Ransomware:
It Is Not Enough To Think You Are Protected

Issue | **Summary** | **Glossary** | **Background** | **Discussion** | **Findings**
Recommendations | **Methodology** | **Bibliography** | **Appendixes** | **Responses**

ISSUE

City and county government computer systems are at risk of Ransomware attacks. Are adequate measures being taken by local government agencies to mitigate the risks and provide recovery options?

SUMMARY

Ransomware has already hit many governmental Information Technology (IT) systems in San Mateo County. In December 2019 the Grand Jury sent an online survey to all 68 public entities in San Mateo County,[1] received 37 survey responses (a 54% response rate), and interviewed several responders including one IT Manager (who had refused to respond to the survey for fear of being successfully attacked once again), for a total of 38 responses via survey and interview. More than 25% (10 of 38) of the public entities responding to the Grand Jury reported that they have been a victim of one or more Ransomware attacks. More concerning is the certainty that there will be more attempts to violate the integrity of our local governments' electronic infrastructure.

This report is intended to present "best practices" in developing a Cybersecurity strategy, then implementing and testing that plan. It addresses actions that can be taken (and have been taken, in some cases) in order to guard against Ransomware attacks, recover from an attack and the additional measures that can be taken to reduce the possibility of an attack. However, it is not an exposé with details of potential system weaknesses, in light of the need for Cybersecurity strategies and practices to be highly confidential. As such, this report walks the line between providing an informed discussion of potential concerns without providing a road map of how to breach public government IT systems.

The single largest exposure every organization has to cyber-thieves is phishing, the illegal practice of sending legitimate-looking emails to an organization's employees. These emails may contain malware or links that, when clicked, infect the computer with a virus that can spread to the entire information systems network.

Although many email software programs include some level of protection against Ransomware attacks, such protections require customization and activation, and it is not clear that local public

[1] See Appendix F: Public Entities in San Mateo County (Cities, County, School Districts, Special Districts)

entity IT departments are undertaking these necessary customization and activation steps. In addition, training for new employees and recurring training for existing employees is critical to dramatically reducing the probability of a Ransomware infection. In some agencies, it appears that only limited training is provided for new employees with little or no recurring training provided for current employees.[2]

Ransomware and other malware attacks are a test to an organization's backup and restoration procedures.[3] The Grand Jury found that none of the survey responders has actually performed a full restore as a test of their backup process. However, without adequate testing, backups do not provide sufficient protection.

Rigorous preparation for an attack is essential if fast and full recovery is desired and the payment of a ransom is to be avoided. There are several significant steps that local public entities should take to improve their defenses, their ability to detect incursions, and their responses to Ransomware attacks. These steps include:

- Using firewalls to protect internal environments from breaches;
- Using malware detection software to monitor incoming emails and network activity;
- Ensuring that users are educated and tested to learn what to watch for and avoid, especially in emails;
- Developing and fully testing a thorough backup and restore strategy to enable a complete recovery from an attack;
- Putting in place internal controls such as subnets, which require departmental authorization to access other department's data or programs.

In addition, cloud hosting should be considered for email and certain applications to reduce the success of Malware and Ransomware attacks on information systems infrastructure.

While all attacks are malicious in terms of time and potential data loss, in the case of Ransomware (or worse, Ransomware 2.0 that also infects backup data) the financial cost of paying the ransom in order to remove the infection and restore a data system can be significant. Alternatively, if the decision is to not pay the ransom but to attempt to recover from the infection manually, the direct and indirect costs could be considerably more.

This report is directed to the governing bodies of government entities in San Mateo County urging them to have their IT staff confidentially and urgently assess their respective Ransomware protection strategies and training and then move with all deliberate speed to address any shortcomings in their Cybersecurity programs.

GLOSSARY

CLOUD COMPUTING
Cloud computing is the delivery of on-demand computing services -- from applications to storage and processing power -- typically over the internet and on a pay-as-you-go basis. Rather

[2] Grand Jury interviews

[3] Epicor Corporation, *Protecting Yourself From Ransomware*, January 2020

than owning their own computing infrastructure or data centers, companies can rent access to anything from applications to storage from a cloud service provider.[4] Some examples of this are Yahoo Mail, services like Google Docs, and customer relationship management software.[5]

CYBERSECURITY
Cybersecurity refers to the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, damage, or unauthorized access.[6] Cybersecurity is a combination of secure systems (hardware and software) built into technology as well as human intervention, monitoring, training, awareness, and recovery.

ENCRYPTION
The process of locking out the contents of a file and the renaming of the file such that it cannot be opened and used in the intended application (e.g. Microsoft Excel). Typically, a 128 Bit (or larger) encryption key (a long series of letters and numbers) is used first to encrypt then later to un-encrypt a file.

MALWARE
Short for "malicious software," this software is designed specifically to damage or disrupt computer systems. Not all malware is Ransomware because some malware has no related attempt to extort money.

PHISHING
The illegal practice of sending email claiming to be from reputable companies to induce individuals to reveal personal information or click on website links or open attachments that then install malware.

RANSOMWARE
Ransomware can be simply described as an infection on a host machine that prevents access to data until a ransom is paid. The most common method of infection is to encrypt files making them totally unreadable by a user. The infection is usually delivered by a *Trojan Horse* (a term referring to the misleading of users of its true intent) installed when a user clicks on a malicious link or attachment in an email.

RANSOMWARE 2.0
This newer version of Ransomware no longer is just malware that encrypts data and asks for ransom, the attacker also threatens to release the data onto the internet and demands money in order not to do so. This newer Ransomware works in such a way that even backup copies of most important files will not be able to save an infected organization.[7] By planting the malware but delaying its activation, Ransomware 2.0 can infect backups thus defeating their value.

---

4 https://www.zdnet.com/article/what-is-cloud-computing-everything-you-need-to-know-from-public-and-private-cloud-to-software-as-a/

5 Pearson Education, Ubuntu Unleashed 2015 Edition: Covering 14.10 and 15.04, page 655

6 https://digitalguardian.com/blog/what-cyber-security

7 https://www.itproportal.com/news/welcome-to-the-era-of-ransomware-20/

BACKGROUND

Ransomware is a real and serious threat to every entity: government organizations, corporations, and individuals. The more dependence an organization has on the software and data in its network(s), the more important the concern should be. Loss of access to mission-critical data, systems, and software can severely impact an organization in both the short and long term.

According to an October 2019 report by the National League of Cities, since 2013, Ransomware attacks have been reported by at least 170 county, city or state government entities across the United States.[8] The actual number is likely to be much higher because it represents only those attacks that have been reported. Many infections go unreported when ransoms are paid,[9] when organizations are seeking to avoid embarrassment, or when the attacks were simply undetected or untraceable.[10] This has been true even in San Mateo County where local public governing entities have had Ransomware attacks that were not publicly reported.[11]

Not only do such data breaches embarrass and slow organizational productivity, they can be very expensive. For example, the MIT Technical Review (2019) asserts: "Ransomware may have cost the U.S. more than $7.5 billion in 2019… the victims were 113 governments and agencies, 764 health-care providers, and up to 1,233 individual schools affected by Ransomware attacks…most local governments do a poor job of practicing Cybersecurity."[12] The cost to the city of Atlanta to recover from its Ransomware breach was estimated at $17 million.[13] Similarly, a recent Baltimore Ransomware breach is estimated to have cost over $18 million.[14] In 2020, the UC San Francisco School of Medicine paid $1.14 million in ransom to recover its own data.[15] These are large cities and entities and although the ransom amounts they paid may not represent the expenses a San Mateo County public organization could incur, they provide examples of the severity of the potential threat and the enormous costs.

Specifically, the costs of a Ransomware attack could include some or all of the following:[16]

- Direct Costs:
    - Paying the ransom to obtain an encryption key and hoping that it works;

---

8 National League of Cities report, *Protecting Our Data: What Cities Should Know About Cybersecurity*. Forward by Clarence Anthony, CEO and Executive Director.

9 https://healthitsecurity.com/news/as-ransomware-attacks-increase-dhs-alerts-to-Cybersecurity-insights

10 Sheehan, Patrick, Ohio Emergency Management Agency, *Cascading Effects of Cyber Security on Ohio*, September 19, 2012

11 Grand Jury survey responses

12 MIT Technology Review, *Ransomware may have cost the US more than $7.5 billion in 2019*, January 2, 2020

13 The Atlanta Journal- Constitution, Stephen Deere. *Confidential Report: Atlanta's cyber attack could cost taxpayers $17 million*. August 2018.

14 Baltimore Sun, Ian Duncan, Baltimore *estimated cost of ransomware attack at $18.2 million as government begins to restore email accounts*. May 29, 2019.

15 San Jose Mercury News, David Wu, "*UCSF pays $1.14 million ransom to recover data*", July 4, 2020

16 https://www.sentinelone.com/blog/what-is-the-true-cost-of-a-ransomware-attack-6-factors-to-consider/

    - Expenditures for outside IT professionals and new systems providers to plan and implement improved breach security based on new Ransomware strategies;
    - Paying for enrollments in credit reporting bureaus to stop or correct identity thefts (from the release of previously confidential or secure personal information) for client/customers.
    - Replacing hardware and/or software.
- Indirect Costs:
    - Operations efforts to restore systems and data;
    - Organizational downtime as well as employee overtime;
    - Reputation loss including negative public relations and loss of confidence by the organizations' constituents;
    - Liabilities for legal costs, including defense of lawsuits for breach of private and confidential information and poor handling of personal data.

According to the Coveware Report,[17] the median ransom payment in the first quarter of 2020 was $44,021. This was an increase of roughly 10% over the last quarter of 2019. Public sector entities represented 12% of attacks, about half of which were school systems. The average days of downtime was 15 representing an alarming number of days of inability to service constituents.[18] This underlines an urgent need to understand and evaluate current local governments' Cybersecurity strategies.

The discussion that follows is intended to encourage local public agencies and their IT staff to confidentially evaluate their respective Cybersecurity plans, software and prevention strategies. Since data and systems security are essential to the operation of every public entity in the County, the discussion will not present a specific road map for potential Ransomware-prevention actions but rather establish a "best practice model" that will enhance understanding of the elements essential for an adequate protection plan.

DISCUSSION

In December 2019, the Grand Jury developed an online survey that was sent to all 68 public entities in San Mateo County.[19] Responses were received from 37 of the entities (a 54% response rate). Additionally, follow-up interviews were conducted with three local public IT Managers, one of whom had refused to complete the online survey for fear of disclosing confidential information that could lead to a successful malware or Ransomware attack. These interviewees were questioned regarding the adequacy of Cybersecurity planning and execution. Following a general analysis of local government practices, this report concludes with a review of Cybersecurity best practices which local agencies should consider adopting.

Two Ransomware Attacks Derailed: Best Practices in Action

17 https://www.coveware.com/blog/q1-2020-ransomware-marketplace-report

18 https://www.msspalert.com/Cybersecurity-research/average-ransomware-payment-rises-again-research/

19 Appendix F

In order to better understand how to successfully defeat a Ransomware attack, the Grand Jury interviewed an IT Manager of a private enterprise that was attacked twice by Ransomware and was able to fully restore the environment and re-establish workflow within just a few hours.

Given the usual secrecy involved in most malware incursions, the following description of this IT manager's actual experience is instructive since it offers an example of "best practices" that can guide others anticipating or facing a Ransomware threat.[20]

This organization suffered two serious breaches less than two months apart and successfully recovered both times. In the first breach, within 45 minutes of a user clicking on an email attachment, the Crypto virus had spread to 12 of the organization's 23 servers. The IT Manager was alerted to the problem both by the user whose PC was locked with the Ransomware demand on his screen and an auto alert from the network scanning software that reported unusual activity.

The IT Manager's first action was to rapidly shut down the entire server network. This of course stopped the spread of the virus, but also prevented users from performing their jobs. Fortunately, their backup strategy implementation worked well as they were able to fully recover within hours.

The major components of the protection strategy employed included:

- Separating the network into discrete departments or segments (creating subnets) which restricted individuals' access to only servers containing their department's software and network storage. This limited the spreading of the virus across various departments within the organization. The analogy is a modern ship with rooms and decks that can be completely closed off from each other in the event of a fire or explosion.
- Taking snapshots (copies) of their Storage Area Network (SAN) twice a day.
- Completing full nightly backups of their SQL databases and incremental backups of the databases at five-minute intervals.
- Performing server backups with a commercial external backup appliance and/or service. See Appendix D for examples of companies in this market.[21]
- Regularly testing the restore process to ensure the successful recovery of critical server hardware. Without testing, there is no assurance that the Cybersecurity plan will work. Moreover, even if it works once, that is no assurance it will work again, without periodic re-testing.
- Conducting weekly backups of critical personnel's full PC hard drives.
- Use the "3-2-1 strategy"[22]: do three backups into two different media including one offsite.

Having all of these Cybersecurity plan components was a good start but it took much more to affect a recovery. First a commercial Virus Removal Software Tool was used which did not work (in this case). Therefore, the IT team used the snapshot copies to replace corrupted data on

---

[20] Grand Jury Interview

[21] These services include onsite and offsite backup and recovery services which are usually located outside the immediate locale.

[22] Management Wire, *The 3-2-1 Backup Rule and Effective Cybersecurity Strategy*, January 7, 2020.

infected server units followed by the application of the incremental backups of the database to complete the restore.

This detailed example represents a well thought out and highly prepared plan, executed with precision. The first breach resulted in 4½ hours of downtime as 12 servers were infected. The second breach resulted in 6 ½ hours of downtime to recover 19 affected servers. The IT team was able to recover the servers and their data both times, become fully operational within hours, and the organization did not pay any ransom demands.

Grand Jury Cybersecurity Survey and Follow-up Interviews

Survey question:[23] "*Has your Organization had a Ransomware attack? Specifically, has there been an instance or multiple instances when an attack has locked up a computer or computers and presented a demand for ransom to unlock the infection?"*

Nine survey responders and one non-survey responder interviewee, a total of 10 of 38 (37 responders to the online survey and one non-survey responder) affirmed an attack had occurred or had possibly occurred in their organization, a 26% "hit" rate. The circumstances of their attacks were reviewed.[24] The non-survey interviewee was the IT manager from a public entity in the County who was unwilling to complete the survey because they did not want to reveal that their organization had been subject to "one or more" Ransomware attacks. Nor were they willing to disclose how successful the Ransomware attack(s) were for fear that they would open themselves up to more attacks.

Survey Question:[25]
"*Is your Information Systems Budget adequate to secure your network properly from malicious attack?"*

Thirty-two of the 37 survey respondents, or 86%, answered Yes to this question. This high percentage of "Yes" responses either indicates a high level of confidence in their defense setup, a reluctance to complain about their IT budget, or as two of our follow-up interviewees revealed[26], a lack of understanding of the complexity of a well-written, well-executed Cybersecurity Plan.[27] Suggesting the latter, The National League of Cities conducted a similar survey of 165 city governments nationwide and asked the same question, ("*Is your budget adequate enough to secure your network properly?")*: 67% replied "No". [28]

Investigation Results Regarding Backup/Restore/Maintenance

The Grand Jury survey and follow-up interviews revealed that, while many local agencies have backup plans,[29] only a portion of those same agencies had successfully recovered lost files from

---

[23] Appendix A – Question #1

[24] Grand Jury Interview

[25] Appendix A – Question #2

[26] Grand Jury Interviews

[27] Federal Communications Commission, *Cyber Security Planning Guide*, October 2012.

[28] National League of Cities report, *Protecting Our Data: What Cities Should Know About Cybersecurity*, page 8

[29] Appendix A – Question #3

backups and none of the survey responders had ever done a full restore of a server.[30] When an attack occurs with inadequate backup processes in place, there is no way to recover. Moreover, a proactive and well-thought-out business continuity plan is something that all system and data administrators must embrace.

What is a good backup strategy? Certain applications provide the ability within the applications themselves to set up different types of backups and schedule them to be performed automatically. A good example of this is SQL.[31] Using a SQL-based approach, both nightly full database backups can be scheduled as well as intermittent transaction log backups (which capture activity during small time increments), so that a recovery could be completed with virtually no loss of data. These backups should then be stored according to the 3-2-1 backup rule[32] whereby three copies or versions are taken, stored on two different media, one of which is offsite. Operating systems and third-party vendors offer a multitude of backup solutions for servers. Snapshots or image backups[33] provide the most complete backup and the fastest restore option.[34]

Raj Samani, Chief Technology Officer for Europe at Intel Security captures the importance of a complete backup strategy, "Most Ransomware attacks can be avoided through good cyber hygiene and effective, regular data backups that are continually tested to ensure they can be restored if needed."[35]

As this discussion shows, the technology to prevent and if necessary, correct, the impact of a malware attack is available. Local government agencies must be pro-active and vigilant in using such to protect their data and their businesses.

Investigation Results Regarding Employee Training

Education is the best defense. "Preventing infection is far easier than correcting the situation as most of the infections are acquired either from a socially engineered email (one that appears reputable or from a familiar source), or from visiting an infected website, so controlling risk on your side is the easiest method."[36]

Answers to Survey Question #5 provide strong evidence for the need for the governing boards to review with their IT managers their defenses against cyberthreats: "*Do you provide training to employees regarding malware?"* 12 responded with a non-qualified "Yes". Nine responded "No" (24%) and 16 responded with a qualified "Yes" (42%) and described their training as

---

30 Appendix A – Question #4

31 Structured Query Language (SQL) is a programming language

32 Management Wire, *The 3-2-1 Backup Rule and Effective Cybersecurity Strategy*, January 7, 2020.

33 Image backup consists of block by block storing of the contents of a hard drive

34 https:\\www.ltnow.com/file-backup-vs-image-backup-which-is-best/

35 Zerto, Raj Samani, *Ransomware – Mitigating the Threat of Cyber Attacks, 2019*

36 Epicor, *Protecting Yourself from Ransomware*, January 2020

needing improvements.[37] As one survey responder commented, "The answer is yes, but a lot more needs to be done."

Cybersecurity training is a well-established industry – providing a focused set of classes and materials designed to reduce users' clicks on harmful links and attachments. Security training, awareness, and assessment should be a routine part of the Cybersecurity strategy in government. Deploying such a program covers the education, training and testing of employees to recognize, delete and report attempted attacks. Studies show these programs reduce but do not eliminate user error.

Government Technology magazine captured it best in their cover story entitled "In the quest to guard against cyberthreats, can we solve the people problem? The Weakest Link."[38] The article concluded that even with the best training programs and defenses, the human element may never be completely overcome.[39] This is precisely why recurring training and user testing is encouraged by best practices.

Handling Incoming Emails – Phishing Defenses

In a worldwide survey of Managed IT Service Providers (MSP's) in 2019, "67% of Ransomware attacks originated from a phishing or spam email…the easiest method of delivery and man does it pay off."[40] The greatest threats take advantage of users "within" the network, i.e., users who click on malicious links or open email attachments that contain viruses or make other mistakes that allow hackers to gain access to the entity's system or network. Trend Micro estimates that the vast majority of all attacks occur when a user clicks on something they should not.[41]

There are different ways to help the user community recognize and protect against a phishing attack. Most network environments utilize spam filters to automatically filter incoming messages. Spam filters are used to detect unsolicited, unwanted, and virus-infested email and stop it from getting into email inboxes.[42] "Additionally, malware detection software can also be highly successful in reducing the risk of Ransomware but the anti-malware definitions (a database of known infectious code) need to be constantly updated…which takes effort and time but represents the single most effective defensive strategy."[43]

Message rules can be used to flag external emails and thereby decrease the probability that a user clicks on bad content. An administrator can set up message rules on a users' client or the email server. An example of a message rule might be if the sending organization includes *@smithco.com* in the sender's address, the message is automatically moved the incoming message into a personal folder called "Smith Company." A better example would be a rule that

---

37 Grand Jury Survey responses

38 Government Technology Magazine, Adam Stone, *The Weakest Link*, Oct/Nov 2018

39 Ibid

40 VadeSecure – Predictive Email Defense, *Ransomware Attacks: Why Email is still the #1 Delivery Method",* January 16, 2020

41 https://blog.trendmicro.com/online-phishing-how-to-stay-out-of-the-hackers-nets/

42 https://www.mailchannels.com/what-is-spam-filtering/

43 Epicor, *Protecting Yourself from Ransomware",* January 2020

flags all external emails (not from the host's domain) and warns about the threats of clicking on attachments or weblinks. An example of this visual potential threat message rule is displayed in Appendix C.

Message rules can be very powerful to alert users of potential threats or to be careful about what they might click on and endanger their system. Some of the vendors listed in Appendix B also can "report" a suspected phishing attempt to an IT administrator. The Grand Jury's review revealed that some of the Information Technology Services departments for local public entities have installed message rules on their email servers to notify users of external emails.[44] This is a "best practice" which all local governmental agencies should consider.

Phishing emails are easy to create, as they do not take a high level of skill to provide the illusion of legitimacy by mimicking web-site brands or using logos from Google images. They can also easily spoof (fake) an email address to look like a trusted source.[45] It can often be very difficult to catch these risky emails, as the spoofed emails are cleverly disguised. A YouTube video created by Cisco Systems illustrates the sophisticated approach a phishing email may take – "Anatomy of an Attack".[46] It shows an attacker constructing a realistic identity deception email and can be viewed at https://www.youtube.com/watch?v=4gR562GW7TI After you watch this video please note, had an email filter caught this message and flagged it as external and warned about clicking on links, the deception may have been caught.

What Does Excellent Cyber Defense Look Like?

Survey Question[47]: *"What defenses do you currently employ to block malware? Please be specific. (Firewall brand/model, Software filters/spam blocker, etc.)"*

Five survey responders did not divulge the infrastructure of their environment. 17 responders provided abbreviated details indicating they do have Cybersecurity protections in place. The remaining 15 responses were explicit about their organizations' hardware and software defense strategies. Below is a survey response that illustrates a well-protected environment using some of the best practices of Cybersecurity:

"At the first layer, we use a PAN 220 Firewall with all subscriptions enabled, (URL Filtering, Antivirus/Vulnerability, Wildfire, etc.), block all international countries both in and outbound. Once traffic is passed for email, it passes through a Barracuda spam filter, filtering and scanning phishing and virus emails, checks with External Reputation servers for known virus and spamming servers, then passes to an on-premise exchange server. The exchange servers have another layer installed, Symantec Antivirus, giving a third layer of scanning. All servers and workstations have the latest version of the antivirus installed controlled by a centralized server. Window patches are applied on a monthly basis to all servers and workstations, and servers are retired once Microsoft ends support for an operating system." [48]

---

44 Grand Jury interviews

45 Ibid

46 Cisco Systems, *Ransomware - Anatomy of an Attack*, https://www.youtube.com/watch?v=4gR562GW7TI

47 Appendix A - Question #6

48 Grand Jury Survey response

The survey respondent's best practices:

- Filtering incoming email for viruses, malware, and phishing attempts;
- Utilizing protection software from multiple vendors;
- Utilizing multiple layers of defense;
- Keeping systems up-to date.

