MARYLAND
OFFICE OF THE INSPECTOR GENERAL FOR EDUCATION

Investigative Report Summary

OIGE Case 21-0001-I

Issued: January 23, 2023

MARYLAND OFFICE OF THE
INSPECTOR GENERAL FOR EDUCATION
Richard P. Henry, Inspector General

January 23, 2023

To the Citizens of Maryland and Baltimore County,

The General Assembly, at its First Session after the adoption of the Maryland Constitution, established throughout the State a thorough and efficient System of Free Public Schools; and shall provide by taxation, or otherwise, for their maintenance.[1] The Maryland Office of the Inspector General for Education (OIGE) plays a vital role in safeguarding State funds provided to local school systems. Our primary mission is to prevent and detect fraud, waste and abuse, and educational mismanagement within School Boards, the Maryland State Department of Education (MSDE), the Interagency Commission of School Construction (IAC), the twenty-four (24) local education agencies (LEA), and non-public schools who receive State funding throughout the State of Maryland. Except under limited exceptions, the Inspector General may not disclose the identity of the source of a complaint or information provided.

Background

The 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[2]. It was further alleged that the repeated OLA findings indicated that the BCPS IT division was not prepared for the cyberattack and failed to protect the personally identifiable information (PII) of students, staff, and BCPS retirees. Lastly, it was alleged that the BCPS failed to disclose the cost associated with ransomware[3] demands, the recovery of information, and improving the IT network following the cyberattack.

Information

The BCPS Division of Information Technology (DIT) provides all technical support services, resources, training, and student learning operations to 173 schools, programs, and centers throughout the school system. The DIT maintains over 100,000 computers and electronic devices

[1] Constitution of Maryland, Article VIII, Education, Section 1
[2] Cyberattack is any attempt to steal, expose, alter, disable, or destroy information through unauthorized access to computer systems.
[3] Ransomware is a type of malicious software, or malware, that prevents a user from accessing computer files, systems, or networks and demands a ransom using online payment methods to regain access to a system or data.

and provides technical support and services to approximately 140,000 users (18,600 employees / 115,000 students, and retirees).

Investigation

The OIGE reviewed the OLA Audit Reports regarding the BCPS dated October 2008, July 2015, and November 2020[4]. The OIGE determined that each report provided detailed findings and recommendations to BCPS related to identified network and PII vulnerabilities. Although each report provided pertinent IT findings, the sensitive elements of OLA's audit findings were not publicized. Therefore, the information concerning these findings was provided to BCPS for improvement and implementation.

The OIGE also reviewed BCPS policy and procedures governing Records Information Management (Policy 2380), Acceptable Use Policy for Technology and Social Media for Authorized Users (Policy 4104).

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[5] 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[6] 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[7] into the BCPS IT network.

An analysis of the anti-virus software used at the time of this incident determined that it was unable to detect the malware program used during this cyberattack. The analysis further indicated that the file format used was not a known identifiable format. Additionally, the malware used by the

[4] Office of Legislative Audits, Maryland General Assembly, https://www.ola.state.md.us/Search/Report
[5] Phishing attack is a form of social engineering, including attempts to obtain sensitive information and appear to be from a trustworthy person or business.
[6] BCPS IT Division regularly employed individuals as individual contractors based on their subject matter knowledge and expertise. The contractor in this matter did not possess general liability or business insurance.
[7] Malware is malicious code or software inserted into a system to compromise data confidentiality, integrity, or availability.

threat actor(s) had been programmed to delay its initial execution to avoid immediate detection. This delay allowed the malware to disable systematically critical functions within the BCPS network that could have prevented the malware from facilitating its attack.

Our review indicated that an indicator of compromise (IOC)[8] was displayed on individuals' computers once the malware was executed. This was shown as a banner indicating that the threat actors had infected the BCPS network, encrypted sensitive data, and made devices unbootable. This occurred on November 24, 2020, near the conclusion of the Board of Education meeting.

The OIGE reviewed records and reports, which indicated that the BCPS DIT took immediate action once it determined the network was compromised.

Findings

Due to an ongoing investigation by federal authorities, the OIGE's findings will be limited in its public disclosure.

Allegation 1. Baltimore County Public Schools (BCPS) system disregarded the Maryland Office of Legislative Audits (OLA) recommendations during their 2008, 2015, and 2020 audit reports.

The OIGE investigation found that BCPS had implemented several network recommendations made by the OLA in their 2008, 2015, and 2020 audit reports. The OIGE determined that several of the recommendations from the 2008 and 2015 audit reports had been partially resolved over each audit report or implemented due to network or system upgrades. The OIGE further determined that the recommendations listed in the OLA 2020 audit report and deemed applicable had been implemented as part of BCPS's network rebuilding process.

The OIGE did substantiate that at the time of the cyberattack, the BCPS had not relocated their publicly accessible database servers as recommended by the OLA. Following the cyberattack, BCPS migrated its database servers into a cloud (encrypted) based computing environment.

Allegation #2. As a result of OLA's published Audit Report dated November 19, 2020, and the findings listed within, the BCPS information technology (IT) system became the target of a cyberattack.

The OIGE did not find any evidence to substantiate this allegation. Based on the information reviewed and interviews conducted, the OIGE concluded that the malware had been delivered before the release of the OLA report.

[8] Indicator of Compromise is also referred to as a ransom note.

Allegation #3. Repeated OLA findings indicated that the BCPS IT division was unprepared for the cyberattack and failed to protect the personally identifiable information (PII) of students, staff, and BCPS retirees due to this cyberattack.

