accept, Reduce, Share/Insure	Chief Information Security Officer, Associate Provost of Infrastructure and Operations, 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

Mitigation Plan	
OBJECTIVE 1: Identify and Communicate Risks	
Actions to Satisfy Objective	**Status Report**
a. Perform annual assessment of systems and infrastructure. b. Enhance existing assessment framework to provide additional insight including reorganizing security program utilizing the NIST Cybersecurity Framework. c. Communicate results to Compliance Executive Committee (CEC) and IT Security Advisory Council on cost/benefit analysis. d. Implement OSU CSF, identify program gaps and prioritize risk areas.	**Initial objective actions complete, with work ongoing:** 1. Chief information security officer (CISO) from Virginia Tech assessed and provided a report on OSU's Information Security Program in February 2019. 2. OSU CISO conducted a NIST CSF based assessment of OSU in September 2019. The assessment was briefed to the Information Security Advisory Council and CEC in September 2019. 3. Vice provost for information and technology directed a Research and Education Network Information Sharing and Analysis Center (REN-ISAC) assessment be performed of the overall OSU information security program in spring 2020, using the NIST CSF as the assessment basis.
OBJECTIVE 2: Improve security management practice to effectively manage cybersecurity risks.	
Actions to Satisfy Objective	**Status Report**
a. Reorganize Office of Information Security as per best practice. b. Reorganize security program under NIST Cybersecurity Framework, as per best practices. c. Adopt two-factor authentication. d. Mitigate actions identified in audits. e. Develop OSU CSF practice and procedure. f. Develop Information Security Architecture. g. Develop security reporting that supports cybersecurity risk determination.	**Initial actions complete, with practice improvements underway:** 1. CISO hired April 2019. Information security program manager hired February 2020. 2. OSU Information Security Program has been realigned to NIST CSF. Program will be designated OSU CSF. 3. All faculty, staff and students are now mandatory DUO. 4. Audit action items completed with follow-up actions identified. 5. Initial practices and services to be developed are Vulnerability Management; Remote Access; and Identity and Access Management. Draft 5-Year Information Security Architecture produced.

OBJECTIVE 3: Mature OSU Information Security Program	
Actions to Satisfy Objective	**Status Report**
a. Formalize the cybersecurity program using the OSU CSF. b. Increase and improve cyber workforce skills and core competencies. c. Strengthen cyber governance. d. Create and update cyber and other related policies.	**Planned activities:** 1. CISO is developing a cybersecurity program strategy, which will nest under the IT Strategy that is currently under development. 2. Workforce Development Task Force is reviewing IT skillsets, including cybersecurity. NIST National Initiative for Cybersecurity Education (NICE) framework to be used to guide standards and training for workforce. 3. Governance Task Force is reviewing IT Governance at OSU; Cybersecurity governance is a key element and will be reflected in the IT Strategy and OSU Cybersecurity Program. 4. Policies and standards under development are Vulnerability Management; Remote Access; and Identity and Access Management.

Performance Metrics		
METRIC 1: The NIST Cybersecurity Framework maturity model is the basis for the OSU CSF Risk Profile used for Personally Identifiable Information (PII) and Controlled Unclassified Information (CUI) systems and data. The benchmark is based upon a scale of 1 to 5.		
Goal	**FY2020 Results**	**Comments**
Maturity goal for five categories: Identify: 3 Protect: 4 Detect: 3 Respond: 3 Recover: 4	Assessed average for five categories Identity: 1.77 Protect: 1.75 Detect: 1.91 Respond: 2.04 Recover: 2.29	OSU CSF Risk profile—Briefed to CEC in September 2019

METRIC 2: Deliver training and resources to employees		
Goal	**FY2020 Results**	**Comments**
Increased participation in employees and student worker training	Delivered information security awareness training to 81% of faculty and staff, and 58% of graduate assistants, student workers, and post-doc scholars.	March 2019 faculty and staff was at 69% complete. Graduate assistants and student workers have been tracked since May 2019, so no annual increase can be reported at this time.