Breaches and attacks that manage to extract data (Ransomware 2.0) expose additional risks to sensitive information. Security professionals point out additional options for securing organizational data:[49]

- Use Subnets[50] to section out servers with separate security permissions and limited access;
- Disable and block unused services, protocols and ports;
- Perform Backup & Recovery (focus on full testing of recovery);
- Strengthen the password policy (long, complex, with expiration dates);
- Employ 2-factor authentication (password then keycode) for external user access.[51]
- Install Anti-malware / Antivirus software on all machines and keep current (update at least monthly);
- Update at least monthly, patches for operating systems, firewalls, spam filters, malware, and other key applications;
- Perform monitoring and auditing of failed logins, password changes, resource usage, and services stopping.

Local public entities can get assistance from The Federal Communications Commission's (FCC) Cyber Security Planning Guide that includes a customized Cyber Security Planning Tool to craft and execute a customizable Cybersecurity plan.[52] As their introduction explains, "data security is crucial … customer and client information, payment information, personal files, bank account details … all of this information is often impossible to replace if lost and dangerous in the hands of criminals… losing (your data) to hackers or malware infection can have far graver consequences."[53] Public entities should take advantage of this Guide in reviewing the current status of their own data system security.

When answering questions of respondents via email it was found that some already use cloud hosting for email.[54] During the interviews it was further uncovered that a school IT manager is considering additional cloud hosting of one or more of their applications. Cloud providers are able to provide layers of protection for a customer's network and software, as well as creating a segregation between their network and their customers. A cloud provider will patch and

---

49 Government Technology Magazine, Adam Stone, *The Weakest Link*, Oct/Nov 2018

50 https://searchnetworking.techtarget.com/tutorial/Protocols-Lesson-6-IP-subnetting-The-basic-concepts

51 The County's Office of the Assessor-County Clerk-Recorder and Elections has already instituted 2-factor authentication. 2018-2019 Grand Jury Report – Security of Election Announcements.

52 Federal Communications Commission, *Cyber Security Planning Guide* https://transition.fcc.gov/cyber/cyberplanner.pdf and FCC *Cyber Security Planner* (customizable) https://www.fcc.gov/cyberplanner

53 Ibid, page PDS-1

54 eMails received from public domain accounts

maintain current software versions, leverage security and malware and have a dedicated security team (24x7x365) that is responsible for staying on top of the security risks.[55]

Conclusions

Grand Jury survey results and in-depth interviews determined that some local government agencies have Cybersecurity strategies in place. For them, this report is asking those IT departments to re-challenge the sufficiency of their employee training, the regular (full) testing of their defense strategies and the adequacy/age of their Cybersecurity strategy including consideration of cloud hosting. For the rest, this is a good time to complete a review and see what additional measures can be taken to beef up their IT security using the information provided in this report as a guide. The biggest trap is believing that a malware attack, or in the worst case a Ransomware attack, is unlikely to happen to organizations and that the Cybersecurity strategies already in place are sufficient to successfully recover.

As learned from the best practices example of the IT manager who thwarted two attacks successfully, a comprehensive Cybersecurity plan includes user prevention steps, spam and malware software, back-ups and full recovery testing. These suggestions as well as those from the professional literature on Cybersecurity include the following list of best practices:

- Anti-Malware definitions need to be constantly updated to retain their effectiveness.
- Software updates need to be kept current.
- To identify external emails, message rules can be used to flag external emails and thereby decrease the probability that a user clicks on bad content.
- To thwart phishing attempts, footers can be added to incoming emails to warn about opening attachments and clicking on links (see Appendix C).
- Security training, awareness and assessment need to be routine along with testing all employees to recognize, delete and report attempted attacks (See Appendix B).
- Establishing a thorough and comprehensive backup process for all Servers using the 3-2-1 rule and establishing a separate backup process for key users' critical folders (e.g., administration, accounting, human resources) to be able to restore/recover from a secure onsite and/or offsite backup.
- Snapshots and/or image backups provide the most complete backup and the fastest recovery option.
- Consider cloud-hosting of email and other applications to provide added security, backup & restore capabilities and filtering benefits to close the largest and easiest route for Ransomware to penetrate entity systems.

FINDINGS

F1. Ransomware is a real and growing threat to public entities including those in San Mateo County.

F2. Across the country, local governments and schools represent 12% of all Ransomware attacks.

55 Government Technology Magazine, Adam Stone, *The Weakest Link*, Oct/Nov 2018

F3. The direct and indirect costs of Ransomware can be significant.

F4. Cybersecurity reviews and assessments, and an updated, well-executed Cybersecurity plan, are critical components of IT security strategy.

F5. A comprehensive Cybersecurity plan should include, at a minimum, information concerning prevention steps, spam and malware software, and backups and full recovery testing.

F6. The identification of phishing attempts, including the use of spam filters, is an important component to protecting an IT system from Ransomware attacks.

F7. Testing a full restore of a server to ensure that backups are reliable should be undertaken regularly as part an entity's backup plan to recover lost information.

F8. Training of new employees, and the recurring training of existing employees, is an important component of defense against Ransomware.

RECOMMENDATIONS

The Grand Jury recommends that each governing body undertake its own confidential effort to protect against Ransomware attacks. Specifically:

R1. 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:

1. System Security (Firewalls, Anti-malware/Antivirus software, use of subnets, strong password policies, updating/patching regularly)
2. Backup & Recovery (In the event of an attack, 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?)
3. 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)

R2. 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.

R3. Given the results of their internal reports, governmental entities may choose to request further guidance by means of a Cybersecurity review from the U.S. Department of

Homeland Security[56] and/or a cyber hygiene assessment from the County Controller's Office.[57]

R4. Given the results of their internal reports, governmental entities may choose to ask their IT departments to review their own Cybersecurity Plan with the detailed template provided by the FCC's Cybersecurity Planning Guide and consider customizing it using FCC's Create Custom Cybersecurity Planning Guide tool (see footnote 52).

METHODOLOGY

Documents

- Attack incident reports were requested from IT Departments who experienced attack(s). No incident reports were received.

Site Tours

- No site tours were performed as a part of this report.

Interviews

Reports issued by the Civil Grand Jury do not identify individuals interviewed. Penal Code Section 929 requires that reports of the Grand Jury not contain the name of any person or facts leading to the identity of any person who provides information to the Civil Grand Jury.

- Three Information Systems Managers of three different public entity IT organizations.
- Two non-public professional IT Managers. Both of these Managers' IT infrastructure environments had been infected with Ransomware attacks. One paid the ransom and the other did not.
- A professional Ransomware expert who often consults with companies who have been attacked or desire assistance preventing attacks. He also teaches classes on preparing for and preventing Ransomware attacks.
- Numerous security industry professionals at the RSA Conference held at Moscone Center in San Francisco between February 24th and 28th 2020.

BIBLIOGRAPHY

Anslinger, Joe. *"File Backup vs. Image Backup – Which is Best?"* Lieberman Technology. June 11, 2013. https://www.ltnow.com/file-backup-vs-image-backup-which-is-best/

Cisco Systems. *Ransomware - Anatomy of an Attack.* https://www.youtube.com/watch?v=4gR562GW7TI

[56] https://www.us-cert.gov/resources/assessments

[57] 2018-2019 San Mateo Grand Jury Report – Security of Election Announcements

Coveware, *"Ransomware Payments Increase In Evolving Distribution of Enterprise Ransomware Variants."* April 29, 2020. https://www.coveware.com/blog/q1-2020-ransomware-marketplace-report

Davis, Jessica. *"As Ransomware Attacks Increase, DHS Alerts to Cybersecurity Insights."* Health IT Security, September 9, 2019. https://healthitsecurity.com/news/as-ransomware-attacks-increase-dhs-alerts-to-cybersecurity-insights

Deere, Stephen. *"Confidential Report: Atlanta's Cyber Attack Could Cost Taxpayers $17 Million."* The Atlanta Journal- Constitution. August 2018.

Department of Homeland Security (DHS): Cybersecurity and Infrastructure Security Agency (CISA). *"Assessments: Cyber Resilience Review (CRR)"* https://www.us-cert.gov/resources/assessments

Duncan, Ian. *"Baltimore Estimated Cost of Ransomware Attack at $18.2 Million as Government Begins to Restore Email Accounts."* Baltimore Sun, May 29, 2019.

Epicor Corporation. *Protecting Yourself From Ransomware*. January 2020.

Fadilpasic, Sead. *"Welcome to the era of Ransomware 2.0"* ITProPortal. February 12, 2020. https://www.itproportal.com/news/welcome-to-the-era-of-ransomware-20/

Federal Communications Commission. *Cyber Security Planning Guide.* https://www.fcc.gov/cyber/cyberplanner.pdf

Gutman, Yotam. *"What is the True Cost of a Ransomware Attack."* SentinelOne. January 8, 2020. https://www.sentinelone.com/blog/what-is-the-true-cost-of-a-ransomware-attack-6-factors-to-consider/

Iloh, Raphael. *"The 3-2-1 Backup Rule and Effective Cybersecurity Strategy."* Management Wire. January 7, 2020. https://www.managementwire.com/the-3-2-1-backup-rule-and-effective-cybersecurity-strategy/

Jendre, Adrien*." Ransomware Attacks: Why Email Is Still the #1 Delivery Method."* Vade Security. January 16, 2020. https://www.vadesecure.com/en/ransomware-attacks-why-email-is-still-the-1-delivery-method/

Kass, DH. *"Average Ransomware Payment Rises Again: Research."* MSSP Alert. April 30, 2020. https://www.msspalert.com/cybersecurity-research/average-ransomware-payment-rises-again-research/

Kraft Technology Group. *"When Was The Last Time You Tested Your Business Backups?"* https://www.kraftgrp.com/when-was-the-last-time-you-tested-your-business-backups/

MailChannels. *"What is Spam Filtering?"* https://www.mailchannels.com/what-is-spam-filtering/

MIT Technology Review, *"Ransomware May Have Cost the US More Than $7.5Billion in 2019."* January 2, 2020. https://www.technologyreview.com/2020/01/02/131035/ransomware-may-have-cost-the-us-more-than-75-billion-in-2019/

National League of Cities Report. *"Protecting Our Data: What Cities Should Know About Cybersecurity."* Forward by Clarence Anthony, CEO and Executive Director.

Pearson Education. *Ubuntu Unleashed*. 2015 Edition. Page 655.

Ranger, Steve. *"What is cloud computing? Everything you need to know about the cloud explained."* ZD Net, December 13, 2018. https://www.zdnet.com/article/what-is-cloud-computing-everything-you-need-to-know-from-public-and-private-cloud-to-software-as-a/

Samani, Raj. *"Ransomware – Mitigating the Threat of Cyber Security Attacks."* Zerto. 2019. https://www.zerto.com/wp-content/uploads/2019/09/ransomware-mitigating-the-threat-of-cyber-security-attacks.pdf

San Mateo Grand Jury Report. *Security of Election Announcements*. 2018-2019.

Search Networking, *"Protocols, Lesson 6: IP subnetting - The basic concepts."* October 2004. https://searchnetworking.techtarget.com/tutorial/Protocols-Lesson-6-IP-subnetting-The-basic-concepts

Sheehan, Patrick. *"Cascading Effects of Cyber Security on Ohio."* Ohio Emergency Management Agency. September 19, 2012.

Stone, Adam. *The Weakest Link.* Government Technology Magazine, October/November 2018.

Trend Micro. *"Online Phishing: How To Stay Out Of The Hackers' Nets"* November 20, 2019. https://blog.trendmicro.com/online-phishing-how-to-stay-out-of-the-hackers-nets/

Wu, David. *"UCSF pays $1.14 Million Ransom to Recover Data."* San Jose Mercury News. July 4, 2020.

APPENDIX A – SURVEY QUESTIONS

1. Has your Organization had a Ransomware attack? Specifically, has there been an instance or multiple instances when an attack has locked up a computer or computers and presented a demand for ransom to unlock the infection?

If you answered Yes or Possibly to Question 1, please provide a detailed description of the attack. What actions were taken once the attack was realized?

2. Is your Information Systems Budget adequate to secure your network properly from malicious attack?

3. Please provide an explanation of your Systems Backup processes? How often are backups run, where do you store the Backups?

4. Have you ever had to Restore from Backups? Please describe in detail why you did the Restore and describe the process used.

5. Do you provide training to employees regarding Malware?

6. What defenses do you currently employ to block malware? Please be specific. (Firewall brand/model, Software filters/spam blocker, etc.)

APPENDIX B – EMPLOYEE TRAINING OPTIONS

Phishing is the primary method of entry in cyber-attacks worldwide. Over the past few years, some security industry companies have come up with excellent testing, training, monitoring, measuring and reporting solution to help with employee training. The primary goal of an employee training program is to change user's behavior when viewing emails that might contain threats.

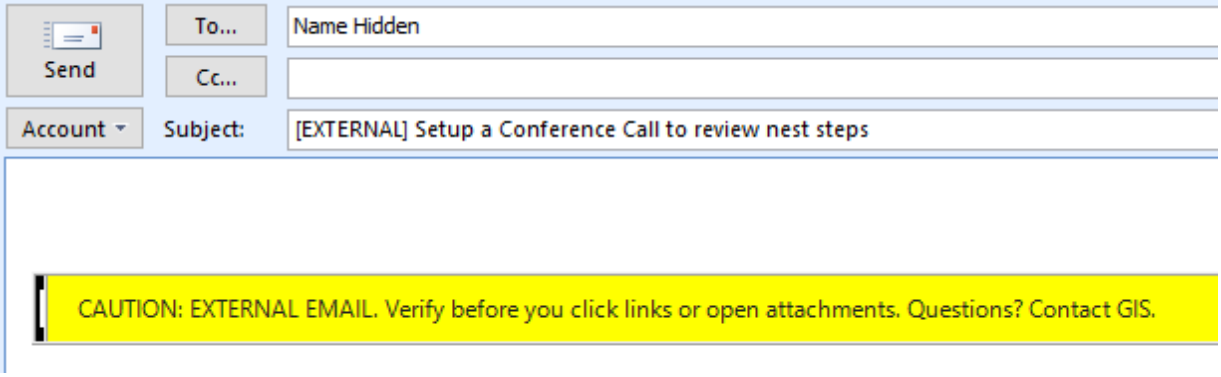
The typical components of these solutions include:

- Customized phishing attacks designed to test employees in spotting attack attempts
- Provide users a simple to use reporting tool to flag suspected attacks
- An incidence response platform for controlling the spread of an attack
- Reporting dashboards tracking user click-throughs
- Employee training programs

Here are some website links for the companies offering training solutions.
www.knowbe4.com
www.lucysecurity.com
www.metacompliance.com
www.mediapro.com
www.cofense.com
www.elevatesecurity.com
www.securitymentor.com

www.habitu8.io

APPENDIX C – EMAIL MESSAGE RULE - EXTERNAL



APPENDIX D – BACKUP & RECOVERY APPLIANCES & SERVICES

There are a large number of companies that provide Backup and Recovery solutions. Solutions Review has prepared a buyer's guide for the leading vendors. Click on the following link or copy and paste this URL into a browser to get your own copy of this guide.

https://solutionsreview.com/backup-disaster-recovery/get-a-free-backup-and-disaster-recovery-buyers-guide/

Specifically, some of the vendors in this report do not provide appliances, only virtual server support. Here is a partial list of appliance and solution vendors:

www.unitrends.com
www.barracuda.com
www.carbonite.com
www.commvault.com
www.dellemc.com
www.axcient.com
www.cohesity.com
www.datto.com
www.infrascale.com

APPENDIX E – PHISHING DEFENSE VENDORS

Some companies that provide solutions that improve email defenses are:

https://www.opswat.com/products/metadefender/email-gateway-security
https://www.agari.com/products/phishing-defense/
https://www.inky.com/anti-phishing-software
https://www.mimecast.com/products/email-security-with-targeted-threat-protection/

APPENDIX F: PUBLIC ENTITIES IN SAN MATEO COUNTY (68)

City/Town Governments (20)

Town of Atherton
City of Belmont
City of Brisbane
City of Burlingame
City of Colma
City of Daly City
City of East Palo Alto
City of Foster City
City of Half Moon Bay
City of Hillsborough
City of Menlo Park
City of Millbrae
City of Pacifica
Town of Portola Valley
City of Redwood City
City of San Bruno
City of San Carlos
City of San Mateo
City of South San Francisco
Town of Woodside

County Government (1)

County of San Mateo, Information Services Department

School Districts (25)

Bayshore Elementary School District
Belmont Redwood Shores School District
Brisbane School District
Burlingame School District
Cabrillo Unified School District
Hillsborough City School District
Jefferson Elementary School District
Jefferson Union High School District
La Honda Pescadero School District
Las Lomitas Elementary School District
Menlo Park City School District
Millbrae School District
Pacifica School District
Portola Valley School District
Ravenswood City School District
Redwood City School District
San Bruno Park School District
San Carlos School District

San Mateo Foster City School District
San Mateo Union High School District
Sequoia Union High School District
San Mateo County Community College School District
San Mateo County Office of Education
South San Francsico Unified School District
Woodside School District

Independent Special Districts (22)
Bayshore Sanitary District
Broadmoor Police Protection District
Coastside County Water District
Coastside Fire Protection District
Colma Fire Protection District
East Palo Alto Sanitary District
Granada Community Services District
Highlands Recreation District
Ladera Recreation District
Menlo Park Fire Protection District
Mid Peninsula Regional Open Space District
Mid-Peninsula Water District
Montara Water and Sanitary District
North Coast County Water District
Peninsula Health Care District
San Mateo County Harbor District
San Mateo County Mosquito and Vector Control District
San Mateo County Resource Conservation District
Sequoia Healthcare
West Bay Sanitary District
Westborough Water District
Woodside Fire Protection District

Not Included: County-governed special districts and subsidiary special districts governed by their respective city councils.

Issued: October 7, 2020

155 ORIENTE ST.
DALY CITY, CA 94014
Phone:415.467.5443
Fax:415.467.1542
www.thebayshoreschool.org

December 16, 2020

Via Email (grandjury@sanmateocourt.org)

The Honorable Danny Y. Chou
Judge of the Superior Court
c/o Jenarda Dubois
Hall of Justice
400 County Center; 2nd Floor
Redwood City, CA 94063-1655

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

Dear Judge Chou:

The Bayshore Elementary School District (the "District") has received and reviewed the 2019-2020 Grand Jury Report entitled "Ransomware: It Is Not Enough To Think You Are Protected." We appreciate the Grand Jury's interest in this matter. Having reviewed and considered the Grand Jury's Findings and Recommendations, the District responds below pursuant to section 933.05 of the California Penal Code.

Please be advised that the District presented the Grand Jury Report to its Board of Trustees, and the District's Board approved these responses, on Tuesday, December 15, 2020.

Findings:

1. *Ransomware is a real and growing threat to public entities including those in San Mateo County.*

   The District agrees with this Finding.

2. *Across the country, local governments and schools represent 12% of all Ransomware attacks.*

   The District lacks information to fully agree or disagree with this Finding given that it did not conduct the research related to this Report. The District, however, accepts the Grand Jury's Finding for the purposes of this Response.

3. *The direct and indirect costs of Ransomware can be significant.*

   The District agrees with this Finding.

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

The District agrees with this Finding.

5. *A comprehensive Cybersecurity 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.

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.

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

   The District lacks information to fully agree or disagree with this Finding given that it did not conduct the research related to this Report. The District, however, accepts the Grand Jury's Finding for the purposes of this Response.

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.

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 attack, 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)*

      The District implemented this Recommendation on December 9, 2020 by directing the District's IT Department to prepare a confidential report [A1] which addresses the three concerns specifically identified above.

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 this Recommendation, 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.

3. *Given the results of their internal reports, governmental entities may choose to request further guidance by means of a Cybersecurity review from the U.S. Department of Homeland Security and/or a cyber hygiene assessment from the County Controller's Office.*

   The District will implement [A2] this Recommendation if warranted and appropriate based on the results of the District's confidential internal report.

4. *Given the results of their internal reports, governmental entities may choose to ask their IT departments to review their own Cybersecurity Plan with the detailed template provided by the FCC's Cybersecurity Planning Guide and consider customizing it using FCC's Create Custom Cybersecurity Planning Guide tool (see footnote 52).*

   The District will implement [A3] this Recommendation if warranted and appropriate based on the results of the District's confidential internal report.

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

Sincerely,

Audra Pittman, Ph.D.
Superintendent
Bayshore Elementary School District

Bayshore Sanitary District

36 INDUSTRIAL WAY
BRISBANE, CALIFORNIA 94005
(415) 467-1144

December 4, 2020

Hon. Danny Y. Chou
Judge of the Superior Court
c/o Jenarda Dubois
Hall of Justice
400 County Center, 8th Floor
Redwood City, CA 94063-1655

Re.: Response to Grand Jury Report "Ransomware: It Is Not Enough To Think You Are Protected"

Hon. Judge Chou:

The following response approved by the District Board at their November 19, 2020 is presented in two sections. The first is our response to the Findings and the second provides our responses to the Recommendations.

Findings

F1. We agree with the finding.
F2. We neither agree nor disagree with this finding since we have no independent knowledge.
F3. We neither agree nor disagree with this finding since we have no independent knowledge.
F4. We agree with the finding.
F5. We agree with the finding.
F6. We agree with the finding.
F7. We agree with the finding.
F8. In general we agree with the finding.

Recommendations

R1. 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:

1. System Security (Firewalls, Anti-malware/Antivirus software, use of subnets, strong password policies updating/patching regularly)

Response: *The recommendation will not be implemented because it is not warranted or reasonable. The District does not have an IT department, there is no District shared network drive and no District email platform. Engineering, administrative, legal and operations and maintenance services are accomplished by contract staff. Those individuals and/or firms maintain their own computer systems. The District does have a computer protected with Norton 360 Premium and Malwarebytes. However, any document stored in the computer is also available via paper and/or maintained by contract staff.*

2. Backup & Recovery (In the event of an attack, 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?)

Response: *The recommendation will not be implemented because it is not warranted or reasonable. The District does not have an IT department, there is no District shared network drive, server and no District email platform. However, the content of the material on the District's computer is backed up to a flash drive.*

3. 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)

Response: *The recommendation will not be implemented because it is not warranted or reasonable. The District does not have an IT department, there is no District shared network drive, no District email platform and no employees..*

R2. 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.

