Souderton Area
School District

A community where character counts

760 Lower Road • Souderton, Pennsylvania 18964-2311
Telephone: 215.723.6061 • Fax: 215.723.8897
www.soudertonsd.org

NETWORK DISRUPTION
FREQUENTLY ASKED QUESTIONS (FAQs)

WHAT WAS THE NETWORK DISRUPTION SASD EXPERIENCED?

On Sunday, September 1st, the District experienced a network disruption that was caused by a cyber attack. Following an investigation by law enforcement and cybersecurity experts, it was determined that ransomware was used in the attack. Once this ransomware was executed in the District's computer network by the attackers, it disabled internal network protections and encrypted data files.

WHAT DID THE DISTRICT DO WHEN IT DISCOVERED THE CYBER ATTACK?

Upon detecting the issue, district personnel immediately shut down the district-wide computer network and disabled Internet connections to avoid further damage. Law enforcement was contacted and the recovery process commenced within hours of the attack's discovery. It was quickly determined that the District's financial systems, which are maintained off-site, were not impacted.

WAS ANY DATA BREACHED/STOLEN?

Law enforcement and cybersecurity personnel have affirmed that ransomware does not typically result in the compromise or theft of data. To date we have found no evidence of personal information being compromised as a result of this event. At this time, we believe the attack was limited to the encryption of data files only. District systems containing personnel and financial information are housed off-site and have not been affected. Backup files of high school students' transcript information were not impacted by this event, which allows us to provide transcript information to students and colleges as we work to decrypt other data files.

WHY WAS THE DISTRICT VULNERABLE TO THIS CYBER ATTACK?

The District uses an array of industry standard and reputable firewall and malware protection services to shield against infiltration attempts by cybercriminals. Despite these protections, the cybercriminals were successful in penetrating and disrupting our network. As stated in the news media, numerous municipalities and school districts in our tri-state area and across the country have been targeted and victimized by cybercriminals in similar attacks.

WHAT ASSISTANCE IS THE DISTRICT RECEIVING?

On the day of the attack, the District worked with local law enforcement to report the issue to the Federal Bureau of Investigation. Subsequently, an agent from the U.S. Secret Service was on-site providing technical advice and facilitating communication with the Department of Homeland Security. A highly specialized cybersecurity firm was then engaged and continues to support data recovery efforts.

HOW WERE CLASSROOM INSTRUCTION AND OTHER DISTRICT FUNCTIONS IMPACTED?

From the onset, many important enterprise functions remained operational including phones, building security systems, business functions, and infrastructure controls. Within 24 hours of the attack, the District was able to restore e-mail and Web site services to facilitate critical communications. Because of this, schools were able to remain open while work continued to mitigate damage from the attack. Because technology is only one of many instructional components employed in classrooms, teachers were able to adapt their instruction to ensure learning continued with minimal disruption.

Revised 9/11/2019