San Mateo Union High School District

Kevin Skelly, Ph.D., Superintendent
Kirk Black, Ed.D., Deputy Superintendent Human Resources and Student Services
Yancy Hawkins, CPA, Associate Superintendent Chief Business Officer
Julia Kempkey, Ed.D., Assistant Superintendent of Curriculum and Instruction

May 6, 2022

Jenarda Dubois
Grand Jury Coordinator
400 County Center, 2nd Floor
Redwood City, CA 94063
Email: grandjury@sanmateocourt.org

RE: Follow-Up Response to the 2019-2020 Grand Jury Report entitled "Ransomware: It Is Not Enough To Think You Are Protected"

Dear Ms. Dubois:

The San Mateo Union High School District (the "District") has received and reviewed the request for a follow-up reply to the District's response to the 2019-2020 San Mateo County Civil Grand Jury report "Ransomware: It Is Not Enough to Think You Are Protected". Updated information is indicated in red.

FINDINGS:

4. Cybersecurity reviews and assessments, and an updated, well-executed Cypersecurity plan, are critical components of IT security strategy.

   The District agrees with this Finding. In progress, the District is in negotiations for a contract with Zenmid to perform comprehensive review of IT policies, network vulnerability assessment, network intrusion tests and cybersecurity training. Assessments includes, but not limited to, website, firewall, servers, core switches and routers, VPN connectors, and best practices in phishing and spam prevention.

5. A comprehensive Cypersecurity plan should include, at a minimum, information concerning prevention steps, spam and malware software, and backups and full recovery testing.

   The District agrees with this Finding. The agreement explained in response #4 includes the items contained in #5.

6. The identification of phishing attempts, including the use of spam filters, is an important component to protecting an IT system from Ransomware attacks.

   The District agrees with this Finding. In progress & ongoing. The District's network engineer monitors the District network daily to look for threats using various network tools.

7. Testing a full restore of a server to ensure that backups are reliable should be undertaken regularly as part of an entity's backup plan to recover lost information.

The District performs server restoration and backup tests annually. These are done through simulation and was rendered and successfully this year.

8. Training of new employees, and the recurring training of existing employees, is an important component of defense against Ransomware.

The District agrees with this Finding. The agreement explained in response #4 includes the items contained in #8.

RECOMMENDATIONS:

1. Each of the governmental entities in San Mateo County with an IT department or IT function (whether in-house, handled by another government unit or outsourced to a private enterprise) as listed in Appendix F, should by November 30, 2020, make a request for a report from their IT organization that addresses the concerns identified in the report, specifically:
    a. System Security (Firewalls, Anti-malware/Antivirus software, use of subnets, strong password policies, updating/patching regularly)
    b. Backup & Recovery (In the event of an attach, can you shut down your system quickly? What is being backed up, how it is being backed up, when are backups run, and where are the backups being stored? Have backups been tested? Can you fully restore a Server from a backup?)
    c. Prevention (turning on email filtering, setting up message rules to warn users, providing employee training on phishing and providing a reporting system to flag suspect content)

SMUHSD implemented this Recommendation on November 2, 2020 by directing the District's IT Department to prepare a confidential report which addresses the three concerns specifically identified above.

SMUHSD has the following in place: Router, Firewall, and Layer 3 switches that minimize potential cyber threats. SMUHSD also updates critical updates to servers and network equipment as they become available. Regular patches/updates will be applied after a minimum of 30 days waiting period.

SMUHSD has malware and phishing detection in place through Gmail. The District will continue to monitor email threats such as phishing and other malware and provide informative warning to the District's end users annually and when necessary.

By June 2021, SMUHSD will implement a "force" password change and implement a strong password policy. The District initiated this process and will continue to force staggered password reset every 6 months for students and staff.

SMUHSD backups use CTB (change base tracking) which minimizes the amount of time it takes for the backup process to complete, the retention policy for both schedules is two weeks. We receive notification of backup status daily and we can go back and check data for integrity which we will do monthly. We are currently backing of 30TB of district data which includes the SIS, and various other file servers. Completed. The District continues to perform hourly backup on local network storage. The District also has transitioned to a

cloud hosted Student Information System that's based on the Amazon AWS network. This allows for a fully redundant system with total rollback recovery in a disaster and is securely monitored by Aeries team for errors, downtime, or suspicious activity.

Our Restore option gives us the ability to restore virtual machines from two weeks prior to any problem. We also have the ability to do a granular file restore of a virtual machine which means that we can mount the backup image and go and retrieve a file from a particular day for up to two weeks. The Sandbox feature allows us to run a machine in protected mode to ensure that the backup is safe before we restore it. Completed.

To date we have not performed a full backup of our data, but we have explored all the features mentioned above and are knowledgeable on how to proceed if the need arises. We will be scheduling a disaster drill once every two to three months and Data recovery drills monthly to ensure all parties are capable of doing this in a crisis situation. Full data backup has been rendered and is repeated on a daily schedule. Full backups include servers & virtual servers. Data recovery drills are performed at least once a year.

By Summer of 2021, SMUHSD will implement offsite storage. The purpose of an offsite storage is to provide another redundancy of our data environment in a worst case scenario. It would be beneficial to explore having an offsite solution to house a copy of our critical services in the event the data center is compromised or lost by some unforeseen event. The District's Student Information System database is now offsite with multiple redundancy mechanism in place for prompt data recovery and restore in a disaster situation. All District mission critical data are saved in multiple locations.

2. These confidential internal reports should be provided to the governing body by June 30, 2021. This report should describe what actions have already been taken and which will be given timely consideration for future enhancements to the existing cybersecurity plan.

   The District intends to implement Recommendations that are not yet in place, provided that the District may require an extension of time (not to exceed six months) beyond June 30, 2021, depending on the scope, complexity, and feasibility of any recommended actions and/or enhancements. As noted above, SMUHSD has implemented and completed the tasks listed above. Most of the required tasks are ongoing. The others will be implemented this fiscal year because of the complexity or dynamic nature of the topics in items #4, #5 and #8.

This follow-up response was presented to and approved by the District Board of Trustees on May 5, 2022.

Please do not hesitate to contact me if you have questions or require additional information.

Sincerely,

Kevin Skelly
Superintendent
San Mateo Union High School District