Response: *This recommendation will not be implemented because it is not warranted or reasonable since the District has no IT department or IT function.*

R3. Given the results of their internal reports, governmental entities may choose to request further guidance by means of a Cybersecurity review from the U.S. Department of Homeland Security and/or a cyber hygiene assessment from the County controller's Office.

Response: *This recommendation will not be implemented because it is not warranted or reasonable since the District has no IT department or IT function.*

R4. Given the results of their internal reports, governmental entities may choose to ask their IT departments to review their own Cybersecurity Plan with the detailed template

provided by the FCC's Cybersecurity Planning Guide and consider customizing it using FCC's Create Custom Cybersecurity Planning Guide tool.

Response: *This recommendation will not be implemented because it is not warranted or reasonable since the District has no IT department or IT function.*

Sincerely,

Iris Gallagher

Iris Gallager, President
Board of Directors

j

November 9, 2020

Via Email (grandjury@sanmateocourt.org)

The Honorable Danny Y. Chou
Judge of the Superior Court
c/o Jenarda Dubois
Hall of Justice
400 County Center; 2nd Floor
Redwood City, CA 94063-1655

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

Dear Judge Chou:

The Belmont-Redwood Shores School District (the "District") has received and reviewed the 2019-2020 Grand Jury Report entitled "Ransomware: It Is Not Enough To Think You Are Protected." We appreciate the Grand Jury's interest in this matter. Having reviewed and considered the Grand Jury's Findings and Recommendations, the District responds below pursuant to section 933.05 of the California Penal Code.

Please be advised that the District presented the Grand Jury Report to its Board of Trustees, and the District's Board approved these responses, on November 9, 2020.

Findings:

1. Ransomware is a real and growing threat to public entities including those in San Mateo County.

The District agrees with this Finding.

2. Across the country, local governments and schools represent 12% of all Ransomware attacks.

The District lacks information to fully agree or disagree with this Finding given that it did not conduct the research related to this Report. The District, however, accepts the Grand Jury's Finding for the purposes of this Response.

3. The direct and indirect costs of Ransomware can be significant.

The District agrees with this Finding.

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

The District agrees with this Finding.

5. A comprehensive Cybersecurity 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.

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.

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 lacks information to fully agree or disagree with this Finding given that it did not conduct the research related to this Report. The District, however, accepts the Grand Jury's Finding for the purposes of this Response.

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.

<u>Recommendations:</u>

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:

> ***1. System Security (Firewalls, Anti-malware/Antivirus software, use of subnets, strong password policies, updating/patching regularly)***
>
> ***2. Backup & Recovery (In the event of an attack, 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?)***
>
> ***3. 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)***

The District implemented this Recommendation on October 23, 2020 by directing the District's IT Department to prepare a confidential report [A1] which addresses the three concerns specifically identified above.

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 this Recommendation, 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.

3. Given the results of their internal reports, governmental entities may choose to request further guidance by means of a Cybersecurity review from the U.S. Department of Homeland Security and/or a cyber hygiene assessment from the County Controller's Office.

The District will implement [A2] this Recommendation if warranted and appropriate based on the results of the District's confidential internal report.

4. Given the results of their internal reports, governmental entities may choose to ask their IT departments to review their own Cybersecurity Plan with the detailed template provided by the FCC's Cybersecurity Planning Guide and consider customizing it using FCC's Create Custom Cybersecurity Planning Guide tool (see footnote 52).

The District will implement [A3] this Recommendation if warranted and appropriate based on the results of the District's confidential internal report.

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

Sincerely,

Dan Deguara
Superintendent

December 16, 2020

The Honorable Danny Y. Chou
Judge of the Superior Court
c/o Jenarda Dubois
Hall of Justice
400 County Center, 2nd Floor
Redwood City, CA 94063-1655

Via Email (grandjury@sanmateocourt.org)

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

Dear Judge Chou:

The Brisbane School District has received and reviewed the 2019-2020 Grand Jury Report entitled "Ransomware: It Is Not Enough to Think You Are Protected." The District appreciates the Grand Jury's interest in this matter.

Having reviewed and considered the Grand Jury's Findings and Recommendations, the District responds as follows, pursuant to section 933.05 of the California Penal Code.

FINDINGS:

F1. *Ransomware is a real and growing threat to public entities including those in San Mateo County.*

The District agrees with this Finding.

F2. *Across the country, local governments and schools represent 12% of all Ransomware attacks.*

The District lacks information to fully agree or disagree with this Finding given that it did not conduct the research related to this Report. The District, however, accepts the Grand Jury's Finding for the purposes of this Response.

F3. *The direct and indirect costs of Ransomware can be significant.*

The District agrees with this Finding.

F4. *Cybersecurity reviews and assessments, and an updated, well-executed Cybersecurity plan, are critical components of IT security strategy.*

The District agrees with this Finding.

F5. *A comprehensive Cybersecurity 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.

F6. *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.

F7. *Testing a full restore of a server to ensure that backups are reliable should be undertaken regularly as part an entity's backup plan to recover lost information.*

The District lacks information to fully agree or disagree with this Finding given that it did not conduct the research related to this Report. The District, however, accepts the Grand Jury's Finding for the purposes of this Response.

F8. *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.

RECOMMENDATIONS:

R1. *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:*

1. *System Security (Firewalls, Anti-malware/Antivirus software, use of subnets, strong password policies, updating/patching regularly)*
2. *Backup & Recovery (In the event of an attack, 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?)*
3. *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)*

The District implemented this Recommendation on November 30, 2020 by directing the district's IT staff to prepare a confidential report which addresses the three concerns specifically identified above.

R2. *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 this Recommendation, 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.

R3. *Given the results of their internal reports, governmental entities may choose to request further guidance by means of a Cybersecurity review from the U.S. Department of Homeland Security and/or a cyber hygiene assessment from the County Controller's Office.*

The District will implement this Recommendation if warranted and appropriate based on the results of the District's confidential internal report.

R4. *Given the results of their internal reports, governmental entities may choose to ask their IT departments to review their own Cybersecurity Plan with the detailed template provided by the FCC's Cybersecurity Planning Guide and consider customizing it using FCC's Create Custom Cybersecurity Planning Guide tool (see footnote 52).*

The District will implement this Recommendation if warranted and appropriate based on the results of the District's confidential internal report.

Should there be additional questions or information needed as pertaining to the District's response to this report, please do not hesitate to contact me.

Sincerely,

Ronan Collver
Superintendent

MICHAEL P .CONNOLLY
CHIEF OF POLICE

BROADMOOR POLICE DEPARTMENT

May 3, 2021

Hon. Danny Y. Chou
Judge of the Superior Court
c/o Jenarda Dubois
Hall of Justice
400 County Center, 8th Floor
Redwood City, CA 94063-1655

Re: Grand Jury Report: "Ransomware: It Is Not Enough to Think You Are Protected"

Dear Judge Chou:

The District of Broadmoor hereby submits the following response tot eh Grand Jury report filed on October 7, 2020. The following is in response to the findings and recommendations as it pertains to the District. These responses were approved by the District Manager on April 30, 2021.

The District of Broadmoor concurs with the findings in the Grand Jury report that ransomware is a significant threat to the District network infrastructure and a cybersecurity plan must be in place to prevent attacks; but more importantly recover from an attack.

The Broadmoor Police Department has protected its network in layers with its partner, Nevtec. The Broadmoor Police Department is working with our Managed Service Provider, Nevtec. Please see attached supporting documentation.

Sincerely,

Michael P. Connolly
Chief of Police

388 EIGHTY EIGHTH STREET • BROADMOOR, CA 94015-1717 • (650) 755-3840 • FAX (650)755-9732

Findings:

1. Ransomware is a real and growing threat to public entities including those in San Mateo County.
   The BMPD agrees with this Finding.
2. Across the country, local governments and schools represent 12% of all Ransomware attacks.
   The BMPD lacks information to fully agree or disagree with this Finding given that it did not conduct the research related to this Report. The BMPD, however, accepts the Grand Jury's Finding for the purposes of this Response.
3. The direct and indirect costs of Ransomware can be significant.
   The BMPD agrees with this Finding.
4. Cybersecurity reviews and assessments, and an updated, well-executed Cybersecurity plan, are critical components of IT security strategy.
   The BMPD agrees with this Finding.
5. A comprehensive Cybersecurity plan should include, at a minimum, information concerning prevention steps, spam and malware software, and backups and full recovery testing.
   The BMPD agrees with this Finding.
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 BMPD agrees with this Finding.
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 BMPD lacks information to fully agree or disagree with this Finding given that it did not conduct the research related to this Report. The BMPD, however, accepts the Grand Jury's Finding for the purposes of this Response.
8. Training of new employees, and the recurring training of existing employees, is an important component of defense against Ransomware.
   The BMPD agrees with this Finding.

Recommendations

The Grand Jury recommends that each governing body undertake its own confidential effort to protect against Ransomware attacks. Specifically:

R1. 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:

1. System Security (Firewalls, Anti-malware/Antivirus software, use of subnets, strong password policies, updating/patching regularly)

The BMPD has protected its network in layers with its partner, Nevtec. The PD utilizes a next generation SonicWALL firewall with unified threat management services (Advanced Gateway Security Services) to inspect all traffic coming in and going out of the network at the gateway (the Firewall). Services include IPS, Gateway AntiVirus & AntiSpyware, Content Filtering, Application Intelligence & Control, and Advanced Threat Protection services.

All servers and computers are protected with Endpoint Protection with Zero Day Threat Services. AntiVirus is not good enough. The solution includes EndPoint Detection & Response (EDR) and a Managed Threat Response (MTR) solution. MTR goes further than EDR by utilizing a team of threat hunters to protect the network 24x7.

Best practices are in place for a strong password policy and for patch management. The BMPD currently has a flat network (multiple subnets do not exist) and is currently reviewing implementing subnets.

2. Backup & Recovery (In the event of an attack, 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?)

The BMPD has backup and recovery solution in place. Servers are backed up on daily basis with snapshots. 7 revisions are saved on a rotating basis with the oldest being overridden by the newest. Data/the backups are being stored offsite, separate from the BMPD network. Currently the BMPD does not have a local repository for backups but is considering a solution suggest by its IT Partner.

3. 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)

The BMPD utilizes Microsoft 365 and the built in spam filtering in MS 365. The BMPD is considering a more robust AntiSpam solution and a monthly email phishing program. BMPD's IT partner, Nevtec, provides an annual Security Awareness training for the staff. New emails sent from outside the BMPD are marked as External to help staff identify phishing attempts. Suspected phishing emails are submitted to the BMPD's IT partner for review.

R2. 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 BMPD will provide these reports by June 20,2021

R3. Given the results of their internal reports, governmental entities may choose to request further guidance by means of a Cybersecurity review from the U.S. Department of 2019-2020 San Mateo County Civil Grand Jury 14 Homeland Security56 and/or a cyber hygiene assessment from the County Controller's Office.57

The BMPD will study the results and determine what actions are needed by June 20, 2021

R4. Given the results of their internal reports, governmental entities may choose to ask their IT departments to review their own Cybersecurity Plan with the detailed template provided by the FCC's Cybersecurity Planning Guide and consider customizing it using FCC's Create Custom Cybersecurity Planning Guide tool (see footnote 52).

The BMPD will implement this Recommendation if warranted and appropriate based on the results of the District's confidential internal report.

1. Has your Organization had a Ransomware attack? Specifically, has there been an instance or multiple instances when an attack has locked up a computer or computers and presented a demand for ransom to unlock the infection? If you answered Yes or Possibly to Question 1, please provide a detailed description of the attack. What actions were taken once the attack was realized?

2. Is your Information Systems Budget adequate to secure your network properly from malicious attack?

3. Please provide an explanation of your Systems Backup processes? How often are backups run, where do you store the Backups?

4. Have you ever had to Restore from Backups? Please describe in detail why you did the Restore and describe the process used.

5. Do you provide training to employees regarding Malware?
6. What defenses do you currently employ to block malware? Please be specific. (Firewall brand/model, Software filters/spam blocker, etc.)

Burlingame School District
Leaders. Thinkers. Creators.

November 10, 2020

Via Email (grandjury@sanmateocourt.org)

The Honorable Danny Y. Chou
Judge of the Superior Court
c/o Jenarda Dubois
Hall of Justice
400 County Center; 2nd Floor
Redwood City, CA 94063-1655

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

Dear Judge Chou:

The Burlingame School District (the "District") has received and reviewed the 2019-2020 Grand Jury Report entitled "Ransomware: It Is Not Enough To Think You Are Protected." We appreciate the Grand Jury's interest in this matter. Having reviewed and considered the Grand Jury's Findings and Recommendations, the District responds below pursuant to section 933.05 of the California Penal Code.

Please be advised that the District presented the Grand Jury Report to its Board of Trustees, and the District's Board approved these responses, on November 10, 2020

Findings:

1. *Ransomware is a real and growing threat to public entities including those in San Mateo County.*

The District agrees with this Finding.

2. *Across the country, local governments and schools represent 12% of all Ransomware attacks.*

The District lacks information to fully agree or disagree with this Finding given that it did not conduct the research related to this Report. The District, however, accepts the Grand Jury's Finding for the purposes of this Response.

3. *The direct and indirect costs of Ransomware can be significant.*

The District agrees with this Finding.

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

The District agrees with this Finding.

5. *A comprehensive Cybersecurity 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.

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.

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

The District lacks information to fully agree or disagree with this Finding given that it did not conduct the research related to this Report. The District, however, accepts the Grand Jury's Finding for the purposes of this Response.

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.

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:*
    1. *System Security (Firewalls, Anti-malware/Antivirus software, use of subnets, strong password policies, updating/patching regularly)*
    2. *Backup & Recovery (In the event of an attack, 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?)*
    3. *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)*

The District implemented this Recommendation on November 10, 2020 by directing the District's IT Department to prepare a confidential report which addresses the three concerns specifically identified above.

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 this Recommendation, 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.

3. *Given the results of their internal reports, governmental entities may choose to request further guidance by means of a Cybersecurity review from the U.S. Department of Homeland Security and/or a cyber hygiene assessment from the County Controller's Office.*

The District will implement this Recommendation if warranted and appropriate based on the results of the District's confidential internal report.

4. *Given the results of their internal reports, governmental entities may choose to ask their IT departments to review their own Cybersecurity Plan with the detailed template provided by the FCC's Cybersecurity Planning Guide and consider customizing it using FCC's Create Custom Cybersecurity Planning Guide tool (see footnote 52).*

The District will implement this Recommendation if warranted and appropriate based on the results of the District's confidential internal report.

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

Sincerely,

Chris Mount-Benites
Superintendent
Burlingame School District

CABRILLO UNIFIED SCHOOL DISTRICT

498 Kelly Avenue, Half Moon Bay, California 94019 • 650 712-7100 • Fax 650 726-0279 • www.cabrillo.k12.ca.us

SUPERINTENDENT
Sean McPhetridge, Ed.D.

GOVERNING BOARD
Mary Beth Alexander
Lizet Cortes
Kimberly Hines
Sophia Layne
Freya McCamant

November 13, 2020

Via Email (grandjury@sanmateocourt.org)

The Honorable Danny Y. Chou
Judge of the Superior Court
c/o Jenarda Dubois
Hall of Justice
400 County Center; 2nd Floor
Redwood City, California 94063-1655

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

Dear Judge Chou:

The Cabrillo Unified School District (the "District") has received and reviewed the 2019-2020 Grand Jury Report entitled "Ransomware: It Is Not Enough To Think You Are Protected." We appreciate the Grand Jury's interest in this matter. Having reviewed and considered the Grand Jury's Findings and Recommendations, the District responds below pursuant to section 933.05 of the California Penal Code.

Please be advised that the District presented the Grand Jury Report to its Board of Trustees, and the District's Board approved these responses, on November 12, 2020.

Findings:

1. *Ransomware is a real and growing threat to public entities including those in San Mateo County.*

The District agrees with this Finding.

2. *Across the country, local governments and schools represent 12% of all Ransomware attacks.*

The District lacks information to fully agree or disagree with this Finding given that it did not conduct the research related to this Report. The District, however, accepts the Grand Jury's Finding for the purposes of this Response.

3. *The direct and indirect costs of Ransomware can be significant.*

The District agrees with this Finding.

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

The District agrees with this Finding.

5. *A comprehensive Cybersecurity 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.

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.

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

The District lacks information to fully agree or disagree with this Finding given that it did not conduct the research related to this Report. The District, however, accepts the Grand Jury's Finding for the purposes of this Response. Please note IT staff in CUSD currently maintain redundant servers at geographically disbursed locations, allowing the District to perform selective server restores of user data as part of our backup plan to recover lost information.

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.

Recommendations:

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:

1. *System Security (Firewalls, Anti-malware/Antivirus software, use of subnets, strong password policies, updating/patching regularly)*
2. *Backup & Recovery (In the event of an attack, 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?)*
3. *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)*

The District implemented this Recommendation on October 21, 2020 by directing the District's IT Department to prepare a confidential report addressing concerns specifically identified above.

1. *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 this Recommendation, 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.

2. *Given the results of their internal reports, governmental entities may choose to request further guidance by means of a Cybersecurity review from the U.S. Department of Homeland Security and/or a cyber hygiene assessment from the County Controller's Office.*

The District will implement this Recommendation if warranted and appropriate based on the results of the District's confidential internal report.

3. *Given the results of their internal reports, governmental entities may choose to ask their IT departments to review their own Cybersecurity Plan with the detailed template provided by the FCC's Cybersecurity Planning Guide and consider customizing it using FCC's Create Custom Cybersecurity Planning Guide tool (see footnote 52).*

The District will implement this Recommendation if warranted and appropriate based on the results of the District's confidential internal report. Meanwhile, please know CUSD has already developed a training to review cybersecurity protocols with employees in our organization.

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

Sincerely,

Sean McPhetridge, Ed.D.
Superintendent
Cabrillo Unified School District

12 November 2020

Hon. Danny Y. Chou
Judge of the Superior Court
c/o Jenarda Dubois
Hall of Justice
400 County Center; 8th Floor
Redwood City, CA 94063-1655

RESPONSE TO GRAND JURY REPORT: "Ransomware: It Is Not Enough To Think You Are Protected"

Honorable Judge Chou,

Thank you for the opportunity to review and comment on the above referenced Grand Jury Report filed on October 7, 2020. The City of Belmont's response to both the findings and recommendations are listed below.

Response to Grand Jury Findings:

F1. Ransomware is a real and growing threat to public entities including those in Belmont County.
Response: The City of Belmont agrees with this finding

F2. Across the country, local governments and schools represent 12% of all Ransomware attacks.
Response: The City of Belmont agrees with this finding

F3. The direct and indirect costs of Ransomware can be significant.
Response: The City of Belmont agrees with this finding.

F4. Cybersecurity reviews and assessments, and an updated, well-executed Cybersecurity plan, are critical components of IT security strategy.
Response: The City of Belmont agrees with this finding.

F5. A comprehensive Cybersecurity plan should include, at a minimum, information concerning prevention steps, spam and malware software, and backups and full recovery testing.
Response: The City of Belmont agrees with this finding.

F6. The identification of phishing attempts, including the use of spam filters, is an important component to protecting an IT system from Ransomware attacks.
Response: The City of Belmont agrees with this finding.

F7. Testing a full restore of a server to ensure that backups are reliable should be undertaken regularly as part an entity's backup plan to recover lost information.
Response: The City of Belmont agrees with this finding.

F8. Training of new employees, and the recurring training of existing employees, is an important component of defense against Ransomware.
Response: The City of Belmont agrees with this finding.

Response to Grand Jury Recommendations:

The Grand Jury recommends that each governing body undertake its own confidential effort to protect against Ransomware attacks. Specifically:

R1. 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:

1. System Security (Firewalls, Anti-malware/Antivirus software, use of subnets, strong password policies, updating/patching regularly)
2. Backup & Recovery (In the event of an attack, 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?)
3. 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)

Response: This recommendation has been implemented
The Belmont City Manager's Office made this request of the City's IT Department upon receipt of the Grand Jury Report. The IT Department will prepare a report for council which will, at a minimum, address the concerns listed in R1.1, R1.2, and R1.3.

R2. 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.

Response: This recommendation will be implemented by the June deadline

The City of Belmont's IT department will prepare a comprehensive report for City Council, planned for Q1 calendar year 2021, that addresses the concerns identified in the report. This report will include actions taken and plans for future enhancements.

R3. Given the results of their internal reports, governmental entities may choose to request further guidance by means of a Cybersecurity review from the U.S. Department of Homeland Security and/or a cyber hygiene assessment from the County Controller's Office.

Response: This recommendation will be implemented on or before June 30, 2021

The City of Belmont IT Department will make a request with the Department of Homeland Security, Cybersecurity & Infrastructure Security Agency, for cyber-hygiene services before June 30, 2021.

R4. Given the results of their internal reports, governmental entities may choose to ask their IT departments to review their own Cybersecurity Plan with the detailed template provided by the FCC's Cybersecurity Planning Guide and consider customizing it using FCC's Create Custom Cybersecurity Planning Guide tool (see footnote 52).

Response: This recommendation will be implemented on or before June 30, 2021

The City of Belmont IT Department will utilize the Federal Communications Commission Cyber Security Planning Guide and the FCC Cyber Security Planner to review and update our cyber-security plans. This work will be completed on or before June 30, 2021.

This response to the Grand Jury was approved at a public meeting on November 10, 2020.

Respectfully,

John D. Jones, Jr., CGCIO, PMP
Information Technology Director

CITY OF BRISBANE

50 Park Place
Brisbane, California 94005-1310
(415) 508-2100
Fax (415) 467-4989

December 16, 2020

Hon. Danny Y. Chou
Judge of the Superior Court
c/o Jenarda Dubois
HaU of Justice
400 County Center; 8th Floor
Redwood City, CA 94063-1655.

Re: Grand Jury Report: "Ransomware: It Is Not Enough To Think You Are Protected"

Dear Honorable Danny Y. Chou:

This letter is in response to the 2019-2020 Grand Jury filed a report on October 7, 2020, titled "Ransomware: It Is Not Enough To Think You Are Protected," which contained findings that pertain to the City of Brisbane.

