BUFFALO PUBLIC SCHOOLS
Office of the Superintendent
65 Niagara Square Room #712 City Hall
Buffalo, New York 14202
Phone (716) 816-3575 * Fax (716) 851-3033
krinercash@buffaloschools.org

March 15, 2021

Colleagues:

Following is a concise update regarding the cybersecurity attack on the Buffalo Public Schools on the morning of March 12, 2021.

Today's update:

Staff has restored the functionality of equipment, systems, and applications in the majority of our buildings over the weekend and today. 54 of 67 locations report no disruption to internet and wireless systems as of this afternoon.

Tuesday, March 16 and 17:

Tuesday, March 16th and Wednesday, March 17th, all district and school based staff will report to their respective sites. Students will remain at home. Tuesday, each school will send a message regarding when to log on for "office hours," to learn the new log on process and participate in asynchronous learning. Wednesday, there will be a full day of remote instruction.

The district will continue to pressure test system restoration and access, as well as communicate any new or required information for students to access virtual learning tools once instruction resumes. Principals will be given instructions from IT regarding specifics on how school staff will assist with these recovery efforts.

What happened?

The Buffalo Public Schools experienced a cybersecurity outage on the morning of March 12, 2021. Our Information Technology staff responded and began to bring systems offline as an urgent precautionary measure.

Scope of the Incident

We are actively working with cybersecurity experts, as well as local, state, and federal law enforcement to fully investigate this criminal cybersecurity attack. Although the investigation into this security incident is ongoing, our comprehensive investigative team has identified key findings related to its root cause and potential overall impact to BPS systems. Meanwhile, IT will continue to provide staff with training and information to safeguard against cybersecurity threats to personally identifiable information.

Timeline to Recovery

Full recovery after a cybersecurity attack on an organization, is a multi-phased process. The district is making headway in restoring critical systems that support the primary function of teaching and learning. We have also prioritized the recovery of any affected business operation systems. The district will implement a longer term comprehensive initiative to enhance IT security and infrastructure going forward.

Status of Personally Identifiable Information (PII)

At this point, our lead investigative consultant and the FBI have not determined that there has been an exposure of PII. The investigation, which is both system forensic and criminal, is in its preliminary stages and will continue round the clock for at least two more weeks.

Information and updates will be provided through all normal communication channels as we continue to investigate and resolve this serious matter.

Respectfully,

Dr. Kriner Cash
Superintendent

cc: Board Members
Cabinet