MARYLAND OFFICE OF THE INSPECTOR GENERAL FOR EDUCATION

INVESTIGATIVE SUMMARY | 21-0001-I

Findings Regarding the Baltimore County Public Schools Cyberattack.

The Maryland Office of the Inspector General for Education (OIGE) initiated an investigation after receiving a complaint alleging that the Baltimore County Public Schools (BCPS) system disregarded the recommendations made by the Maryland Office of Legislative Audits (OLA) during their 2008, 2015, and 2020 audit reports. The complaint further alleged that because OLA published its November 2020 report findings, the BCPS information technology (IT) system became the target of a cyberattack.

The OIGE investigation revealed that on November 24, 2020, a cyberattack disrupted the BCPS website and remote learning programs. The OIGE determined that the cyberattack occurred approximately fifteen days before the disruption of the BCPS network. The cyberattack resulted from an unsolicited Phishing attack and was addressed to an education professional. In this case, the email pretended to be an official representing a college and contained an attached file purporting to be an invoice. The email format appeared legitimate to the BCPS staff member because it used a recognized email address and extension.

The staff member attempted to open the attachment but was initially unable to do so. The staff member then contacted a BCPS tech liaison (TL) assigned to the school for IT assistance. A tech liaison is a BCPS staff member (collateral duty) who has knowledge of basic IT operations and can assist an individual who is experiencing difficulties accessing their computer or other assigned electronic device. The BCPS IT division utilizes these individuals throughout the system to expedite IT services for staff and students.

The OIGE found that the TL examined the email sent to the staff member and concluded it suspicious. Because of the TL's concerns and the attachment's format, they forwarded the email to the BCPS DIT security contractor for assistance. The OIGE investigation revealed that the contractor mistakenly opened the email with the attachment using their unsecured BCPS email domain account and not in their secured email domain. Consequently, opening the attachment in the unsecured environment served as the catalyst, which delivered the undetected malware into the BCPS IT network.

The staff member attempted to open the attachment but was initially unable to do so. The staff member then contacted a BCPS tech liaison (TL) assigned to the school for IT assistance. A tech liaison is a BCPS staff member (collateral duty) who has knowledge of basic IT operations and can assist an individual who is experiencing difficulties accessing their computer or other assigned electronic device. The BCPS IT division utilizes these individuals throughout the system to expedite IT services for staff and students.

The OIGE determined that the cost to recover from this cyberattack, implement system upgrades, and migrate to the new platform has exceeded $9,682,437 million thus far. This cost includes initial emergency recovery, transition and tape recovery, and other system upgrades. The OIGE also determined that BCPS has reduced prior IT operating expenses by approximately $1 million because of system upgrades.

The OIGE has completed its investigation.

***

Unless otherwise noted, the OIGE applies the preponderance of the evidence standard in determining whether local school system personnel have committed misconduct.