Listed below are the Jury's findings and recommendations followed by the City of Brisbane response in bold. The Brisbane City Council reviewed and approved the below recommendations at a public meeting on November 19, 2020. The City of Brisbane responds to the Grand Jury's findings, conclusions and recommendations as follows:

The San Mateo County 2019-2020Grand Jury makes the following findings to the City Councils of the cities of San Mateo County:

F1. Ransomware is a real and growing threat to public entities including those in San Mateo County. **AGREE**

F2. Across the country, local governments and schools represent 12% of all Ransomware attacks. **The City has no reason to disagree with this finding**

F3. The direct and indirect costs of Ransomware can be significant. **AGREE**

F4. Cybersecurity reviews and assessments, and an updated, and well-executed Cybersecurity plan, are critical components of IT security strategy. **AGREE**

F5. A comprehensive Cybersecurity plan should include, at a minimum, information concerning prevention steps, spam and malware software, and backups and full recovery testing. **AGREE**

F6. The identification of phishing attempts, including the use of spam filters, is an important component to protecting an IT system from Ransomware attacks. **AGREE**

F7. Testing a full restore of a server to ensure that backups are reliable should be taken regularly as part of an entity's backup plan to recover lost information. **AGREE**

F8. Training new employees, and the recurring training of existing employees, is an important component of defense against Ransomware. **AGREE**

Recommendations from the Grand Jury

R1. 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:
1. System Security (Firewalls, Anti-malware/Antivirus software, use of subnets, strong password policies, updating/patching regularly)
2. Backup & Recovery (In the event of an attack, 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?)
3. 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).

The city uses two outside entities to assist with the security of its IT infrastructure NevTec and Endsight. The City will be requesting the firms to provide a report that details the information outlined above. The report will be completed prior to June 30, 2021.

R2. These confidential internal reports should be provided to the governing body by June 30, 2021. This report should describe what actions have all ready been taken and which will be given timely consideration for future enhancements to the existing cybersecurity plan.

The City will provide these reports to the City Council by June 30, 2021.

R3. Given the results of their internal reports, governmental entities may choose to request further guidance by means of a Cybersecurity review from the U.S. Department of Homeland Security5 6 and/or a cyber-hygiene assessment from the County Controller's Office.

The City will study and discuss the results to determine the next steps.

R4. Given the results of their internal reports, governmental entities may choose to ask their- IT departments to review their own Cybersecurity Plan with the detailed template provided by the FCC's Cybersecurity Planning Guide and consider customizing it using FCC's Create Custom Cybersecurity Planning Guide tool.

On behalf of the City of Brisbane, I would like to thank the members of the Grand Jury for their efforts.

Sincerely,

Terry O'Connell
Mayor, City of Brisbane

CC: San Mateo County Grand Jury
Brisbane City Clerk

The City of Burlingame

TEL: (650) 558-7200
FAX: (650) 566-9282
www.burlingame.org

CITY HALL -- 501 PRIMROSE ROAD
BURLINGAME, CALIFORNIA 94010-3997

December 7, 2020

Honorable Danny Y. Chou
Judge of the Superior Court
c/o Jenarda Dubois
Hall of Justice
400 County Center, 2nd Floor
Redwood City, CA 94063-1655

Subject: City of Burlingame's response to 2019-2020 Civil Grand Jury Report entitled "Cybersecurity – It Is Not Enough To Think you Are Protected"

Dear Judge Chou:

After reviewing the 2019-2020 Grand Jury report entitled "Cybersecurity – It Is Not Enough To Think you Are Protected," the following are the City of Burlingame's responses to the Grand Jury's findings:

F1. Ransomware is a real and growing threat to public entities including those in San Mateo County.

Response: The City of Burlingame agrees with this finding.

F2. Across the country, local governments and schools represent 12% of all Ransomware attacks.

Response: The City of Burlingame agrees with this finding, although no effort was made to substantiate the actual statistic.

F3. The direct and indirect costs of Ransomware can be significant.

Response: The City of Burlingame agrees with this finding.

F4. Cybersecurity reviews and assessments, and an updated well-executed Cybersecurity plan, are critical components of IT security strategy.

Response: The City of Burlingame agrees with this finding.

F5. A comprehensive Cybersecurity plan should include, at a minimum, information concerning prevention steps, spam and malware software, and backups and full recovery testing.

Response: The City of Burlingame agrees with this finding.

F6. The identification of phishing attempts, including the use of spam filters, is an important component to protecting an IT system from Ransomware attacks.

Response: The City of Burlingame agrees with this finding.

F7. Testing a full restore of a server to ensure that backups are reliable should be undertaken regularly as part an entity's backup plan to recover lost information.

Response: The City of Burlingame agrees with this finding.

F8. Training of new employees, and the recurring training of existing employees, is an important component of defense against Ransomware.

Response: The City of Burlingame agrees with this finding.

The following are the City of Burlingame's responses to the Grand Jury's recommendations:

R1. 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:

Response: The City of Burlingame requested a written response to this recommendation from its IT management team, in lieu of a separate report addressing these concerns, so that management could develop a response to the final three recommendations of the report.

1. **System Security (Firewalls, Anti-malware/Antivirus software, use of subnets, strong password policies, updating/patching regularly)**

   The City of Burlingame utilizes several strategies to protect against nefarious acts including but not limited to:
   - Industry recognized leaders' dedicated firewall appliances at all electronic entry points into the City. On each firewall, all ports are blocked by default. Only known needed ports are opened, thus limiting the type of traffic coming into the City network infrastructure.
   - All servers and desktops run an industry leader endpoint protection software, which is automatically updated. It provides key protections including: endpoint detection and response (EDR), which detects and investigates suspicious activity with AI-driven analysis; anti-ransomware from sources including browsers, multi-media, MS Office applications, and email; behavioral analysis (acting on many files in a short period) issuing warnings, stopping errant processes, and notifying IT of such activity; malicious macros and other forms of code detections and protections; and exploit prevention techniques, which detect and stop common and known key vulnerabilities including zero-day attacks. The software communicates with the manufacturer's cloud site, which continuously updates the local software with the latest protections.
   - VLANs, or virtual segmented networks, are used strategically throughout the organization to limit end-point access to servers and networks in which access is needed.
   - Password policies are considered very strong and include required changing periodically, as well as not allowing the re-use of recent passwords. Required changing has been suspended during the pandemic due to having to VPN into the City's network, adding a layer of complexity as well as the reality of passwords expiring for users who don't VPN in and only access cloud services such as email, with no user friendly method of notifying users or them having an easy, intuitive way to change their password.

- All servers are patched as appropriate, generally after a short while once a patch has been released and tested by others as bug free.
- Two Factor Authentication is being researched and expected to be implemented City wide once the best solution for the City is determined.

2. **Backup & Recovery (In the event of an attack, 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?)**

   More than 12.5 TB of user data is backed up in multiple ways. Most importantly, a shadow copy is created twice daily on the server to allow for easy rollback of deleted or changed files. In addition, files are backed up to an on-premise dedicated appliance. The appliance replicates itself to the manufacturer's cloud on a daily basis. In the event the on-premise device becomes infected with mal-ware, including ransomware, the device can be wiped clean and the data restored from the cloud's backup. If the backup device itself fails, within three business days a new appliance will be shipped, which is pre-loaded with the City's backed-up data. Data can also be recovered directly from the manufacturer's cloud storage. Daily backups are preserved for 12 days, weekly backups are preserved for five weeks, monthly backups are saved for 12 months, and yearly revisions are kept for no less than two years. The process is continuously being tested in normal operations via requests from users asking IT to restore data from one of the previous day's backups.

   All databases in the City's robust database infrastructure are included in all backup processes. As new databases are brought online, the using department is involved in determining the requirements of the backup. For example, is recovery to the previous night adequate, or is there a legitimate requirement to be able to restore the database to within the last hour, such as the City's utility billing database in which hundreds of transactions occur daily? All database servers run a process (agent) that is part of the backup appliance solution. In addition, some databases also use the native database engine to back up a database, which is also included in the overall backup process.

   The City runs in a robust, industry-best virtual environment. This not only allows the City to realize cost savings by having many virtual servers running on fewer physical servers, it also allows the City to maintain hot-standby servers in the Police Department data center.

   It is the opinion of the City's IT Manager that the testing of a system-wide recovery is not practical as it is a mix of different functions, services, and protections. In his opinion, it would be near, if not impossible, for any single incident, short of a major catastrophe such as an earthquake or fire in the City Hall data center, to bring down the entire infrastructure. Different functions/components are generally tested during the normal course of business as functions fail, servers are patched, or requested data is restored.

   All network devices have their configurations backed up nightly in the event of an equipment failure or breach.

3. **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)**

   The City utilizes both cloud and an on-premise dedicated SPAM prevention appliance and software in which all email is first run though before being delivered to recipients. The appliance continuously communicates with the manufacturer's secure site to update its protections to the latest known threats. In addition, the appliance wraps all links within an email with a path which, when clicked, first goes through the manufacturer's secure cloud services to confirm (to the extent possible) that the link is legitimate and not a known hacking site.

The City pre-pends the subject of certain emails with [suspect] when an email contains one of many known-to-be-trouble phrases such as "gift cards." Every external email pre-pends the body of the email with a warning that the email is from an external source and to use caution when responding or clicking on any links contained within. With more staff working remotely, IT staff has increased its frequency of cautionary e-mails warning all users of common phishing schemes and malicious links. Staff intends to work with the HR Department on implementing a segment on cybersecurity within its new employee orientation program.

Additional City Security Strategies

As cloud services become more a part of the City's infrastructure, City IT strives to connect cloud services to its internal Active Directory security model. This allows IT staff to disable users in a single, secure place, which in turn disables them on the connected cloud services.

City IT is investigating the implementation of multi-factor authentication. This effort has been ramped up given the current pandemic environment in which the majority of the workforce is located outside of a City facility. Whereas in the past security was focused on blocking external parties from the City's network, the pandemic has turned that strategy into one which secures endpoints theoretically located anywhere in the world. Multi-factor authentication is one of the predominant methods of securing access from outside the City's firewalls.

The City carries cyber security insurance in the event of a data breach, which provides the City with resources to assist in the cost of recovery, including notifications to those whose personal information was likely breached. The insurance carrier also has resources available to assist the City in implementing best practices to deter cybersecurity attacks.

R2. 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.

Response: The recommendation will not be implemented, as the City believes an analysis and discussion of its cybersecurity practices are continually underway. An in-depth written report at a particular point of time would not be useful to Council or management, as its efficacy would be recognized only by the technical staff that produced the report. In the wrong hands, such a report could be used to circumvent the cybersecurity protocols the City has in place and/or is considering. In addition, management does not believe a comprehensive cybersecurity report is the best use of the City's IT resources. The pandemic has necessitated a largely technology-driven response, and IT staff is occupied with enabling users to safely access the IT resources needed to provide continued services to the public as efficiently as possible.

If the City Council or management request additional detail or have specific concerns regarding these protocols, these will be immediately addressed. The summaries developed in response to R1 are meant to convey that the City's IT staff are aware of the risks mentioned in the Grand Jury's report, as evidenced by the measures currently established to prevent cyberattacks and be able to recover promptly should they occur. Staff continuously examines best practices in cybersecurity, evaluating various tools available to protect access to data, software, and hardware systems, and their suitability for the City's use.

R3. Given the results of their internal reports, governmental entities may choose to request further guidance by means of a Cybersecurity review from the U.S. Department of Homeland Security and/or a cyber hygiene assessment from the County Controller's Office.

Response: This recommendation will not be implemented because it is not warranted at this time. Although the City IT personnel recognize the value of a cybersecurity review from the U.S. Department of Homeland Security (DHS), staff feels the security measures currently in place represent affordable, usable, and practical best practices in cybersecurity. As noted in response to R1, City staff is very much aware of the heightened risks of cyberattacks, and has implemented protocols to guard against them and facilitate recovery in the event they do occur. Through research, trade journals and websites, and participation in a state-wide coalition of municipal IT leadership, staff continuously monitors, maintains, and upgrades to the latest cybersecurity measures, software and hardware, and best practices. If at some point in the future IT resources become available, staff will reach out to DHS and/or the County Controller's Office for their respective assessments.

R4. Given the results of their internal reports, governmental entities may choose to ask their IT departments to review their own Cybersecurity Plan with the detailed template provided by the FCC's Cybersecurity Planning Guide and consider customizing it using FCC's Create Custom Cybersecurity Planning Guide tool (see footnote 52).

Response: This recommendation will not be implemented because it is not warranted at this time. The FCC's Cybersecurity Planning Guide was reviewed and compared to solutions currently implemented in the City. In most cases, the recommendations were already enabled, or are planned to be in the near future. Recommended solutions within the Planning Guide not currently in place nor planned have been evaluated and deemed to be less suitable for use by the City, generally due to one or more of the following: IT assessment of the solution cost versus the risk it mitigates; alternative, yet equivalent, solutions already in place; and/or usability/complexity issues for City staff users.

The Burlingame City Council approved this response letter at its public meeting on December 7, 2020.

Sincerely,

DocuSigned by:
D066C125928D48D...
Emily Beach
Mayor

OFFICE OF THE CITY MANAGER
CITY OF DALY CITY

333 – 90TH STREET
DALY CITY, CA 94015-1895
(650) 991-8125

November 9, 2020

Honorable Danny Y. Chou
Judge of the Superior Court
c/o Jenarda Dubois
Hall of Justice
400 County Center, 8th Floor
Redwood City, CA 94063-1655

Re: Grand Jury Response: "Ransomware: It is Not Enough to Think You Are Protected"

Dear Hon. Danny Y. Chou:

We are in receipt of the Grand Jury's final report, "Ransomware: It is Not Enough to Think You Are Protected." Please find the City of Daly City's responses to the findings and recommendations below. This response letter was approved by the City Council at a public meeting held on November 9, 2020.

FINDINGS

FI. Ransomware is a real and growing threat to public entities including those in San Mateo County.
The City of Daly City agrees with this Finding.

F2. Across the country, local governments and schools represent 12% of all Ransomware attacks.
Based on the information cited in the Grand Jury report, as of the date of such information, the City of Daly City agrees with this Finding.

F3. The direct and indirect costs of Ransomware can be significant.
The City of Daly City agrees with this Finding.

F4. Cybersecurity reviews and assessments, and an updated, well-executed Cybersecurity plan, are critical components of IT security strategy.
The City of Daly City agrees with this Finding.

F5. A comprehensive Cybersecurity plan should include, at a minimum, information concerning prevention steps, spam and malware software, and backups and full recovery testing.
The City of Daly City agrees with this Finding.

F6. The identification of phishing attempts, including the use of spam filters, is an important component to protecting an IT system from Ransomware attacks.
The City of Daly City agrees with this Finding.

F7. Testing a full restore of a server to ensure that backups are reliable should be undertaken regularly as part an entity's backup plan to recover lost information.
The City of Daly City agrees with this Finding.

F8. Training of new employees, and the recurring training of existing employees, is an important component of defense against Ransomware.
The City of Daly City agrees with this Finding.

RECOMMENDATIONS
The Grand Jury recommends that each governing body undertake its own confidential effort to protect against Ransomware attacks. Specifically:

R1. 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:

R.1.1. System Security (Firewalls, Anti-malware/Antivirus software, use of subnets, strong password policies, updating/patching regularly)

The City of Daly City has implemented this Recommendation. Multiple Firewall devices (both software and hardware, details of which are redacted for the sake of security) are in place to protect against outside attack as well as attacks across subnets, the latter of which are in place and are used in keeping with IT-Industry practices to segment network infrastructure both for security as well as overall efficiency. In addition, the City has historically used conventional antivirus/antimalware software on both servers and end-user computers (predominantly desktop and notebook PCs) from a variety of vendors including Symantec, McAfee, Microsoft and Kaspersky. Beginning in Q4 of 2020, the City migrated to a security platform with Sophos, an industry leader in endpoint protection and managed threat response (MTR). Finally, all City-owned/managed servers and end-user computers are regularly patched in the ordinary course of business.

R.1.2. Backup & Recovery (In the event of an attack, 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?)

The City of Daly City has implemented this Recommendation. The City has long performed regular and complete ("bare metal") backups of all on- site servers and data. (Details of products and processes used are redacted for the sake of security; further, "Cloud" providers, such as Microsoft Office 365/Exchange Online, provide secure data backup and redundancy as part of their service.) The City's backups include onsite, offsite and "cold storage" backups in one form or another as part of our disaster recovery plan. The City's backups have been periodically tested and we have successfully restored both data as well as complete servers from backups.

R.1.3. 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).

The City of Daly City has implemented this Recommendation. Microsoft's Exchange Online filters email for spam and malware are configured and enabled in our environment and we periodically send reminder and training emails to our user community to provide education and awareness of cyberthreats, including phishing. We have also implemented a standardized warning message to our users alerting them about messages originating outside of our organization. We encourage our users to forward suspect messages for further review and possible action.

R2. 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 City of Daly City's IS Team has provided the initial report to the Director of Finance as of October 20, 2020. An internal report will be completed and provided to the City Council by June 30, 2021.

R3. Given the results of their internal reports, governmental entities may choose to request further guidance by means of a Cybersecurity review from the U.S. Department of Homeland Security and/or a cyber hygiene assessment from the County Controller's
Office.

The City of Daly City will consider this Recommendation when the internal report is completed.

R4. Given the results of their internal reports, governmental entities may choose to ask their IT departments to review their own Cybersecurity Plan with the detailed template provided by the FCC's Cybersecurity Planning Guide and consider customizing it using FCC's Create Custom Cybersecurity Planning Guide tool.

The City of Daly City will consider this Recommendation when the internal report is completed.

The City of Daly City appreciates the opportunity to respond to the Grand Jury Report, ":
"Ransomware: It is Not Enough to Think You Are Protected."
Should the Grand Jury require additional information, please contact me directly at (650) 991-8127.

Sincerely,

Shawnna Maltbie
City Manager

OFFICE OF THE CITY COUNCIL

City of Foster City

January 5, 2021

Hon. Danny Y. Chou
Judge of the Superior Court
c/o Jenarda Dubois
Hall of Justice
400 County Center; 8th Floor
Redwood City, CA 94063-1655

Dear Judge Chou:

The City Council for the City of Foster City has had an opportunity to review the 2020 Grand Jury report entitled "*Ransomware: It is Not Enough to Think You Are Protected*." After reviewing the report and allowing for public comment at its regular meeting on January 4, 2021, the City Council offers the following responses:

Responses to Findings

Finding F1. Ransomware is a real and growing threat to public entities including those in San Mateo County.

Response: The respondent agrees with the finding.

Finding F2. Across the country, local governments and schools represent 12% of all Ransomware attacks.

Response: The respondent agrees with the finding.

Finding F3. The direct and indirect costs of Ransomware can be significant.

Response: The respondent agrees with the finding.

Finding F4. Cybersecurity reviews and assessments, and an updated, well-executed Cybersecurity plan, are critical components of IT security strategy.

Response: The respondent agrees with the finding.

Finding F5. A comprehensive Cybersecurity plan should include, at a minimum, information concerning prevention steps, spam and malware software, and backups and full recovery testing.

Response: The respondent agrees with the finding.

Finding F6. The identification of phishing attempts, including the use of spam filters, is an important component to protecting an IT system from Ransomware attacks.

Response: The respondent agrees with the finding.

Finding F7. Testing a full restore of a server to ensure that backups are reliable should be undertaken regularly as part an entity's backup plan to recover lost information.

Response: The respondent agrees with the finding.

Finding F8. Training of new employees, and the recurring training of existing employees, is an important component of defense against Ransomware.

Response: The respondent agrees with the finding.

Response to Recommendations

R1. 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:

1. System Security (Firewalls, Anti-malware/Antivirus software, use of subnets, strong password policies, updating/patching regularly)

2. Backup & Recovery (In the event of an attack, 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?)

3. 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)

Response: The recommendation has been implemented.

R2. 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.

Response: The recommendation will be implemented within the requested timeframe.

R3. Given the results of their internal reports, governmental entities may choose to request further guidance by means of a Cybersecurity review from the U.S. Department of Homeland Security and/or a cyber hygiene assessment from the County Controller's Office.

Response: The recommendation will be implemented.

R4. Given the results of their internal reports, governmental entities may choose to ask their IT departments to review their own Cybersecurity Plan with the detailed template provided by the FCC's Cybersecurity Planning Guide and consider customizing it using FCC's Create Custom Cybersecurity Planning Guide tool (see footnote 52).

Response: The recommendation will be implemented.

This response was approved by the Foster City City Council, via Minute Order, at its regular meeting on January 4, 2021.

Respectfully submitted,

Sanjay Gehani
Mayor, City of Foster City

cc: grandjury@sanmateocourt.org

MINUTE ORDER

No. 1722

OFFICE OF THE CITY CLERK
FOSTER CITY, CALIFORNIA

Date: January 5, 2021

Attention: City Council/EMID Board
Peter Pirnejad, City/District Manager
Dante Hall, Assistant City Manager
Jean Savaree, City Attorney

City Council/EMID Board of Directors Meeting Date: January 4, 2021

Subject: Response to the San Mateo County Grand Jury Report "Ransomware: It Is Not Enough to Think You Are Protected"

Motion by Councilmember Froomin, seconded by Councilmember Hindi, and carried unanimously by roll call vote, 5-0-0, IT WAS ORDERED to approve a letter to the Honorable Danny Y. Chou, Judge of the Superior Court, in response to the San Mateo County Civil Grand Jury Report, dated October 7, 2020, entitled "Ransomware: It Is Not Enough to Think You Are Protected."

DocuSigned by:
Priscilla Schaus
6131E59FA33B4AB...
CITY CLERK/DISTRICT SECRETARY

CITY OF HALF MOON BAY

501 Main Street
Half Moon Bay, CA 94019

December 1, 2020

Honorable Danny Y. Chou
Judge of the Superior Court
C/O Jenarda Dubois
Hall of Justice
400 County Center; 8th Floor
Redwood City, CA 94063-1655

Subject: October 7, 2020 Grand Jury Report: "Ransomware: It Is Not Enough To Think You Are Protected"

Dear Honorable Judge Chou:

The City Council of the City of Half Moon Bay, at its December 1, 2020 meeting, reviewed and approved the following responses to the San Mateo County Civil Grand Jury 2019-2020 Report entitled "Ransomware: It Is Not Enough To Think You Are Protected"

Findings

The report includes eight (8) findings covering a wide range of technology issues. The City of Half Moon Bay (City) agrees with each of the eight (8) findings (F1 through F8).