Due to the periods of the OLA Audit Reports (15 years) and the availability of former IT staff and executives, the OIGE could substantiate this allegation in part and could not confirm it in others.

The OIGE's review of the OLA's 2020 Audit Report found that BCPS had similar repeat findings in 2015. Both audits found that BCPS continued to maintain internal network servers. However, the OLA IT analysis indicated that this configuration did not provide adequate network security and noted a similar finding from their 2015 audit report.[9]

The OIGE did find that since the cyberattack, the BCPS has implemented an array of new security measures to ensure network integrity. The BCPS has also implemented Multifactor Authentication (MFA) standards for all staff, improved firewall technology, and enhanced device protections to detect and prevent malware. Additionally, the BCPS has migrated all essential network functions to a cloud-based environment and implemented security updates to ensure devices receive real-time security patches.

Allegation #4. BCPS failed to disclose the cost associated with ransomware demands, information recovery, and IT network improvement following the cyberattack.

Based on the information-sharing restrictions put in place by federal law enforcement at the time of the cyberattack, the OIGE could not substantiate the allegation regarding ransomware demands. Law enforcement agencies (federal, state, or local) may instruct individuals, staff, or other entities to restrict their communications with the public, the media, and members of their agency. This practice ensures the investigation's integrity, avoids misinformation or speculation by the public, and avoids sharing critical information concerning the investigation or other similar investigations conducted by threat actors.

The OIGE investigation found that BCPS IT staff were requested, by federal law enforcement, not to discuss the cyberattack with any other entity, including local officials. The OIGE further determined that BCPS staff were advised that the FBI would coordinate with local law enforcement due to the seriousness of the cyberattack.

The OIGE reviewed the network forensic analysis report and found that the malware had not corrupted BCPS's backup files. Unfortunately, when BCPS attempted to use the latest backup version to recover affected network information, they found that specific sectors[10] contained

[9] Office of Legislative Audits, Department of Legislative Services, Maryland General Assembly, Financial Management Practice Audit Report, Baltimore County Public Schools, November 2020, page 30.
[10] A sector is the smallest physical storage unit on a disk.

within the backup file were unreadable or damaged[11]. The analysis further determined that the identified sectors were limited to human resources and payroll information data. To mitigate further network damage, BCPS decided it would be in the school system's and staff's best interest to use an older backup file. The OIGE found that the backup file used to recover the human resources and payroll data was approximately one year old and did not include personnel, payroll, or benefit changes made before the cyberattack.

The OIGE found that using this backup file had other impacts on BCPS staff and retirees. However, due to the time between the cyberattack and the period used to recover personnel data, information related to payroll, tax deductions, benefits, and other personnel matters was calculated at previously authorized deduction rates, statuses, or income levels.

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.

Recommendations

1) Follow the 3-2-1 backup rule. This industry-standard rule directs organizations to keep/retain three copies of their data on two different devices/mediums with one off-site storage solution.

2) Use cloud backup with intelligence. The cloud could enable the school system to meet rapid recovery requirements and lower on-premises infrastructure costs.

3) Perform periodic recovery tests regularly. The mere existence of a backup does not imply that it can be recovered. Storage media can easily be corrupted, but most IT users are unaware of it. The backup system should include an automated process that automatically validates each new backup and warns of any problems.

4) Plan for recovery times. By having multiple backup strategies in place, you can avoid unnecessary delays.

5) Staff training. Training cannot be an annual event but must be an ongoing process. The best way to protect against ransomware is to prevent it with a comprehensive security awareness training program. Since phishing is the most common and effective method to spread ransomware, an effective ransomware training program should include ways to mitigate phishing attacks and how phishing can specifically lead to ransomware attacks.

[11] Damaged or bad sectors occur due to several reasons, including long-term use, physical damage, and improper formatting.

6) Develop procedures to report and respond to threats. It is critical to develop a robust training program for staff to avoid opening phishing threats and alert their IT department to take appropriate action before any damage occurs.

7) BCPS Executive Leadership should develop and implement a process to immediately resolve the benefits and payroll irregularities resulting from using outdated backups to restore its human resources data affecting staff and retirees.

It should be noted that this report only addresses the alleged complaints and will not disclose confidential law enforcement information. The OIGE, in coordination with the Federal Bureau of Investigation (FBI), offers this report for informational purposes only. It is not intended to provide legal information or to address all circumstances that might arise. If criminal actions are identified in this matter, those actions will be the sole responsibility of law enforcement. Individuals and entities using this report for other cases are encouraged to consult with their legal counsel.

The OIGE understands that information may be changed or updated after an investigation has been completed. The OIGE appreciates the cooperation provided by the members of the Baltimore County Public School system, the BCPS Office of Law, the BCPS IT Division, the Baltimore County Police Department, the Federal Bureau of Investigation, and the Maryland Department of Information Technology.

Consistent with Education Article §9.10-104, the Inspector General has identified issues of concern and will report these issues to the Governor, the General Assembly, the State Board of Education, and the State Superintendent of Schools.

Respectfully,

Richard P. Henry
Inspector General

cc: Ms. Jane E. Lichter, Chairperson, Baltimore County Board of Education
Ms. Robin L. Harvey, Vice Chairperson, Baltimore County Board of Education
Dr. Darryl L. Williams, Ed.D., Superintendent of Baltimore County Public Schools
Ms. Margaret Ann-Howie, Esq., Chief Counsel, Office of Law
Members At Large, Baltimore County Board of Education