Protecting Oregon's Critical Educational Assets Against Aggressive Cyber Threats

Threats to Oregon Universities

Oregon's higher education institutions must respond to an increasing number of sophisticated cyberattacks that range from minor attacks involving individuals, such as payroll fraud, to ransomware attempts and large breaches that affect thousands.

Recent reports, such as the Microsoft Digital Defense Report 2022, document that cyber criminals and Nation State actors have a specific interest in higher education, because of the richness of their data resources that include research discoveries and intellectual property, financial information, and the sensitive data of students, employees, and others.

Postsecondary institutions have obligations that set them apart from corporations and government entities. The purpose of higher education in many ways is to share information in an open environment that provides academic freedom and allows any and all parties to peruse accumulated information. Postsecondary institutions must balance the fulfillment of an obligation for openness with protecting crucial and sensitive information assets.

The attractiveness of universities, and the challenge to cybersecurity, is enhanced by difficult to protect IT environments. To achieve missions that range from delivery of health care to instruction, research, and outreach, universities require highly complex IT environments (with IT devices from laptops to building controls and scientific instruments) that are used and accessed through the diverse IT devices of extended and decentralized communities of faculty, staff, and students.

The increasing threat to universities is demonstrated in an analysis from Emsisoft, "The State of Ransomware." During the first quarter of 2021, the education sector accounted for nearly 10% of globally reported cyberattacks, compared with 7.5% during the first quarter of 2020. Oregon State University alone detected 286,668 phishing e-mails over 30 days in 2022.

Microsoft Threat Data:

Most affected sectors for reported malware attacks (one form of cyberattack) in the last thirty days (Retrieved on Dec 14, 2022)

Education	(81%)
Retail and Consumer Goods	(9%)
Health Care and Pharmaceuticals	(5%)
Telecommunications	(2%)
Financial Services and Insurance	(2%)
Power and Utilities	(1%)

The Request

HECC POP 204 was developed in response to an increasingly hostile cybersecurity environment that presents unprecedented risks and threats to Oregon's universities. It also responds to the burdens

created by new federal regulatory and information protection requirements and maintains university competitiveness for research funding.

HECC POP 204 would allocate $21.8M to address escalating cyberthreats to Oregon's universities to help protect Oregon's investments in its public universities and student and staff personal data. More specifically, it would address the greater cost of cyber insurance, deepen cybersecurity staffing, and support purchase of new cybersecurity tools that enhance the university's cyber-defense posture.

For More Information

Please contact Dana Richardson, Oregon Council of Presidents, at richardsond@mail.wou.edu, or the government relations staff member from any of the seven public universities. Thank you for supporting Oregon's students.