Recommendations

R1: 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:

1. System Security (Firewalls, Anti-malware/Antivirus software, use of subnets, strong password policies, updating/patching regularly)
2. Backup & Recovery (In the event of an attack, 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 the backups been tested? Can you fully restore a Server from a backup?)
3. Prevention (turning on email filtering, setting up a message rules to warn users, providing employee training on phishing and providing a reporting system to flag suspect content)

Response: The recommendation has been completed. The City requested information from the IT department which provided information on the above recommendations. The City then confirmed, verified, and improved security in all three categories. The City has now met or exceeded the recommendations.

CITY OF HALF MOON BAY

501 Main Street
Half Moon Bay, CA 94019

R2: 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.
Response: The recommendation has already been completed as part of an annual security review.

R3: Given the results of their internal reports, governmental entities may choose to request further guidance by means of a Cybersecurity review from the U.S. Department of Homeland Security and/or a cyber hygiene assessment from the County Controller's Office.
Response: The recommendation will not be implemented at this time, but we may choose to do so in the future. The City already has a 3rd party auditor that reviews security periodically.

R4: Given the results of their internal reports, governmental entities may choose to ask their IT departments to review their own Cybersecurity Plan with the detailed template provided by the FCC's Cybersecurity Planning Guide and consider customizing it using FCC's Create Custom Cybersecurity Planning Guide Tool.
Response: The recommendation has not yet been implemented. The City will implement this recommendation within the next 6 months.

Thank you for your consideration of the foregoing.

Sincerely,

Adam Eisen
Mayor

CITY COUNCIL AGENDA
REGULAR MEETING
CITY OF HALF MOON BAY

TUESDAY, DECEMBER 1, 2020

REMOTE PARTICIPATION (SEE NEXT PAGE)

Adam Eisen, Mayor
Robert Brownstone, Vice Mayor
Deborah Penrose, Councilmember
Harvey Rarback, Councilmember
Debbie Ruddock, Councilmember

7:00 PM

This agenda contains a brief description of each item to be considered. Those wishing to address the City Council on any matter not listed on the Agenda, but within the jurisdiction of the City Council to resolve, may come forward to the podium during the Public Forum portion of the Agenda and will have a maximum of three minutes to discuss their item. Those wishing to speak on a Public Hearing matter will be called forward at the appropriate time during the Public Hearing consideration.

Please Note: Anyone wishing to present materials to the City Council, please submit seven copies to the City Clerk.

Copies of written documentation relating to each item of business on the Agenda are on file in the Office of the City Clerk at City Hall and the Half Moon Bay Library where they are available for public inspection. If requested, the agenda shall be available in appropriate alternative formats to persons with a disability, as required by Section 202 of the Americans with Disabilities Act of 1990 (42 U.S.C. Sec. 12132.) Information may be obtained by calling 650-726-8271.

In compliance with the Americans with Disabilities Act, special assistance for participation in this meeting can be obtained by contacting the City Clerk's Office at 650-726-8271. A 48-hour notification will enable the City to make reasonable accommodations to ensure accessibility to this meeting (28 CFR 35.102-35.104 ADA Title II).

http://hmbcity.com/

SPECIAL REMOTE PROTOCOLS

In accordance with Governor Newsom's Executive Order No-29-20, this will be a teleconference meeting without a physical location to help stop the spread of COVID-19. This meeting will be conducted entirely by remote participation, in compliance with the Governor's Executive Order N-29-20 allowing for deviation of teleconference rules required by the Ralph M. Brown Act.

This meeting will be conducted via Zoom Webinar. Members of the public are welcome to login into the webinar as Attendees. During any public comment portions, attendees may use the "raise your hand" feature and will be called upon and unmuted when it is their turn to speak. Written comments (jblair@hmbcity.com) submitted by 5:00 p.m. on meeting day will be added to the online agenda packet and emailed to the City Council. The meeting will also be streamed on Channel 27, on pacificcoast.tv, on Facebook in English at www.facebook.com/cityofhalfmoonbay and in Spanish at www.facebook.com/halfmoonbayrecreation. Please click to join the webinar: https://zoom.us/j/93627876187 or join by phone at 669-900-9128, using Webinar ID 936-2787-6187.

CALL TO ORDER / ROLL CALL

PUBLIC FORUM

PROCLAMATIONS AND PRESENTATIONS
COUNTY OF SAN MATEO - CONTACT TRACING PRESENTATION

MAYOR'S ANNOUNCEMENTS OF COMMUNITY ACTIVITIES AND COMMUNITY SERVICE

REPORT OUT FROM RECENT CLOSED SESSION MEETINGS

CITY MANAGER UPDATES TO COUNCIL
COVID-19 UPDATE
POPLAR PILOT PARKING PROJECT UPDATE

1. CONSENT CALENDAR

1.A WAIVE READING OF RESOLUTIONS AND ORDINANCES

1.B SAN MATEO COUNTY MOSQUITO AND VECTOR CONTROL DISTRICT BOARD OF TRUSTEES APPOINTMENT

Staff Recommendation: By motion, reappoint Kati Martin as the City of Half Moon Bay's representative to the San Mateo County Mosquito Abatement District Board of Trustees for a four-year term commencing on January 4, 2021.

STAFF REPORT

1.C APPROVE CITY'S RESPONSE TO THE OCTOBER 7, 2020 GRAND JURY REPORT ENTITLED "RANSOMWARE: IT IS NOT ENOUGH TO THINK YOU ARE PROTECTED"

Staff Recommendation: By motion, authorize the Mayor to sign and submit a letter of response to the October 7, 2020 Grand Jury Report titled "Ransomware: It Is Not Enough To think You Are Protected" no later than January 5, 2020.

STAFF REPORT

ATTACHMENT 1

ATTACHMENT 2

1.D AB1600 REPORT ON DEVELOPMENT IMPACT FEES FOR FISCAL YEAR ENDED JUNE 30, 2020

Staff Recommendation: Accept the AB 1600 Report on Development Impact Fees for fiscal year ended June 30, 2020.

STAFF REPORT

1.E AGREEMENT WITH STEPFORD, INC. FOR INFORMATION TECHNOLOGY SERVICES

Staff Recommendation: Adopt a resolution authorizing the City Manager to execute a revision to the three-year contract agreement with Stepford, Inc. for fiscal years 2019 through 2022. The revisions will cover the remaining two years of the agreement beginning July 1, 2020 and ending June 30, 2022 for the continuation of information technology services at a cost of $180,180 per year.

STAFF REPORT

RESOLUTION

1.F 2021 RESIDENTIAL DWELLING UNIT ALLOCATION PURSUANT TO HALF MOON BAY MUNICIPAL CODE CHAPTER 17.06 (MEASURE D)

Staff Recommendation: Adopt a resolution setting the 2021 Residential Dwelling Unit Allocation and Administration System pursuant to Half Moon Bay Municipal Code Chapter 17.06 for 66 residential dwelling units, 44 units for Downtown and 22 units outside of Downtown.

STAFF REPORT

RESOLUTION

ATTACHMENT 2

1.G FIRST AMENDMENT TO THE HALF MOON BAY HISTORY ASSOCIATION LEASE AGREEMENT FOR 503 JOHNSTON STREET

Staff Recommendation: Adopt a resolution authorizing the City Manager to execute a First Amendment to the Lease Agreement with the Half Moon Bay History Association by granting a one-year extension to begin construction of a new museum on the history property located at 503 Johnston Street.

STAFF REPORT

RESOLUTION

ATTACHMENT 2

ATTACHMENT 3

ATTACHMENT 4

2. ORDINANCES AND PUBLIC HEARINGS

3. RESOLUTIONS AND STAFF REPORTS

3.A PROPOSED ACQUISITION OF THE COASTSIDE INN BY THE COUNTY OF SAN MATEO FOR USE AS AN EMERGENCY HOMELESS SHELTER

Staff Recommendation: Receive a report on the County's proposed acquisition of the Coastside Inn, located at 230 Cabrillo Highway S, in Half Moon Bay, for use as emergency shelter for homeless residents on the Coastside during the COVID-19 pandemic, and future uses to be determined.

STAFF REPORT

ATTACHMENT 1

3.B UPDATE ON LOCAL RECOVERY EFFORTS FROM COVID-19 AND DEVELOPMENT OF RECOMMENDATIONS TOWARD A MORE RESILIENT, VIBRANT, AND DIVERSIFIED COASTSIDE ECONOMY

Staff Recommendation: Receive an update on efforts to assist local businesses and the Coastside community in recovery from COVID-19 and in developing recommendations toward a more resilient, vibrant, and diversified Coastside economy.

STAFF REPORT

3.C 880 STONE PINE ROAD ACQUISITION

Staff Recommendation: Adopt a resolution, in relation to the acquisition of 880 Stone Pine Road from the Peninsula Open Space Trust, for use as the City's corporation yard, authorizing:

1. An additional deposit of $25,000 to POST, if the City chooses to exercise an extension of the escrow period;
2. The use of no more than $2,180,000 in Operating Reserves to close escrow on the acquisition;
3. Receipt of iBank financing proceeds for reimbursement of expenses related to the acquisition and potential improvements to the property; and
4. Authorizing the City Manager to take any required actions to complete the transaction, including accepting any non-substantive changes to the terms and conditions of the acquisition and financing.

STAFF REPORT

RESOLUTION

COMMISSION / COMMITTEE UPDATES

FOR FUTURE DISCUSSION / POSSIBLE AGENDA ITEMS

CITY COUNCIL REPORTS

ADJOURNMENT

December 8, 2020

via electronic mail
grandjury@sanmateocourt.org

Honorable Danny Y. Chou
Judge of the Superior Court
c/o Jenarda Dubois
Hall of Justice
400 County Center, 8th Floor
Redwood City, CA 94063-1655

RE: Civil Grand Jury Report: ""Ransomware: It is not enough to think that you are protected""

Dear Judge Chou:

The City Council of the City of Menlo Park (City) voted at its public meeting on December 8, 2020 to authorize this response to San Mateo County's civil grand jury 2019-20 report ""Ransomware: It is not enough to think that you are protected"" released on October 7, 2020.

Responses to Findings

F1. Ransomware is a real and growing threat to public entities including those in San Mateo County.

City response: *City of Menlo Park agrees that cybersecurity threats, including ransomware, are a growing threat to public agencies.*

F2. Across the country, local governments and schools represent 12% of all Ransomware attacks.

City response: *City of Menlo Park agrees with the finding that local governments are increasingly the target of cybersecurity threats.*

F3. The direct and indirect costs of Ransomware can be significant.

City response: *City of Menlo Park agrees that the direct and indirect costs of cybersecurity threats are significant*.

F4. Cybersecurity reviews and assessments, and an updated, well-executed Cybersecurity plan, are critical components of IT security strategy.

City response: *City of Menlo Park agrees with the finding.*

F5. A comprehensive Cybersecurity plan should include, at a minimum, information concerning prevention steps, spam and malware software, and backups and full recovery testing.

City response: *City of Menlo Park agrees with the finding.*

F6. The identification of phishing attempts, including the use of spam filters, is an important component to protecting an IT system from Ransomware attacks.

City response: *City of Menlo Park agrees with the finding.*

F7. Testing a full restore of a server to ensure that backups are reliable should be undertaken regularly as part an entity's backup plan to recover lost information.

City response: *City of Menlo Park agrees with the finding.*

F8. Training of new employees, and the recurring training of existing employees, is an important component of defense against Ransomware.

City response: *City of Menlo Park agrees with the finding.*

RECOMMENDATIONS

The Grand Jury recommends that each governing body undertake its own confidential effort to protect against Ransomware attacks. Specifically:

R1. 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:

1. System Security (Firewalls, Anti-malware/Antivirus software, use of subnets, strong password policies, updating/patching regularly)

2. Backup & Recovery (In the event of an attack, 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?)

3. 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)

City response. *Implemented.*

R2. 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.

***City response**: Will be implemented by June 30, 2021.*

R3. Given the results of their internal reports, governmental entities may choose to request further guidance by means of a Cybersecurity review from the U.S. Department of Homeland Security56 and/or a cyber hygiene assessment from the County Controller's Office.

***City response:** Further analysis required pending results from R1.*

R4. Given the results of their internal reports, governmental entities may choose to ask their IT departments to review their own Cybersecurity Plan with the detailed template provided by the FCC's Cybersecurity Planning Guide and consider customizing it using FCC's Create Custom Cybersecurity Planning Guide tool.

***City response:** Further analysis required pending results from R1.*

Sincerely,

DocuSigned by:
Cecilia Taylor
4A373F6C54BE48A...

Cecilia Taylor
Mayor

City of Millbrae

621 Magnolia Avenue, Millbrae, CA 94030

January 13, 2021

Honorable Danny Y. Chou
Judge of the Superior Court
c/o Jenarda Dubois
Hall of Justice
400 County Center, 8th Floor
Redwood City, CA 94063-1655

Re: City of Millbrae's Response to Grand Jury Report: "Ransomware: It Is Not Enough To Think You Are Protected"

Dear Honorable Judge Chou,

The City of Millbrae has had the opportunity to review the Grand Jury report referenced above at its regular City Council January 12, 2021 meeting. The City offers the following responses to the findings and recommendations on behalf of the City Council, City Manager and the Mayor of Millbrae:

Responses to Findings

F1. Ransomware is a real and growing threat to public entities including those in San Mateo County.

Response: The City agrees with this finding.

F2. Across the country, local governments and schools represent 12% of all Ransomware attacks.

Response: The City agrees with this finding.

F3. The direct and indirect costs of Ransomware can be significant.

Response: The City agrees with this finding.

F4. Cybersecurity reviews and assessments, and an updated, well-executed Cybersecurity plan, are critical components of IT security strategy.

Response: The City agrees with this finding.

F5. A comprehensive Cybersecurity plan should include, at a minimum, information concerning prevention steps, spam and malware software, and backups and full recovery testing.

Response: The City agrees with this finding.

F6. The identification of phishing attempts, including the use of spam filters, is an important component to protecting an IT system from Ransomware attacks.

Response: The City agrees with this finding.

F7. Testing a full restore of a server to ensure that backups are reliable should be undertaken regularly as part an entity's backup plan to recover lost information.

Response: The City agrees with this finding.

F8. Training of new employees, and the recurring training of existing employees, is an important component of defense against Ransomware.

Response: The City agrees with this finding.

Response to Grand Jury Recommendations

R1. 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:

1. System Security (Firewalls, Anti-malware/Antivirus software, use of subnets, strong password policies, updating/patching regularly)
2. Backup & Recovery (In the event of an attack, 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?)
3. Prevention (turning on email filtering, setting up message rules to warn users, providing employee training on phishing and providing a report system to flag suspect content)

Response: The recommendation has been implemented. The City's IT Consultants has established strategic prevention and recovery plans and implementation measure to combat attacks and protect the City's system from damage resulting from loss of data or use of systems.

R2. 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.
Response: The City intends to implement this recommendation by June 30, 2021.

R3. Given the results of their internal reports, governmental entities may choose to request further guidance by means of a Cybersecurity review from the U.S. Department of Homeland Security and/or a cyber hygiene assessment from the County Controller's Office.
Response: The City will implement this recommendation if warranted and appropriate based on the result of the City's confidential internal report.

R4. Given the results of their internal reports, governmental entities may choose to ask their IT departments to review their own Cybersecurity Plan with the detailed template provided by the FCC's Cybersecurity Planning Guide and consider customizing its using FCC's Create Custom Cybersecurity Planning Guide tool (see footnote 52).
Response: The City intends to implement this recommendation by June 30, 2021.

The City appreciates the opportunity to share its comments on the Grand Jury Report.

Sincerely,

Ann Schneider
Mayor

Cc: City Council
City Manager
City Attorney

Scenic Pacifica
Incorporated Nov. 22, 1957

CITY OF PACIFICA
170 Santa Maria Avenue • Pacifica, California 94044-2506
www.cityofpacifica.org

December 14, 2020

Honorable Judge Chou:
Hall of Justice
400 County Center; 8th Floor
Redwood City, CA 94063-1655

Subject: Re: City of Pacifica's response to the Grand Jury Report: "Ransomware: It Is Not Enough To Think You Are Protected"

Honorable Judge Chou:

Thank you for the opportunity to review and comment on the above referenced Grand Jury Report filed on October 7, 2020. Pursuant to Penal Code section 933 (c), the City of Pacifica's response to both the Findings and Recommendations are provided below. The Pacifica City Council, including the Mayor, reviewed and approved the responses at a public meeting on December 14, 2020.

Response to Grand Jury Findings:

F1. Ransomware is a real and growing threat to public entities including those in San Mateo County.

Response to F1. The City agrees with the finding.

F2. Across the country, local governments and schools represent 12% of all Ransomware attacks.

Response to F2. The City agrees with the finding.

F3. The direct and indirect costs of Ransomware can be significant.

Response to F3. The City agrees with the finding.

F4. Cybersecurity reviews and assessments, and an updated, well-executed Cybersecurity plan, are critical components of IT security strategy.

Response to F4. The City agrees with the finding.

F5. A comprehensive Cybersecurity plan should include, at a minimum, information concerning prevention steps, spam and malware software, and backups and full recovery testing.

Response to F5. The City agrees with the finding.

F6. The identification of phishing attempts, including the use of spam filters, is an important component to protecting an IT system from Ransomware attacks.

Response to F6. The City agrees with the finding.

F7. 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.

Response to F7. The City agrees with the finding.

F8. Training of new employees, and the recurring training of existing employees, is an important component of defense against Ransomware.

Response to F8. The City agrees with the finding.

Response to Grand Jury Recommendations:

R1. 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:

1. System Security (Firewalls, Anti-malware/Antivirus software, use of subnets, strong password policies, updating/patching regularly)
2. Backup & Recovery (In the event of an attack, can you shut down your system quickly? What is being backed up, how is it 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?)
3. 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)

Response to R1. The recommendation has been implemented. The City Manager has requested the City's IT division prepare a report addressing the concerns in the Grand Jury report.

R2. 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.

Response to R2. The recommendation has not yet been implemented. The City's IT Division is in the process of implementing the recommendation and is preparing this report, which is expected to be completed and provided to the governing body by April 2021 or earlier.

R3. Given the results of their internal reports, governmental entities may choose to request further guidance by means of a Cybersecurity review from the U.S. Department of Homeland Security and/or a cyber hygiene assessment from the County Controller's Office.

Response to R3. The recommendation has not yet been implemented, as the internal report has not been completed. The City's IT Division will request guidance by means of a Cybersecurity review from the appropriate agency listed, based on the results of the internal report when complete.

R4. Given the results of their internal reports, government entities may choose to ask their IT departments to review their own Cybersecurity Plan with the detailed template provided by the FCC's Cybersecurity Planning Guide and consider customizing it using FCC's Create Custom Cybersecurity Planning Guide tool.

Response to R4. The recommendation has not yet been implemented. Once the internal report is completed the City's IT Division will evaluate utilizing the FCC's Cybersecurity Planning Guide to assist in updating its Cybersecurity Plan.

Sincerely,

KEVIN WOODHOUSE
City Manager

cc: Pacifica City Council

CITY OF SAN BRUNO

Rico E. Medina
Mayor

CITY OF SAN BRUNO
OFFICE OF THE MAYOR

December 8, 2020

Honorable Danny Y. Chou
Judge of the Superior Court
c/o Jenarda Dubois
Hall of Justice
400 County Center; 8th Floor
Redwood City, CA 94063-1655

Re: Response of the City of San Bruno to the Grand Jury Report "Ransomware: It is not enough to think you are protected"

Dear Judge Chou:

Thank you for the opportunity to respond to the Grand Jury report titled "Ransomware: It is not enough to think you are protected."

The City of San Bruno's ("City") response to the eight listed findings and the four recommendations are listed below. The City Council approved this response at its regular meeting on December 08, 2020.

FINDINGS

F1: Ransomware is a real and growing threat to public entities including those in San Mateo County.

The City agrees that ransomware is a real and growing threat to itself and other public entities in San Mateo County.

F2: Across the country, local governments and schools represent 12% of all Ransomware attacks.

The City does not have information to either agree or disagree with the finding as it relates to cities other than San Bruno.

F3: The direct and indirect costs of Ransomware can be significant

The City agrees with the finding as it relates to San Bruno.

F4: Cybersecurity reviews and assessments, and an updated, well-executed Cybersecurity plan, are critical components of IT Security strategy.

The City agrees with the finding as it relates to San Bruno.

F5: A comprehensive Cybersecurity plan should include, at a minimum, information concerning prevention steps, spam and malware software, and backups and full recovery testing.

The City agrees with the finding as it relates to San Bruno.

F6: The identification of phishing attempts, including the use of spam filters, is an important component to protecting an IT system from Ransomware attacks

The City agrees with the finding as it relates to San Bruno.

F7: 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 City agrees with the finding as it relates to San Bruno.

F8: Training of new employees, and the recurring training of existing employees, is an important component of defense against Ransomware.

The City agrees with the finding as it relates to San Bruno.

RECOMMENDATIONS

R1: 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:

1. **System Security (Firewalls, Anti-malware/Antivirus software, use of subnets, strong password policies, updating/patching regularly)**

2. **Backup & Recovery (In the event of an attack, can you shut down your system quickly? What is being backed up, how is it 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?**

3. **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)**

The recommendation has been implemented as of November 30, 2020.

R2: 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 City will comply with this recommendation.

R3: Given the results of their internal reports, government entities may choose to request further guidance by means of a Cybersecurity review from the U.S. Department of Homeland Security and/or a cyber hygiene assessment from the County Controller's Office

The City will consider this recommendation during its review of internal reports.

R4: Given the results of their internal reports, government entities may choose to ask their IT departments to review their own Cybersecurity Plan with the detailed template provided by the FCC's Cybersecurity Planning Guide and consider customizing it using FCC's Create Custom Cybersecurity Planning Guide tool

The City will consider this recommendation during its review of internal reports.

Sincerely,

Rico E Medina

Rico E. Medina
Mayor

CITY OF SAN CARLOS
OFFICE OF THE CITY MANAGER

600 ELM STREET
SAN CARLOS, CA 94070
(650) 802-4228
CITYOFSANCARLOS.ORG

November 23, 2020

Honorable Danny Y. Chou
Judge of the Superior Court
c/o Charlene Kresevich
Hall of Justice
400 County Center, 2nd Floor
Redwood City, CA 94063-1655

RE: Request for Response to the Grand Jury Report "Ransomware: It Is Not Enough To Think You Are Protected"

Dear Judge Chou:

The City of San Carlos is replying to a request by the court to respond to the Grand Jury Report "Ransomware: It Is Not Enough To Think You Are Protected". Below are our responses to the Findings and Recommendations that were approved by the San Carlos City Council on November 23, 2020.

