Technology Board Report - January 2025
Sam Rigby

PowerSchool Data Breach

- In December, a non-authorized person used a PowerSchool employee's compromised credentials to access and download student and staff data from thousands of school districts nationwide.
- PowerSchool has stated that the data breach has been contained and that there is no further evidence of unauthorized access.
- We have confirmed that LPSD's PowerSchool database was accessed and some data downloaded.
- LPSD does not store student or staff social security numbers in PowerSchool, so that information was not compromised.
- PowerSchool believes the hacker primarily aimed to use the stolen data to demand a ransom rather than sell or distribute it to other bad actors.
- PowerSchool has provided reasonable assurances that its internal cybersecurity practices have been adjusted to close the exploited vulnerabilities.
- PowerSchool has engaged Experian to offer complimentary identity protection and credit monitoring services to all students and educators whose information was compromised. This offer applies regardless of whether an individual's Social Security number was exfiltrated. Additional information will be shared with staff and students as it becomes available.

While this incident did not result from any action or inaction by LPSD employees or contractors, it highlights the need for strong internal cybersecurity policies and protocols. I am continuing to work to strengthen LPSD's cybersecurity posture.

Web Filtering - The Children's Internet Protection Act (CIPA) requires schools that receive discounts for internet access to have internet safety policies, including but not limited to web content filtering.

Web filtering is incredibly complex and requires continuous management. Several months ago, we invested countless hours rebuilding all the layers of our web filter from the ground up, only to learn that recent software updates implemented new privacy and security features that allowed many of our filter layers to be easily bypassed.

Helpdesk tickets regarding web filtering are in the top 3 we see most frequently, so I know it can be frustrating for staff and students when they cannot immediately access a website that has been unintentionally blocked or miscategorized. However, our priority is safeguarding our students from harmful and inappropriate content on the internet, as required by law.

Failed Battery Backups - We recently replaced the battery backups (UPSs) powering our school networks. The UPSs protect our equipment from power fluctuations and unexpected shutdowns during brief power outages. Unfortunately, several of the new UPSs we deployed this year failed during extended power outages. We are working with our tech liaisons to retrieve the failed UPSs for warranty replacement.

Travel - We are finalizing plans for a February trip to a few sites with immediate tech needs.