BUFFALO PUBLIC SCHOOLS
Office of Information Technology
Myra Burden, Chief Technology Officer
65 Niagara Square
Suite 807 City Hall
Buffalo, NY 14202
Phone: (716) 816-3572
Email: myburden@buffaloschools.org

March 12, 2021

Dear Colleagues,

During the morning of March 12, 2021, Buffalo Public Schools was hit with a ransomware event. The IT department immediately went into problem resolution mode reaching out to a number of expert colleagues and professionals who have had experience with these types of events.

Current Status

- At this time, no demands have been made; however the FBI has found out that ransom may be between $100-300K and could be negotiable.
- Currently the technical team is triaging the impact and coordinating recovery efforts.
- The FBI is engaged and assisting.
- The primary goal of the team is the recovery of critical systems for the continuity of teaching and learning.
- The IT team is comprised of BPS staff, district enterprise system vendors, and other industry experts; they are moving expeditiously but with care, in an effort to preserve critical data, minimize the risk of reinfection and to support the criminal investigation.

Technical Next Steps for Recovery

- Office365, Teams, Infinite Campus, Munis, Schoology, Versatran, Blackboard, Clever, ATK2 (phone system) are identified critical systems for recovery.
- Validate the status of Office365.
- Validate the status of Tyler Munis (backup) and can it be restored in a cloud environment.
- Validate the status of Infinite Campus.
- Validate the status of Azure AD and can it be the primary source for authentication.
- Create a clean segmented network and restore to Cloud if possible.
- Restore authentication services.

Cyber Investigation Next Steps

- Superintendent approved an emergency contract with Grey Castle for cyber security investigation. The district's Chief Financial Officer, General Counsel, and Director of Purchase were notified and agreed to the execution of the emergency agreement.
- Work with Grey Castle to collect initial investigative information.
- Install Carbon Black on all servers and endpoints.

We anticipate knowing the scope of the problem, the extent of the work required to address the problem, and the timeframe to return services to normal over the next few days. I will continue to update accordingly throughout the weekend as we make progress on this critical project.

Respectfully,

Myra Burden
Chief Technology Officer

"Putting Children & Families First to Ensure High Academic Achievement for All"