FINDINGS:

The Grand Jury asked the City to agree with the Findings. While City staff did not conduct the investigation ourselves, we assume the information is accurate and are willing to agree with all 8 of the Findings.

RECOMMENDATIONS:

Recommendation 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:

1. System Security (Firewalls, Anti-malware/ Antivirus software, use of subnets, strong password policies, updating/patching regularly)

2. Backup & Recovery (In the event of an attack, 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?)

3. 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)

Response. The recommendation has been implemented as requested.

Recommendation 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.

Response. The recommendation has not yet been implemented, but will be implemented as requested by June 30, 2021. However, the recommendation requires further analysis by our IT staff and the City Attorney to ensure that our cybersecurity plan and any updated elements remain confidential and not subject to public disclosure. The City wants to be careful that its security protocols, enhancements, and strategies are not accessible to potential hackers.

Recommendation 3. Given the results of their internal reports, governmental entities may choose to request further guidance by means of a Cybersecurity review from the U.S. Department of Homeland Security and/or a cyber-hygiene assessment from the County Controller's Office.

Response. This recommendation will require further analysis. The City contracts with Gartner, Inc., officially known as Gartner, a global research and advisory firm providing information, advice, and tools for leaders in IT. Since we contract with Gartner, we will follow its best practices.

Recommendation 4. Given the results of their internal reports, governmental entities may choose to ask their IT departments to review their own Cybersecurity Plan with the detailed template provided by the FCC's Cybersecurity Planning Guide and consider customizing it using FCC's Create Custom Cybersecurity Planning Guide tool.

Response. The recommendation will require further analysis. As noted above, the City will follow Gartner best practices.

Sincerely,

Jeff Maltbie, City Manager

CITY OF SAN MATEO
CITY COUNCIL

330 W. 20th Avenue
San Mateo, CA 94403
www.cityofsanmateo.org
(650) 522-7040

November 16, 2020

Hon. Danny Y. Chou
Judge of the Superior Court
c/o Jenarda Dubois
Hall of Justice
400 County Center; 8th Floor
Redwood City, CA 94063-1655

RESPONSE TO GRAND JURY REPORT: "Ransomware: It Is Not Enough To Think You Are Protected"

Honorable Judge Chou,

Thank you for the opportunity to review and comment on the above referenced Grand Jury Report filed on October 7, 2020. The City of San Mateo's response to both the findings and recommendations are listed below.

Response to Grand Jury Findings:

F1. Ransomware is a real and growing threat to public entities including those in San Mateo County.

Response: The City of San Mateo agrees with this finding

F2. Across the country, local governments and schools represent 12% of all Ransomware attacks.

Response: The City of San Mateo agrees with this finding

F3. The direct and indirect costs of Ransomware can be significant.

Response: The City of San Mateo agrees with this finding.

F4. Cybersecurity reviews and assessments, and an updated, well-executed Cybersecurity plan, are critical components of IT security strategy.

Response: The City of San Mateo agrees with this finding.

F5. A comprehensive Cybersecurity plan should include, at a minimum, information concerning prevention steps, spam and malware software, and backups and full recovery testing.

Response: The City of San Mateo agrees with this finding.

F6. The identification of phishing attempts, including the use of spam filters, is an important component to protecting an IT system from Ransomware attacks.

Response: The City of San Mateo agrees with this finding.

F7. Testing a full restore of a server to ensure that backups are reliable should be undertaken regularly as part an entity's backup plan to recover lost information.

Response: The City of San Mateo agrees with this finding.

F8. Training of new employees, and the recurring training of existing employees, is an important component of defense against Ransomware.

Response: The City of San Mateo agrees with this finding.

Response to Grand Jury Recommendations:

The Grand Jury recommends that each governing body undertake its own confidential effort to protect against Ransomware attacks. Specifically:

R1. 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:

1. System Security (Firewalls, Anti-malware/Antivirus software, use of subnets, strong password policies, updating/patching regularly)
2. Backup & Recovery (In the event of an attack, 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?)
3. 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)

Response: This recommendation has been implemented

The San Mateo City Manager's Office made this request of the City's IT Department upon receipt of the Grand Jury Report. The IT Department will prepare a study session presentation for council which will, at a minimum, address the concerns listed in R1.1, R1.2, and R1.3.

R2. 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.

Response: This recommendation will be implemented by the June deadline

The City of San Mateo's IT department will prepare a comprehensive study session for City Council, planned for Q1 calendar year 2021, that addresses the concerns identified in the report. This report will include actions taken and plans for future enhancements.

R3. Given the results of their internal reports, governmental entities may choose to request further guidance by means of a Cybersecurity review from the U.S. Department of Homeland Security and/or a cyber hygiene assessment from the County Controller's Office.

Response: This recommendation will be implemented on or before June 30, 2021

The City of San Mateo IT Department will make a request with the Department of Homeland Security, Cybersecurity & Infrastructure Security Agency, for cyber-hygiene services before June 30, 2021.

R4. Given the results of their internal reports, governmental entities may choose to ask their IT departments to review their own Cybersecurity Plan with the detailed template provided by the FCC's Cybersecurity Planning Guide and consider customizing it using FCC's Create Custom Cybersecurity Planning Guide tool (see footnote 52).

Response: This recommendation will be implemented on or before June 30, 2021

The City of San Mateo IT Department will utilize the Federal Communications Commission Cyber Security Planning Guide and the FCC Cyber Security Planner to review and update our cyber-security plans. This work will be completed on or before June 30, 2021.

This response to the Grand Jury was approved at a public meeting on November 16, 2020.

Respectfully,

Joe Goethals,
Mayor – City of San Mateo

City Manager's Department

December, 03 2020

Hon. Danny Y. Chou
Judge of the Superior Court
c/o Jenarda Dubois
Hall of Justice
400 County Center: 8th Floor
Redwood City, CA 94063-1655

Re: Grand Jury Report: "Ransomware: It Is Not Enough To Think You Are Protected"

Dear Judge Chou:

The City of South San Francisco (the "City") hereby submits the following response to the Grand Jury report filed on October 7, 2020. The following is in response to the findings and recommendations as it pertains to the City. These responses were approved by the City Council at the City Council meeting held on November 24, 2020.

The City of South San Francisco concurs with the findings in the Grant Jury report that ransomware is a significant threat to the City network infrastructure and a cybersecurity plan must be in place to prevent attacks; but more importantly recover from an attack.

The City Information Technology Department will provide a confidential internal cybersecurity plan outlining the measures in place to prevent ransomware, a continuity plan, and list of future security enhancements by June 30, 2021.

Sincerely,

Mike Futrell
City Manager

City of South San Francisco

P.O. Box 711 (City Hall,
400 Grand Avenue)
South San Francisco, CA

City Council

Resolution: RES 163-2020

File Number: 20-926 **Enactment Number: RES 163-2020**

RESOLUTION APPROVING AND AUTHORIZING THE CITY MANAGER TO SIGN THE RESPONSE TO THE SAN MATEO COUNTY GRAND JURY REPORT TITLED "RANSOMWARE: IT IS NOT ENOUGH TO THINK YOU ARE PROTECTED".

WHEREAS, on October 7, 2020, the Grand Jury released a report titled "Ransomware: It Is Not Enough To Think You Are Protected" with recommendations directed at cities to address issues relating to Ransomware; and

WHEREAS, Recommendation R1 in the Grand Jury report suggests that, by November 30, 2020, the City Council request a confidential internal report addressing the findings in the report; and

WHEREAS, the confidential internal report addressing the Grand Jury's findings should be provided to the City Council by June 30, 2021, describing what actions have been taken and future enhancements to the existing cybersecurity plan; and

WHEREAS, staff has prepared a response to the Grand Jury report, attached herein as Exhibit A.

NOW, THEREFORE, BE IT RESOLVED that the City Council of the City of South San Francisco does hereby approve and authorize the City Manager to sign the response, attached hereto as Exhibit A, to the San Mateo County Grand Jury Report titled "Ransomware: It Is Not Enough To Think You Are Protected."

* * * * *

At a meeting of the City Council on 11/24/2020, a motion was made by Councilmember Nagales, seconded by Councilmember Nicolas, that this Resolution be approved. The motion passed.

Yes: 5 Mayor Garbarino, Vice Mayor Addiego, Councilmember Nagales, Councilmember Nicolas, and Councilmember Matsumoto

Attest by Rosa Govea Acosta

Rosa Govea Acosta, City Clerk

February 26, 2021

Hon. Danny Y. Chou
Judge of the Superior Court
c/o Jenarda Dubois
Hall of Justice
400 County Center, 8th Floor
Redwood City, CA 94063-1655

Subject: Coastside County Water District Response to Grand Jury Report Entitled "Ransomware: It Is Not Enough To Think You Are Protected"

Honorable Chou:

The Coastside County Water District (District) received the 2019-2020 Grand Jury report entitled "Ransomware: It Is Not Enough To Think You Are Protected." The District's Board of Directors reviewed the report and approved this response at the December 8 regular Board meeting. This letter responds to all of the Civil Grand Jury's findings and recommendations in the report.

Responses to Findings:

The District agrees with findings F1 and F3-F8. With regard to finding F2, the District agrees that local governments and schools across the country are involved in Ransomware attacks, however the District does not have sufficient information to know the percentage of Ransomware attacks that local governments and schools represent.

Responses to Recommendations:

R1: 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:

1. System Security (Firewalls, Anti-malware/ Antivirus software, use of subnets, strong password policies, updating/patching regularly)
2. Backup & Recovery (In the event of an attack, 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?)
3. 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)

Response 1: Recommendation R1 has been implemented. The District has an outside third party IT consultant and, prior to November 30, 2020, requested a report from the IT consultant that addresses system security, backup and recovery, and prevention.

R2: 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.

Response 2: Recommendation R2 has not yet been implemented, but will be implemented by June 30, 2021.

R3: Given the results of their internal reports, governmental entities may choose to request further guidance by means of a Cybersecurity review from the U.S. Department of Homeland Security and/or a cyber hygiene assessment from the County Controller's Office.

Response 3: Recommendation R3 requires further analysis, and will be evaluated upon receipt of the report from the District's IT consultant. If the District chooses to request further guidance from the U.S. Department of Homeland Security or the County Controller's Office, it will do so within two months of receiving the IT consultant's report.

R4. Given the results of their internal reports, governmental entities may choose to ask their IT departments to review their own Cybersecurity Plan with the detailed template provided by the FCC's Cybersecurity Planning Guide and consider customizing it using FCC's Create Custom Cybersecurity Planning Guide tool.

Response 4: Recommendation R4 requires further analysis, and will be evaluated upon receipt of the report from the District's IT consultant. If the District chooses to request its IT consultant to review the District's cybersecurity plan with the FCC's Cybersecurity Planning Guide and customizing the plan using FCC's Create Custom Cybersecurity Planning Guide tool, it will do so within two months of receiving the IT consultant's report.

The District appreciates the effort that the Grand Jury put into the important cybersecurity issue and the opportunity to respond to the Grand Jury report. Please let us know if the District can provide additional information.

Very truly yours,

Glenn Reynolds
President, Board of Directors
Coastside County Water District

cc: Board of Directors
Mary Rogren, General Manager

COASTSIDE FIRE PROTECTION DISTRICT

1191 MAIN STREET ■ HALF MOON BAY, CA 94019

TELEPHONE (650) 726-5213
FAX (650) 726-0132

December 11, 2020

Hon. Danny Y. Chou
Judge of the Superior Court
c/o Jenarda Dubois
Hall of Justice
400 County Center; 8th Floor
Redwood City, CA 94063-1655

Dear Judge Chou:

The Coastside Fire Protection District Board has had an opportunity to review the 2020 Grand Jury report entitled "*Ransomware: It is Not Enough to Think You Are Protected.*" The District Board after reviewing the report and allowing for public comment at its Special Board meeting on December 9, 2020 offers the following responses:

Responses to Findings

Finding F1. Ransomware is a real and growing threat to public entities including those in San Mateo County.

Response: The respondent agrees with the finding.

Finding F2. Across the country, local governments and schools represent 12% of all Ransomware attacks.

Response: The respondent agrees with the finding.

Finding F3. The direct and indirect costs of Ransomware can be significant.

Response: The respondent agrees with the finding.

Finding F4. Cybersecurity reviews and assessments, and an updated, well-executed Cybersecurity plan, are critical components of IT security strategy.

Response: The respondent agrees with the finding.

Finding F5. A comprehensive Cybersecurity plan should include, at a minimum, information concerning prevention steps, spam and malware software, and backups and full recovery testing.

Response: The respondent agrees with the finding.

Finding F6. The identification of phishing attempts, including the use of spam filters, is an important component to protecting an IT system from Ransomware attacks.

Response: The respondent agrees with the finding.

Finding F7. Testing a full restore of a server to ensure that backups are reliable should be undertaken regularly as part an entity's backup plan to recover lost information.

Response: The respondent agrees with the finding.

Finding F8. Training of new employees, and the recurring training of existing employees, is an important component of defense against Ransomware.

Response: The respondent agrees with the finding.

Response to Recommendations

R1. 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:

1. System Security (Firewalls, Anti-malware/Antivirus software, use of subnets, strong password policies, updating/patching regularly)

2. Backup & Recovery (In the event of an attack, 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?)

3. 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)

Response: The recommendation has been implemented.

R2. 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.

Response: The recommendation will be implemented within the requested timeframe.

R3. Given the results of their internal reports, governmental entities may choose to request further guidance by means of a Cybersecurity review from the U.S. Department of Homeland Security and/or a cyber hygiene assessment from the County Controller's Office.

Response: The recommendation will be implemented within the requested timeframe.

R4. Given the results of their internal reports, governmental entities may choose to ask their IT departments to review their own Cybersecurity Plan with the detailed template provided by the FCC's Cybersecurity Planning Guide and consider customizing it using FCC's Create Custom Cybersecurity Planning Guide tool (see footnote 52).

Response: The recommendation will be implemented.

Respectfully submitted,

G Burke

Gary Burke
President, Coastside Fire Protection District

Cc: grandjury@sanmateocourt.org

Board of Fire Commissioners
Maryanne Hazard
Gina Sheridan
Peter Dabai

COLMA FIRE DISTRICT

50 REINER STREET
COLMA, CALIFORNIA 94014
Phone (650) Plaza 5-5666
Fax (650) 755-5691

Fire Chief
Geoffrey C. Balton

04 January 2021

Honorable Danny Y. Chou
Judge of the Superior Court
C/o Jenarda Dubois
Hall of Justice
400 County Center; 8th Floor
Redwood City, CA 94063-1655

Subject: District response Grand Jury Report: "Ransomware: It Is Not Enough to Think You Are Protected."

Dear Honorable Judge Chou,

Thank you for the opportunity to respond to the above-mentioned Grand Jury report. On behalf of the Colma Fire District and the Board of Directors, thank you for the information related to this topic.

The Grand Jury report and our response will be on the agenda for our January 2021 meeting. We will continue this topic to future meetings.

FINDINGS:

F1: We agree with this finding.
F2: We agree with this finding.
F3: We agree with this finding.
F4: We agree with this finding.
F5: We agree with this finding.
F6: We agree with this finding.
F7: We agree with this finding.
F8: We agree with this finding.

RECOMMENDATIONS:

R1: We accept this recommendation and will comply.

R2: We accept this recommendation and will comply by June 30, 2021

R3: We accept this recommendation and will comply by January 31, 2020

R4: We accept this recommendation and will comply.

We want to thank you again for the opportunity to respond to the Grand Jury.

Sincerely,

Peter Dabai
Chairman, Board of Directors

Geoffrey Balton
Fire Chief

County of San Mateo

Inter-Departmental Correspondence

Department: COUNTY MANAGER
File #: 20-962 Board Meeting Date: 12/8/2020

Special Notice / Hearing: None
Vote Required: Majority

To: Honorable Board of Supervisors

From: Michael P. Callagy, County Manager

Subject: Board of Supervisors' Response to the 2019-2020 Civil Grand Jury Report "Ransomware: It is Not Enough to Think You Are Protected"

RECOMMENDATION:
Approve the Board of Supervisors' response to the 2019-2020 Civil Grand Jury Report, "Ransomware: It is Not Enough to Think You Are Protected"

BACKGROUND:
On October 7, 2020, the 2019-2020 San Mateo County Civil Grand Jury issued a report titled "Ransomware: It is Not Enough to Think You Are Protected." The Board of Supervisors is required to submit comments on the findings and recommendations pertaining to the matters over which it has some decision-making authority within 90 days. The Board's response to the report is due to the Honorable Danny Y. Chou no later than January 5, 2021.

DISCUSSION:
The Grand Jury made 8 findings and 4 recommendations in its report. The Board responses follow each finding and the 4 recommendations that the Grand Jury requested that the Board respond to within 90 days.

FINDINGS

Finding 1:
Ransomware is a real and growing threat to public entities including those in San Mateo County.

Response: The respondent agrees with the finding.

Finding 2:
Across the country, local governments and schools represent 12% of all Ransomware attacks.

Response: The respondent agrees with the finding.

Finding 3:
The direct and indirect costs of Ransomware can be significant.

Response: The respondent agrees with the finding.

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

Response: The respondent agrees with the finding.

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

Response: The respondent agrees with the finding.

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

Response: The respondent agrees with the finding.

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

Response: The respondent agrees with the finding.

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

Response: The respondent agrees with the finding.

RECOMMENDATIONS

Recommendation 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:

1. System Security (Firewalls, Anti-malware/Antivirus software, use of subnets, strong password policies, updating/patching regularly)
2. Backup & Recovery (In the event of an attack, 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?)
3. 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)

Response: The respondent will implement the recommendation with the assistance of the County's Information Services Department (ISD). The San Mateo County Sheriff's Office and the San Mateo County Assessor-Clerk-Recorder-Elections (ACRE) also agree with the recommendation and will implement the recommendation through their respective internal IT service divisions.

Recommendation 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.

Response: The recommendation has not yet been implemented by respondent but will be implemented in the future with a specific time frame for implementation and reporting.

Recommendation 3:

Given the results of their internal reports, governmental entities may choose to request further guidance by means of a Cybersecurity review from the U.S. Department of Homeland Security and/or a cyber hygiene assessment from the County Controller's Office.

Response: The respondent will implement the recommendation with the assistance of the County's Information Services Department (ISD). The San Mateo County Sheriff's Office and the San Mateo County Assessor-Clerk-Recorder-Elections (ACRE) also agree with the recommendation and will implement the recommendation through their respective internal IT service divisions, including obtaining guidance from the U.S. Department of Homeland Security, as necessary.

Recommendation 4:

Given the results of their internal reports, governmental entities may choose to ask their IT departments to review their own Cybersecurity Plan with the detailed template provided by the FCC's Cybersecurity Planning Guide and consider customizing it using FCC's Create Custom Cybersecurity Planning Guide tool (see footnote 52).

Response: The respondent will implement the recommendation with the assistance of the County's Information Services Department (ISD). The San Mateo County Sheriff's Office and the San Mateo County Assessor-Clerk-Recorder-Elections (ACRE) also agree with the recommendation and will implement the recommendation through their respective internal IT service divisions, as necessary.

FISCAL IMPACT:
There is no fiscal impact associated with the acceptance of this report.

EAST PALO ALTO SANITARY DISTRICT

RESOLUTION NO. 1272

RESOLUTION OF THE BOARD OF DIRECTORS OF THE EAST PALO ALTO SANITARY DISTRICT APPROVING AND AUTHORIZING THE GENERAL MANAGER TO SIGN AND SUBMIT THE DISTRICT'S RESPONSE TO THE SAN MATEO COUNTY CIVIL GRAND JURY REPORT TITLED "RANSOMWARE: IT IS NOT ENOUGH TO THINK YOU ARE PROTECTED"

WHEREAS, on October 7, 2020, the San Mateo County Civil Grand Jury released a report titled "Ransomware: It Is Not Enough To Think You Are Protected" with recommendations directed at local public entities to address issues relating to Ransomware; and

WHEREAS, the purpose of the report is to have local public entities assess their cyber-security strategies and address any deficiencies to ensure adequate measures are being taken to mitigate risks and establish recovery options; and

WHEREAS, the report contains eight (8) findings and four (4) recommendations addressed to sixty-eight (68) public entities in San Mateo County, including the District. The report directs each of these public entities to respond to the findings and recommendations; and

WHEREAS, staff has reviewed the findings and recommendations and has prepared a response to the report, attached hereto as Exhibit A.

NOW, THEREFORE, BE IT RESOLVED that the Board of Directors of the East Palo Alto Sanitary District does hereby approve and authorize the General Manager to sign and submit the response, attached hereto as Exhibit A, to the San Mateo County Grand Jury Report titled "Ransomware: It Is Not Enough To Think You Are Protected."

PASSED AND ADOPTED by the District Board of the East Palo Alto Sanitary District at a Special Board Meeting thereof held on the 18th day of March, 2021 by the following vote:

Ayes:	Members:	Joan Sykes-Miessi, Martha Stryker, Betsy Yanez, Glenda Savage, Dennis Scherzer
Noes:	Members:	
Abstain:	Members:	
Absent:	Members:	

President of the District Board of the
East Palo Alto Sanitary District of
San Mateo County, State of California

ATTEST:

Secretary of the District Board of the
East Palo Alto Sanitary District of
San Mateo County, State of California

Exhibit A

[see attached]

EPASD
EAST PALO ALTO SANITARY DISTRICT

BOARD OF DIRECTORS
Joan Sykes-Miessi, President
Martha Stryker, Vice President
Bethzabe Yañez, Secretary
Glenda Savage, Director
Dennis Scherzer, Director

901 Weeks Street
East Palo Alto, CA 94303
Phone: (650) 325-9021
Fax: (650) 325-5173
www.epasd.com

Akin Okupe, M.B.A, P.E., General Manager

March 9, 2021

Hon. Danny Y. Chou
Judge of the Superior Court
c/o Jenarda Dubois
Hall of Justice
400 Country Center; 8th Floor
Redwood City, CA 94063-1655

Re: Grand Jury Report "Ransomware: Is It Not Enough To Think You Are Protected"

Dear Sir,

I would like to thank the Grand Jury of San Mateo County for taking a leadership role on this subject. I would also like to emphasize that we fully agree with the findings of the Grand Jury Report as stated in the attached letter dated October 7, 2020.

