Oregon Community College Association

Cybersecurity Talking Points – January 2022

Ransomware attacks and cyberthreats have become significant operations concerns for community colleges and universities around the country over the past several years and have become more pronounced with the onset of the COVID-19 pandemic. These threats and attacks aim to hold institutional, employee and student data hostage for ransom money or to take this personal data for monetary gain. This means cybersecurity is of the utmost importance for institutional operations. In addition, most colleges do not have the in-house capacity or expertise to manage cybersecurity, even though it's as much a cost of doing business now as keeping the lights on. *Inside Higher Ed* recently ran an article about the influx of cyber threats on institutions, and the subsequent increase in cybersecurity insurance premiums.

Oregon community colleges are seeking one-time funds ($5.1 million) for training, security gap analysis and resolution, and upgrades to current systems to protect institutions from cybersecurity attacks. Colleges plan to hire a contractor to assist with advanced email protection and data recovery in the event of an attack. Each college would be allotted up to $300,000 to begin addressing this existential challenge.

Talking Points:

- Colleges seek $5.1 million to address cybersecurity protection measures at the 17 institutions. Each institution would be allotted up to $300,000 for the effort.

- Funds would support:
    - Training for college staff in vulnerability management, security awareness and phishing awareness;
    - Artificial Intelligence tool to protect against fraudulent account creation;
    - Outsourced email protection and data recovery;
    - Additional staffing to support cybersecurity protection; and
    - Data loss prevention.

- An estimated 82 colleges and public school districts have been the victims of cyberattacks in 2021, disrupting learning at more than 1,000 individual institutions and schools across the country, according to the cybersecurity company Emsisoft. Microsoft has reported that education is currently the most targeted industry in malware attacks. Nationally, there's been a 300% increase in cyberattacks in education over the past year.

- At least three American community colleges have been attacked by cybercriminals using ransomware since Nov. 30, the latest in a wave of such attacks targeting at least 19 higher education institutions in 2021.

- Even as attacks have buffeted colleges, experts say many remain woefully underprepared and underinsured. As a result, they are vulnerable to paralyzing and costly data breaches and system shutdowns, for which they often must pay crippling ransoms. Ransomware gangs are targeting colleges in part because they often are under-resourced. Community colleges are at particular risk, but even wealthy corporations have struggled to prevent increasingly sophisticated ransomware attacks.