In consideration of the above, we have been implementing some of the recommendations but yet to fully implement all of the recommendations. We have solicited proposals from notable consultants to help us with the full implementation of the recommendations. One of the proposals received is hereby attached.

In this regard, we hope to be in full compliance within the next three months.

Thank you for your anticipated action.

Sincerely

Mr. Akin Okupe,
General Manager

accendnetworks

75 E. Santa Clara St., #600
San Jose, CA 95113
Email: paula@accendnetworks.com
Phone: (408) 784-2345 Local / 855-8ACCEND Toll Free
Fax: (877) 266-3207
Email paula@accendnetworks.com the signed proposal if accepting.

Statement of Proposal

for

Master IP Plan

(Cybersecurity Enhancement)

EPASD
EAST PALO ALTO
SANITARY DISTRICT

Nazifa Rahimi, nrahimi@epasd.com

March 17, 2021

accendnetworks

Accend Networks is proposing the following to assist EPASD with the Master IP Plan for Cybersecurity Enhancement Initiative:

SERVICES	**COST**
Install and Ensure Anti-virus, Anti-malware, and Windows Updates are running monthly (includes brief monthly reports and analytics):	
• For 11 Devices (9 Desktops, 1 Exchange Server, and 1 File Server)	$838.00
Total Monthly Cost	**$838.00**

Other Integration Features:

AntiVirus\Anti-Malware	$2.40 per endpoint
Backup	
• Cloud Backup	$0.28 per GB
• Local Backup	$.14 per GB

Security Consultant/Advisory:

• ISP Router/Firewall/Switches/Network Design & Architect (CCIE LEvel)	$150/hr
• Structured Cabling Installation/Upgrade (Labor only, materials not included)	$95/hr
• Flat Rate Travel Charge for any on-site visit (within 30 miles radius)	$55

PAYMENT TERMS:

An upfront payment is required to get network services running in the most expedited matter and up to network standard.

Proposal Accepted:

Name: _____Nazifa Rahimi_____
Title: _____
Signature: _____
Date: _____

HIGHLANDS RECREATION DISTRICT EST. 1957

Highlands Recreation District

1851 Lexington Avenue • San Mateo, CA 94402
(650) 341-4251 • Fax (650) 349-9627
www.highlandsrec.ca.gov

"A Community Place to Learn, Grow & Play"

December 8, 2020

Via Email (grandjury@sanmateocourt.org)

The Honorable Danny Y. Chou
Judge of the Superior Court
c/o Jenarda Dubois
Hall of Justice
400 County Center, 2nd Floor
Redwood City, CA 94063-1655

Re: Response to the 2019-2020 Grand Jury Report entitled *"Ransomware: It Is Not Enough To Think You Are Protected."*

Honorable Judge Chou,

The Highlands Recreation District (District) has received and reviewed the 2019-2020 Grand Jury Report entitled "Ransomware: It Is Not Enough To Think You Are Protected." We appreciate the opportunity to review and comment on the report that was filed on October 7, 2020.

Please be advised that the response to the Grand Jury report was reviewed and approved by the Highlands Recreation District Board of Directors on December 8, 2020.

Response to Grand Jury Findings:

F1. Ransomware is a real and growing threat to public entities including those in San Mateo County.
Response: The District agrees with this Finding.

F2. Across the country, local governments and schools represent 12% of all Ransomware attacks.
Response: The District lacks information to fully agree or disagree with this Finding as it did not conduct the research for this report. However, the District accepts the Grand Jury's Finding for the purpose of this response.

F3. The direct and indirect costs of Ransomware can be significant.
Response: The District agrees with this Finding.

F4. Cybersecurity reviews and assessments, and an updated, well-executed Cybersecurity plan, are critical components of IT security strategy.
Response: The District agrees with this Finding.

F5. A comprehensive Cybersecurity plan should include, at a minimum, information concerning prevention steps, spam and malware software, and backups and full recovery testing.
Response: The District agrees with this Finding.

F6. The identification of phishing attempts, including the use of spam filters, is an important component to protecting an IT system from Ransomware attacks.
Response: The District agrees with this Finding.

F7. Testing a full restore of a server to ensure that backups are reliable should be undertaken regularly as part an entity's backup plan to recover lost information.
Response: The District lacks information to fully agree or disagree with this Finding as it did not conduct the research for this report. However, the District accepts the Grand Jury's Finding for the purpose of this response.

F8. Training of new employees, and the recurring training of existing employees, is an important component of defense against Ransomware.
Response: The District agrees with this Finding.

Response to Grand Jury Recommendations:

The Grand Jury recommends that each governing body undertake its own confidential effort to protect against Ransomware attacks. Specifically:

R1. 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:

1. System Security (Firewalls, Anti-malware/Antivirus software, use of subnets, strong password policies, updating/patching regularly).
2. Backup & Recovery (In the event of an attack, 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?).
3. 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).

Response: The District implemented this recommendation on November 27, 2020 when it consulted with E-IKON, LLC. Technology Consultant to prepare a confidential report addressing concerns specifically identified above.

R2. 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.

Response: The District intends to implement this recommendation by the June deadline by providing a confidential internal report to the District Board of Directors that addresses the concerns identified in the report. The report will include actions taken and plans for future enhancements.

R3. Given the results of their internal reports, governmental entities may choose to request further guidance by means of a Cybersecurity review from the U.S. Department of Homeland Security56 and/or a cyber hygiene assessment from the County Controller's Office.

Response: The District will implement this recommendation if warranted and appropriate based on the results of the District's confidential internal report.

R4. Given the results of their internal reports, governmental entities may choose to ask their IT departments to review their own Cybersecurity Plan with the detailed template provided by the FCC's Cybersecurity Planning Guide and consider customizing it using FCC's Create Custom Cybersecurity Planning Guide tool (see footnote 52).

Response: The District will review the Federal Communications Commission Cybersecurity Planning Guide and the FCC Cyber Security Planner and implement this recommendation if warranted and appropriate based on the results of the District's confidential internal report.

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

Respectfully,

Derek Schweigart
General Manager
Highlands Recreation District

Hillsborough
CITY SCHOOL DISTRICT

300 El Cerrito Avenue
Hillsborough, CA 94010
t: (650) 342-5193
www.hcsdk8.org

November 12, 2020

The Honorable Danny Y. Chou
Judge of the Superior Court
c/o Jenarda Dubois
Hall of Justice
400 County Center; 2nd Floor
Redwood City, CA 94063-1655

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

Dear Judge Chou:

The Hillsborough City School District (the "District") has received and reviewed the 2019-2020 Grand Jury Report entitled "Ransomware: It Is Not Enough To Think You Are Protected." We appreciate the Grand Jury's interest in this matter. Having reviewed and considered the Grand Jury's Findings and Recommendations, the District responds below pursuant to section 933.05 of the California Penal Code.

Please be advised that the District presented the Grand Jury Report to its Board of Trustees, and the District's Board approved these responses, on November 12, 2020.

Findings:

1. *Ransomware is a real and growing threat to public entities including those in San Mateo County.*

   The District agrees with this Finding.

2. *Across the country, local governments and schools represent 12% of all Ransomware attacks.*

   The District lacks information to fully agree or disagree with this Finding given that it did not conduct the research related to this Report. The District, however, accepts the Grand Jury's Finding for the purposes of this Response.

3. *The direct and indirect costs of Ransomware can be significant.*

   The District agrees with this Finding.

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

Hillsborough CITY SCHOOL DISTRICT

300 El Cerrito Avenue
Hillsborough, CA 94010
t: (650) 342-5193
www.hcsdk8.org

The District agrees with this Finding.

5. *A comprehensive Cybersecurity 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.

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.

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

   The District agrees with this Finding.

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.

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:*

   1. *System Security (Firewalls, Anti-malware/Antivirus software, use of subnets, strong password policies, updating/patching regularly)*
   2. *Backup & Recovery (In the event of an attack, 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?)*
   3. *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)*

   The District implemented this Recommendation on October 20, 2020 by directing the District's IT Department to prepare a confidential report which addresses the three concerns specifically identified above.

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.*

Hillsborough
CITY SCHOOL DISTRICT

300 El Cerrito Avenue
Hillsborough, CA 94010
t: (650) 342-5193
www.hcsdk8.org

The District intends to implement this Recommendation, 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.*Given the results of their internal reports, governmental entities may choose to request further guidance by means of a Cybersecurity review from the U.S. Department of Homeland Security and/or a cyber hygiene assessment from the County Controller's Office.*

The District will implement this Recommendation if warranted and appropriate based on the results of the District's confidential internal report.

3. *Given the results of their internal reports, governmental entities may choose to ask their IT departments to review their own Cybersecurity Plan with the detailed template provided by the FCC's Cybersecurity Planning Guide and consider customizing it using FCC's Create Custom Cybersecurity Planning Guide tool (see footnote 52).*

   The District will implement this Recommendation if warranted and appropriate based on the results of the District's confidential internal report.

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

Sincerely,

Carlomagno

Louann Carlomagno, Ed.D.
Superintendent

JEFFERSON
Elementary School District

Governing Board
Shakeel Ali
Marie Brizuela
Clayton Koo
Manufou Liaiga-Anoa'i
Maybelle Manio

Superintendent
Bernardo Vidales

November 18, 2020

Via Email (grandjury@sanmateocourt.org)

The Honorable Danny Y. Chou
Judge of the Superior Court
c/o Jenarda Dubois
Hall of Justice
400 County Center; 2nd Floor
Redwood City, CA 94063-1655

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

Dear Judge Chou:

The Jefferson Elementary School District (the "District") has received and reviewed the 2019-2020 Grand Jury Report entitled "Ransomware: It Is Not Enough To Think You Are Protected." We appreciate the Grand Jury's interest in this matter. Having reviewed and considered the Grand Jury's Findings and Recommendations, the District responds below pursuant to section 933.05 of the California Penal Code.

Please be advised that the District presented the Grand Jury Report to its Board of Trustees, and the District's Board approved these responses, on November 18, 2020

Findings:

1. *Ransomware is a real and growing threat to public entities including those in San Mateo County.*

The District agrees with this Finding.

2. *Across the country, local governments and schools represent 12% of all Ransomware attacks.*

The District lacks information to fully agree or disagree with this Finding given that it did not conduct the research related to this Report. The District, however, accepts the Grand Jury's Finding for the purposes of this Response.

3. *The direct and indirect costs of Ransomware can be significant.*

The District agrees with this Finding.

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

The District agrees with this Finding.

5. *A comprehensive Cybersecurity 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.

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.

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

The District lacks information to fully agree or disagree with this Finding given that it did not conduct the research related to this Report. The District, however, accepts the Grand Jury's Finding for the purposes of this Response.

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.

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:*
    1. *System Security (Firewalls, Anti-malware/Antivirus software, use of subnets, strong password policies, updating/patching regularly)*
    2. *Backup & Recovery (In the event of an attack, 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?)*
    3. *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)*

The District implemented this Recommendation on November 5, 2020 by directing the District's IT Department to prepare a confidential report which addresses the three concerns specifically identified above.

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 this Recommendation, 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.

3. *Given the results of their internal reports, governmental entities may choose to request further guidance by means of a Cybersecurity review from the U.S. Department of Homeland Security and/or a cyber hygiene assessment from the County Controller's Office.*

The District will implement this Recommendation if warranted and appropriate based on the results of the District's confidential internal report.

4. *Given the results of their internal reports, governmental entities may choose to ask their IT departments to review their own Cybersecurity Plan with the detailed template provided by the FCC's Cybersecurity Planning Guide and consider customizing it using FCC's Create Custom Cybersecurity Planning Guide tool (see footnote 52).*

The District will implement this Recommendation if warranted and appropriate based on the results of the District's confidential internal report.

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

Sincerely,

Bernardo Vidales
Superintendent
Jefferson Elementary School District

Jefferson Union High School District

ADMINISTRATIVE OFFICES – SERRAMONTE DEL REY
699 Serramonte Boulevard, Suite 100
Daly City, CA 94015-4132
650-550-7900 • FAX 650-550-7888

Board of Trustees
Andrew Lie
Carla Ng-Garrett
Nick Occhipinti
Kalimah Y. Salahuddin
Rosie U. Tejada

Dr. Terry A. Deloria
Superintendent

November 3, 2020

Via Email (grandjury@sanmateocourt.org)

The Honorable Danny Y. Chou
Judge of the Superior Court
c/o Jenarda Dubois
Hall of Justice
400 County Center; 2nd Floor
Redwood City, CA 94063-1655

Re: Response to the 2019-2020 Grand Jury Report entitled "Ransomware: It Is Not Enough to Think You Are Protected."

Dear Judge Chou:

The Jefferson Union High School District (the "District") has received and reviewed the 2019-2020 Grand Jury Report entitled "Ransomware: It Is Not Enough To Think You Are Protected." We appreciate the Grand Jury's interest in this matter. Having reviewed and considered the Grand Jury's Findings and Recommendations, the District responds below pursuant to section 933.05 of the California Penal Code.

Please be advised that the District presented the Grand Jury Report to its Board of Trustees, and the District's Board approved these responses, on November 2, 2020

Findings:

1. *Ransomware is a real and growing threat to public entities including those in San Mateo County.*

The District agrees with this Finding.

2. *Across the country, local governments and schools represent 12% of all Ransomware attacks.*

The District lacks information to fully agree or disagree with this Finding given that it did not conduct the research related to this Report. The District, however, accepts the Grand Jury's finding for the purposes of this Response.

3. *The direct and indirect costs of Ransomware can be significant.*

The District agrees with this Finding.

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

The District agrees with this Finding.

5. *A comprehensive Cybersecurity 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.

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.

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

The District lacks information to fully agree or disagree with this Finding given that it did not conduct the research related to this Report. The District, however, accepts the Grand Jury's finding for the purposes of this Response.

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.

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:*
    1. *System Security (Firewalls, Anti-malware/Antivirus software, use of subnets, strong password policies, updating/patching regularly)*
    2. *Backup & Recovery (In the event of an attack, 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?)*
    3. *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)*

The District implemented this Recommendation on February 19, 2020 by directing the District's IT Department to prepare a confidential report which addresses the three concerns specifically identified above with the exception of *providing employee training on phishing.* The District intends to implement this Recommendation by June 30, 2021.

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 this Recommendation, 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.

3. *Given the results of their internal reports, governmental entities may choose to request further guidance by means of a Cybersecurity review from the U.S. Department of Homeland Security and/or a cyber hygiene assessment from the County Controller's Office.*

The District will implement this Recommendation if warranted and appropriate based on the results of the District's confidential internal report.

4. *Given the results of their internal reports, governmental entities may choose to ask their IT departments to review their own Cybersecurity Plan with the detailed template provided by the FCC's Cybersecurity Planning Guide and consider customizing it using FCC's Create Custom Cybersecurity Planning Guide tool (see footnote 52).*

The District will implement this Recommendation if warranted and appropriate based on the results of the District's confidential internal report.

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

Sincerely,

Dr. Terry A. Deloria
Superintendent
Jefferson Union High School District

LA HONDA-PESCADERO UNIFIED SCHOOL DISTRICT
PO Box 189 • 360 Butano Cut Off, Pescadero, CA 94060
650-879-0286 • FAX 650-879-0816

Amy Wooliever, Superintendent

December 11, 2020

Via Email (grandjury@sanmateocourt.org)

The Honorable Danny Y. Chou
Judge of the Superior Court
c/o Jenarda Dubois
Hall of Justice
400 County Center; 2nd Floor
Redwood City, CA 94063-1655

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

Dear Judge Chou:

The La Honda-Pescadero Unified School District (the "District") has received and reviewed the 2019-2020 Grand Jury Report entitled "Ransomware: It Is Not Enough To Think You Are Protected." We appreciate the Grand Jury's interest in this matter. Having reviewed and considered the Grand Jury's Findings and Recommendations, the District responds below pursuant to section 933.05 of the California Penal Code.

Please be advised that the District presented the Grand Jury Report to its Board of Trustees, and the District's Board approved these responses, on December 15, 2020.

Findings:

1. *Ransomware is a real and growing threat to public entities including those in San Mateo County.*

The District agrees with this Finding.

2. *Across the country, local governments and schools represent 12% of all Ransomware attacks.*

The District lacks information to fully agree or disagree with this Finding given that it did not conduct the research related to this Report. The District, however, accepts the Grand Jury's Finding for the purposes of this Response.

3. *The direct and indirect costs of Ransomware can be significant.*

The District agrees with this Finding.

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

The District agrees with this Finding.

5. *A comprehensive Cybersecurity 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.

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.

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

The District lacks information to fully agree or disagree with this Finding given that it did not conduct the research related to this Report. The District, however, accepts the Grand Jury's Finding for the purposes of this Response.

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.

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:*
    1. *System Security (Firewalls, Anti-malware/Antivirus software, use of subnets, strong password policies, updating/patching regularly)*
    2. *Backup & Recovery (In the event of an attack, 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?)*
    3. *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)*

The District implemented this Recommendation on December 11th, by requesting the District's Facility Director to prepare a confidential report which addresses the three concerns specifically identified above. The District does not have an IT Department.

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 this Recommendation, 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.

3. *Given the results of their internal reports, governmental entities may choose to request further guidance by means of a Cybersecurity review from the U.S. Department of Homeland Security and/or a cyber hygiene assessment from the County Controller's Office.*

The District will implement this Recommendation if warranted and appropriate based on the results of the District's confidential internal report.

4. *Given the results of their internal reports, governmental entities may choose to ask their IT departments to review their own Cybersecurity Plan with the detailed template provided by the FCC's Cybersecurity Planning Guide and consider customizing it using FCC's Create Custom Cybersecurity Planning Guide tool (see footnote 52).*

The District will implement this Recommendation if warranted and appropriate based on the results of the District's confidential internal report.

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

Sincerely,

Amy Wooliever
Superintendent
La Honda-Pescadero Unified School District

Ladera Recreation District
150 Andeta Way
Portola Valley, CA 94028

Response to Grand Jury Report re: Ransomware
December 14, 2020
Hon. Danny Y. Chou
Judge of the Superior Court
c/o Jenarda Dubois
Hall of Justice
400 County Center; 8th Floor
Redwood City, CA 94063-1655

Dear Judge Chou:

The Ladera Recreation District has had an opportunity to review the 2020 Grand Jury report entitled "Ransomware: It is Not Enough to Think You Are Protected." The Board, after reviewing the report and allowing for public comment at its Ladera Recreation District meeting on December 23, 2020 offers the following responses:

Responses to Findings

Finding F1. Ransomware is a real and growing threat to public entities including those in San Mateo County.

***Response**: The District agrees with the finding.*

Finding F2. Across the country, local governments and schools represent 12% of all Ransomware attacks.

***Response**: The District lacks the information to fully agree or disagree with this finding, but for purposes of this response, the District accepts the Grand Jury's findings.*

Finding F3. The direct and indirect costs of Ransomware can be significant.

***Response**: The District agrees with the finding.*

Finding F4. Cybersecurity reviews and assessments, and an updated, well-executed Cybersecurity plan, are critical components of IT security strategy.

***Response**: The District agrees with the finding.*

Finding F5. A comprehensive Cybersecurity plan should include, at a minimum, information concerning prevention steps, spam and malware software, and backups and full recovery testing.

Response: *The District agrees with the finding.*

Finding F6. The identification of phishing attempts, including the use of spam filters, is an important component to protecting an IT system from Ransomware attacks.

Response*: The District agrees with the finding.*

Finding F7. 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.

Response: *The District agrees with the finding.*

Finding F8. Training of new employees, and the recurring training of existing employees, is an important component of defense against Ransomware.

Response: *The District agrees with the finding.*

Response to Recommendations

R1. 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:

1. System Security (Firewalls, Anti-malware/Antivirus software, use of subnets, strong password policies, updating/patching regularly)

2. Backup & Recovery (In the event of an attack, 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?)

3. 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)

Response*: The recommendation has been implemented.*

R2. 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.

Response: *The recommendation will be implemented within the requested timeframe.*

R3. Given the results of their internal reports, governmental entities may choose to request further guidance by means of a Cybersecurity review from the U.S. Department of Homeland Security and/or a cyber hygiene assessment from the County Controller's Office.

Response: *If necessary, the recommendation will be implemented within the requested timeframe.*

R4. Given the results of their internal reports, governmental entities may choose to ask their IT departments to review their own Cybersecurity Plan with the detailed template provided by the FCC's Cybersecurity Planning Guide and consider customizing it using FCC's Create Custom Cybersecurity Planning Guide tool (see footnote 52).

Response: *If necessary, the recommendation will be implemented within the requested timeframe.*

Respectfully submitted,

Diane Gow
General Manager
Ladera Recreation District

Cc: grandjury@sanmateocourt.org

District Office
1011 Altschul Avenue
Menlo Park, CA 94025
(650) 854-6311

Las Lomitas School
299 Alameda de las Pulgas
Atherton, CA 94027
(650) 854-5900

La Entrada School
2200 Sharon Road
Menlo Park, CA 94025
(650) 854-3962

December 15, 2020

The Honorable Danny Y. Chou
Judge of the Superior Court
c/o Jenarda Dubois
Hall of Justice
400 County Center; 2nd Floor
Redwood City, CA 94063-1655

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

Dear Judge Chou:

The Las Lomitas Elementary School District (the "District") has received and reviewed the 2019-2020 Grand Jury Report entitled "Ransomware: It Is Not Enough To Think You Are Protected." We appreciate the Grand Jury's interest in this matter. Having reviewed and considered the Grand Jury's Findings and Recommendations, the District responds below pursuant to section 933.05 of the California Penal Code.

As required, the District presented the Grand Jury Report to its Board of Trustees, and the District's Board of Trustees approved these responses on December 14, 2020.

Findings:

F1. Ransomware is a real and growing threat to public entities including those in San Mateo County.

The District agrees with this Finding.

F2. Across the country, local governments and schools represent 12% of all Ransomware attacks.

The District lacks information to fully agree or disagree with this Finding given that it did not conduct the research related to this Report. The District, however, accepts the Grand Jury's Finding for the purposes of this Response.

F3. The direct and indirect costs of Ransomware can be significant.

The District agrees with this Finding.

F4. Cybersecurity reviews and assessments, and an updated, well-executed Cybersecurity plan, are critical components of IT security strategy.

The District agrees with this Finding.

F5. A comprehensive Cybersecurity 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.

F6. 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.

F7. Testing a full restore of a server to ensure that backups are reliable should be undertaken regularly as part an entity's backup plan to recover lost information.

The District lacks information to fully agree or disagree with this Finding given that it did not conduct the research related to this Report. The District, however, accepts the Grand Jury's Finding for the purposes of this Response.

F8. 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.

Recommendations:

R1. 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:

1. *System Security (Firewalls, Anti-malware/Antivirus software, use of subnets, strong password policies, updating/patching regularly)*
2. *Backup & Recovery (In the event of an attack, 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?)*
3. *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)*

The District implemented this Recommendation on November 30, 2020 by directing the District's IT Department to prepare a confidential report which addresses the three concerns specifically identified above.

R2. 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 this Recommendation. Depending on the scope, complexity, and feasibility of the recommended actions and/or enhancements required, the implementation schedule of some items (e.g. those which require user training) may extend into the 2021-2022 school year.

R3. Given the results of their internal reports, governmental entities may choose to request further guidance by means of a Cybersecurity review from the U.S. Department of Homeland Security and/or a cyber hygiene assessment from the County Controller's Office.

The District will implement this Recommendation to request further guidance if warranted and appropriate based on the results of the District's confidential internal report.

R4. Given the results of their internal reports, governmental entities may choose to ask their IT departments to review their own Cybersecurity Plan with the detailed template provided by the FCC's Cybersecurity Planning Guide and consider customizing it using FCC's Create Custom Cybersecurity Planning Guide tool (see footnote 52).

The District will implement this Recommendation to use the FCC's Cybersecurity Planning Guide if warranted and appropriate based on the results of the District's confidential internal report.

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

Sincerely,

Dr. Beth Polito
Superintendent
Las Lomitas Elementary School District

Menlo Park City School District
181 Encinal Avenue
Atherton, CA 94027
Phone (650) 321-7140
Fax (650) 321-7184
www.mpcsd.org

MENLO PARK CITY SCHOOL DISTRICT

November 12, 2020

BOARD APPROVED
NOV 12 2020
MENLO PARK
CITY SCHOOL DISTRICT

Via Email (grandjury@sanmateocourt.org)

The Honorable Danny Y. Chou
Judge of the Superior Court
c/o Jenarda Dubois
Hall of Justice
400 County Center; 2nd Floor
Redwood City, CA 94063-1655

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

Dear Judge Chou:

The Menlo Park City School District (the "District") has received and reviewed the 2019-2020 Grand Jury Report entitled "Ransomware: It Is Not Enough To Think You Are Protected." We appreciate the Grand Jury's interest in this matter. Having reviewed and considered the Grand Jury's Findings and Recommendations, the District responds below pursuant to section 933.05 of the California Penal Code.

Please be advised that the District presented the Grand Jury Report to its Board of Trustees, and the District's Board approved these responses, on November 12, 2020.

Findings:

1. *Ransomware is a real and growing threat to public entities including those in San Mateo County.*

The District agrees with this Finding.

1. *Across the country, local governments and schools represent 12% of all Ransomware attacks.*

The District lacks information to fully agree or disagree with this Finding given that it did not conduct the research related to this Report. The District, however, accepts the Grand Jury's Finding for the purposes of this Response.

1. *The direct and indirect costs of Ransomware can be significant.*

The District agrees with this Finding.

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

The District agrees with this Finding.

1. *A comprehensive Cybersecurity 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.

1. *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.

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

The District lacks information to fully agree or disagree with this Finding given that it did not conduct the research related to this Report. The District, however, accepts the Grand Jury's Finding for the purposes of this Response.

1. *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.

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:*
    1. *System Security (Firewalls, Anti-malware/Antivirus software, use of subnets, strong password policies, updating/patching regularly)*
    2. *Backup & Recovery (In the event of an attack, 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?)*
    3. *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)*

The District implemented this Recommendation on November 12, 2020 by directing the District's IT Department to prepare a confidential report which addresses the three concerns specifically identified above.

1. *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 this Recommendation, 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.

1. *Given the results of their internal reports, governmental entities may choose to request further guidance by means of a Cybersecurity review from the U.S. Department of Homeland Security and/or a cyber hygiene assessment from the County Controller's Office.*

The District will implement this Recommendation if warranted and appropriate based on the results of the District's confidential internal report.

1. *Given the results of their internal reports, governmental entities may choose to ask their IT departments to review their own Cybersecurity Plan with the detailed template provided by the FCC's Cybersecurity Planning Guide and consider customizing it using FCC's Create Custom Cybersecurity Planning Guide tool (see footnote 52).*

The District will implement this Recommendation if warranted and appropriate based on the results of the District's confidential internal report.

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

Sincerely,

Erik Burmeister
Superintendent
Menlo Park City School District

Menlo Park Fire Protection District

170 Middlefield Road · Menlo Park, CA 94025 · Tel: 650.688.8400 · Fax: 650.323.9129
Website: www.menlofire.org · Email: mpfd@menlofire.org

Fire Chief
Harold Schapelhouman

Board of Directors
Robert Jones
Jim McLaughlin
Chuck Bernstein
Virginia Chang Kiraly
Robert J. Silano

December 15, 2020

Honorable Danny Y. Chou
Judge of the Superior Court
c/o Jenarda Dubois
Hall of Justice
400 County Center, 8th Floor
Redwood City, CA. 94063-1655

Re: Grand Jury Report "Ransomware: It Is Not Enough To Think You Are Protected"

Honorable Judge Chou:

The Menlo Park Fire Protection District (District) received the 2019-2020 Grand Jury report entitled "Ransomware: It Is Not Enough To Think You Are Protected." The District's Board of Directors reviewed the report and approved this response at the December 15, 2020, regular Board meeting. This letter responds to all of the Civil Grand Jury's findings and recommendations in the report.

Responses to Findings:

The District agrees with findings F1 and F3-F8. With regard to finding F2, the District agrees that local governments and schools across the country are involved in Ransomware attacks. However, the District does not have sufficient information to know the percentage of Ransomware attacks that local governments and schools represent.

Responses to Recommendations:

R1. 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:

1. System Security (Firewalls, Anti-malware/ Antivirus software, use of subnets, strong password policies, updating/patching regularly)

2. Backup & Recovery (In the event of an attack, 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?)
3. 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)

Response 1: Recommendation R1 has been implemented. The District has requested a report from its IT department by the required deadline that addresses system security, backup and recovery, and prevention.

R2. 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.

Response 2: Recommendation R2 has not yet been implemented, but will be implemented by June 30, 2021.

R3. Given the results of their internal reports, governmental entities may choose to request further guidance by means of a Cybersecurity review from the U.S. Department of Homeland Security and/or a cyber hygiene assessment from the County Controller's Office.

Response 3: Recommendation R3 requires further analysis, and will be evaluated upon receipt of the report from the District's IT department. If the District chooses to request further guidance from the U.S. Department of Homeland Security or the County Controller's Office, it will do so by June 30, 2021.

R4. Given the results of their internal reports, governmental entities may choose to ask their IT departments to review their own Cybersecurity Plan with the detailed template provided by the FCC's Cybersecurity Planning Guide and consider customizing it using FCC's Create Custom Cybersecurity Planning Guide tool.

Response 4: Recommendation R4 requires further analysis, and will be evaluated upon receipt of the report from the District's IT consultant. If the District chooses to request its IT department to review the District's cybersecurity plan with the FCC's Cybersecurity Planning Guide and customizing the plan using FCC's Create Custom Cybersecurity Planning Guide tool, it will do so by June 30, 2021.

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

Sincerely,

Harold Schapelhouman

Harold Schapelhouman
Fire Chief
Menlo Park Fire Protection District

March 24, 2021

Honorable Danny Y. Chou
Judge of the Superior Court
c/o Jenarda Dubois
Hall of Justice
400 County Center, 8th Floor
Redwood City, CA 94063-1655

Dear Judge Chou,

We are in receipt of the Civil Grand Jury report entitled, "Ransomware: It Is Not Enough To Think You Are Protected" (Report).

As a preliminary matter, the transmittal of the Grand Jury Report did not specify that the Midpeninsula Regional Open Space District ("District") was required to provide a response, but it is pleased to do so, pursuant to a follow up letter from the Grand Jury Coordinator dated February 22, 2021. The District's Board of Directors held a public meeting on March 24, 2021 and approved this response.

Also of note, the Report states that in 2019, all local agencies in San Mateo County were contacted via an online survey about ransomware. The District has no record of being contacted or receiving a survey on this topic. We respectfully request confirmation that you have our correct mailing address, as noted on this letterhead. Future mailings should be sent in C/O the General Manager. Email copies can also be sent to info@openspace.org.

The District responds to the Grand Jury's recommendations as follows:

Findings

The District generally agrees with the Findings of the Grand Jury.

Recommendations

R1. Each of the governmental entities in San Mateo County with an IT department or IT function should make a request for a report from their IT organization that addresses the concerns identified in the report, specifically:

1. System Security (Firewalls, Anti-malware/Antivirus software, use of subnets, strong password policies, updating/patching regularly)
2. Backup & Recovery (In the event of an attack, 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?)
3. 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)

District Response: The District has implemented this recommendation by directing the District's Information Systems and Technology Department to prepare a confidential report addressing concerns specifically identified in this recommendation. Moreover, the District has been aggressively implementing numerous cybersecurity measures, in particular over the last three years, given the rise of ransomware, phishing, and hacking attempts that have been known to unfortunately occur with other public agencies.

R2. 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.

Response: This recommendation will be implemented by June 30, 2021.

R3. Given the results of their internal reports, governmental entities may choose to request further guidance by means of a Cybersecurity review from the U.S. Department of Homeland Security and/or a cyber hygiene assessment from the County Controller's Office.

Response: The District appreciates the suggestion to request further guidance from these entities. The recommendation has not yet been implemented and will be considered after the confidential internal report is issued to the governing body.

R4. Given the results of their internal reports, governmental entities may choose to ask their IT departments to review their own Cybersecurity Plan with the detailed template provided by the FCC's Cybersecurity Planning Guide and consider customizing it using FCC's Create Custom Cybersecurity Planning Guide tool.

Response: The District will implement this recommendation as appropriate. After providing a written report to the Board of Directors, the District's Information Systems and Technology Department will make a recommendation to the General Manager whether the FCC's Planning Guide tool, or a cyber security audit, best meets District needs.

Very truly yours,

Curt Riffle, Board President
Midpeninsula Regional Open Space District

Cc: Board of Directors, Midpeninsula Regional Open Space District
Ana M. Ruiz, General Manager

MID-PENINSULA
WATER DISTRICT

3 Dairy Lane, Belmont, CA 94002
tel: 650.591.8941 fax: 650.591.4998 MidPeninsulaWater.org

December 18, 2020

Hon. Danny Y. Chou
Judge of the Superior Court
c/o Jenarda Dubois
Hall of Justice
400 County Center, 8th Floor
Redwood City, CA 94063-1655

Re: Response by Mid-Peninsula Water District to Grand Jury Report Entitled "Ransomware: It is Not Enough to Think You Are Protected" issued October 7, 2020

Honorable Chou:

The Mid-Peninsula Water District (MPWD) has reviewed and considered the referenced Grand Jury report, and responds to the report's findings and recommendations as follows:

RESPONSES TO FINDINGS:
The MPWD cannot agree or disagree with Findings F1 through F3 without undertaking independent research and analysis.

The MPWD generally agrees with Findings F4 through F8.

RESPONSES TO RECOMMENDATIONS:
Response to R1: The recommendation has been implemented. The MPWD requested the CONFIDENTIAL internal report from its IT consultant.

Response to R2: The recommendation has not been implemented but the CONFIDENTIAL internal report will be provided to the MPWD Board of Directors by June 30, 2021.

Response to R3: The recommendation requires further analysis and will be evaluated upon receipt of the CONFIDENTIAL internal report from the MPWD's IT consultant. If the MPWD chooses to request further guidance from the U.S. Department of Homeland Security or the County's Controller's Office, it will do so by June 30, 2021.

Response to R4: The recommendation requires further analysis and will be evaluated upon receipt of the CONFIDENTIAL internal report from the MPWD's IT consultant. If the MPWD chooses to request its IT consultant to review the MPWD's cybersecurity plan with the template provided by the FCC's Cybersecurity Planning Guide and/or customize the MPWD's plan using the FCC's Create Custom Cybersecurity Planning Guide tool, it will do so by June 30, 2021.

This response was considered and approved by the MPWD Board of Directors at its regularly scheduled meeting on Thursday, December 17, 2020.

Sincerely,

Tammy A. Rudock
General Manager

Millbrae School District *Together We Achieve The Extraordinary!*
555 Richmond Drive, Millbrae, CA 94030
650-697-5693 • 650-697-6865 (fax) • http://www.millbraeschooldistrict.org

DEBRA FRENCH
Superintendent

DR. MARIA SANTA CRUZ
Chief Business Officer

TARA KEITH
Director of Student Services

December 15, 2020

Via Email (grandjury@sanmateocourt.org)

The Honorable Danny Y. Chou
Judge of the Superior Court
c/o Jenarda Dubois
Hall of Justice
400 County Center; 2nd Floor
Redwood City, CA 94063-1655

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

Dear Judge Chou:

The Millbrae School (the "District") has received and reviewed the 2019-2020 Grand Jury Report entitled "Ransomware: It Is Not Enough To Think You Are Protected." We appreciate the Grand Jury's interest in this matter. Having reviewed and considered the Grand Jury's Findings and Recommendations, the District responds as follows, pursuant to section 933.05 of the California Penal Code.

FINDINGS

1. *Ransomware is a real and growing threat to public entities including those in San Mateo County.*

The District agrees with this finding.

2. *Across the country,local governments and schools represent 12% of all Ransomware attacks.*

The District cannot agree or disagree with this Finding, as the District did not conduct the research cited in the Report on which this Finding is based. The District therefore defers to the Grand Jury with regard to this Finding.

3. *The direct and indirect costs of Ransomware can be significant.*

The District agrees with this Finding.

Millbrae School District *Together We Achieve The Extraordinary!*
555 Richmond Drive, Millbrae, CA 94030
650-697-5693 • 650-697-6865 (fax) • http://www.millbraeschooldistrict.org

DEBRA FRENCH
Superintendent

DR. MARIA SANTA CRUZ
Chief Business Officer

TARA KEITH
Director of Student Services

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

The District agrees with this Finding.

5. *A comprehensive Cybersecurity 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.

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.

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

The District agrees with this Finding.

8. *The resources of the SMCDC, which identifies and tracks measles cases in San Mateo County, may be inadequate to contain a major outbreak.*

The District cannot agree or disagree with this Finding, as the District did not conduct the research cited in the Report on which this Finding is based. The District therefore defers to the Grand Jury with regard to this Finding.

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:*
1. System Security (Firewalls, Anti-malware/Antivirus software, use of subnets, strong password policies, updating/patching regularly)
2. Backup & Recovery (In the event of an attack, 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?)

Millbrae School District *Together We Achieve The Extraordinary!*
555 Richmond Drive, Millbrae, CA 94030
650-697-5693 • 650-697-6865 (fax) • http://www.millbraeschooldistrict.org

DEBRA FRENCH
Superintendent

DR. MARIA SANTA CRUZ
Chief Business Officer

TARA KEITH
Director of Student Services

3. 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)

The District implemented this Recommendation on December 15, 2020 by directing the District's IT Department to prepare a confidential report which addresses the three concerns specifically identified above.

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 this Recommendation, 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.

3. *Given the results of their internal reports, governmental entities may choose to request further guidance by means of a Cybersecurity review from the U.S. Department of Homeland Security and/or a cyber hygiene assessment from the County Controller's Office.*

The District will implement the Recommendation if warranted and appropriate based on the results of the District's confidential internal report.

4. *Given the results of their internal reports, governmental entities may choose to ask their IT department to review their own Cybersecurity Plan with the detailed template provided by the FCC's Cybersecurity Planning Guide and consider customizing it using FCC's Create Custom Cybersecurity Planning Guide tool (see footnote 52).*

The District will implement the Recommendation if warranted and appropriate based on the results of the District's confidential internal report..

Please be advised that Both the Grand Jury Report and the District's responses were presented to and approved by the District's Governing Board on December 15, 2020.

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

Sincerely,

Millbrae School District

Together We Achieve The Extraordinary!

555 Richmond Drive, Millbrae, CA 94030

650-697-5693 • 650-697-6865 (fax) • http://www.millbraeschooldistrict.org

DEBRA FRENCH
Superintendent

DR. MARIA SANTA CRUZ
Chief Business Officer

TARA KEITH
Director of Student Services

Debra French
Superintendent
Millbrae School District

Montara Water & Sanitary District

Serving the Communities of Montara and Moss Beach

P.O. Box 370131
8888 Cabrillo Highway
Montara, CA 94037-0131

Tel: (650) 728-3545
Fax: (650) 728-8556
E-mail: mwsd@coastside.net

Visit Our Web Site: http://www.mwsd.montara.com

March 22, 2021

Via Email (grandjury@sanmateocourt.org)
The Honorable Danny Y. Chou
Judge of the Superior Court
c/0 Jenarda Dubois
Hall of Justice
400 County Center; 2nd Floor
Redwood City, California 94063-1655

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

Dear Judge Chou,

The Montara Water and Sanitary District (MWSD) has received and reviewed the 2019-2020 Grand Jury Report entitled "Ransomware: It Is Not Enough To Think You Are Protected." We appreciate the Grand Jury's interest in this matter. Having reviewed and Considered the Grand Jury's Findings and Recommendations, the District responds below pursuant to section 933.05 of the California Penal Code.

MWSD presented the Grand Jury Report to its Board of Directors, and the District's Board approved these responses, on March 18, 2021.

Findings

1. *Ransomware is a real and growing threat to public entities including those in San Mateo County*

   MWSD agrees with this Finding

2. *Across the country, local governments and schools represent 12% of all Ransomware attacks*

   MWSD lacks information to fully agree or disagree with this Finding however we recognize that local governments and schools are likely to be targeted by Ransomware attacks.

3. *The direct and indirect costs of Ransomware can be significant*

   MWSD agrees with this Finding

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

   MWSD agrees with this Finding

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

   MWSD agrees with this Finding

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

   MWSD agrees with this Finding

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 data.*

   MWSD agrees with this Finding in principle but recognizes that regular full hardware restoration may be impractical due to hardware, logistical and budget restraints. Partial data only restores may be more appropriate.

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

   MWSD agrees with this Finding

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:*
    1. *System Security (Firewalls, Anti-malware/Antivirus software, use of subnets, strong password policies, updating/patching regularly)*
    2. *Backup & Recovery (In the event of an attack, can you shut down your system quickly? What is being backed up, how it is being backed up, when are the backups run, and where are the backups being stored? Have backups been tested? Can you fully restore a Server from a Backup?)*
    3. *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)*

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.*

   MWSD has implemented these Recommendation by requesting a confidential report which addresses the three concerns specifically identified above. The report will be provided to the governing board by June 30, 2021.

3. *Given the results of their internal reports, governmental entities may choose to request further guidance by means of a Cybersecurity review from the U.S. Department of Homeland Security and/or a cyber hygiene assessment from the County Controller's Office*

   MWSD will implement this Recommendation if warranted based on the district's confidential internal report.

4. *Given the results of their internal reports, governmental entities may choose to ask their IT departments to review their own Cybersecurity Plan with the detailed template provided by the FCC's Cybersecurity Planning Guide and consider customizing it using FCC's Create Custom Cybersecurity Planning Guide tool (see footnote 52).*

   MWSD will implement this Recommendation if warranted and appropriate based on the results of the District's confidential internal report.

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

Sincerely,

Clemens Heldmaier
General Manager
Montara Water and Sanitary District

2400 Francisco Blvd.
P.O. Box 1039
Pacifica, CA 94044
www.nccwd.com

Phone (650) 355-3462
Fax (650 355-0735

December 18, 2020

Honorable Donny Y. Chou
Judge of the Superior Court
c/o Jenarda Dubois
Hall of Justice
400 County Center, 2nd Floor
Redwood City, CA 94063-1655

Subject: North Coast County Water District Response to Grand Jury Report: "Ransomware: It Is Not Enough To Think You Are Protected"

Honorable Donny Y. Chou:

The North Coast County Water District (District) hereby submits its responses to the findings and recommendations of the Grand Jury regarding its review of the Grand Jury Report: "Ransomware: It Is Not Enough To Think You Are Protected." The District's Board of Directors reviewed the report and approved this response at the December 16 regular Board meeting. The Grand Jury made eight (8) findings and four (4) recommendations. Each finding and recommendation will be addressed separately.

Findings

F1. Ransomware is a real and growing threat to public entities including those in San Mateo County.

The District agrees with the finding.

F2. Across the country, local governments and schools represent 12% of all Ransomware attacks.

The District agrees that local governments and schools across the country are involved in Ransomware attacks, however the District does not have sufficient information to know the percentage of Ransomware attacks that local governments and schools represent.

F3. The direct and indirect costs of Ransomware can be significant.

The recommendation has been implemented. The District has an outside third-party IT consultant and, prior to November 30, 2020, requested a report from the IT consultant that addresses system security, backup and recovery, and prevention.

R2. 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.

Recommendation R2 has not yet been implemented, but will be implemented by June 30, 2021.

R3. Given the results of their internal reports, governmental entities may choose to request further guidance by means of a Cybersecurity review from the U.S. Department of Homeland Security and/or a cyber hygiene assessment from the County Controller's Office.

Recommendation R3 requires further analysis, and will be evaluated upon receipt of the report from the District's IT consultant. If the District chooses to request further guidance from the U.S. Department of Homeland Security or the County Controller's Office, it will do so within two months of receiving the IT consultant's report.

R4. Given the results of their internal reports, governmental entities may choose to ask their IT departments to review their own Cybersecurity Plan with the detailed template provided by the FCC's Cybersecurity Planning Guide and consider customizing it using FCC's Create Custom Cybersecurity Planning Guide tool.

Recommendation R4 requires further analysis, and will be evaluated upon receipt of the report from the District's IT consultant. If the District chooses to request its IT consultant to review the District's cybersecurity plan with the FCC's Cybersecurity Planning Guide and customizing the plan using FCC's Create Custom Cybersecurity Planning Guide tool, it will do so within two months of receiving the IT consultant's report.

The District appreciates this opportunity to respond to the Grand Jury report on the Ransomware attacks and the importance of cybersecurity. Should you require any additional information please do not hesitate to contact Adrianne Carr, General Manager at (650) 355-3462 or at acarr@nccwd.com.

Sincerely,

Anne DeJarnatt

Anne DeJarnatt, President
Board of Directors
North Coast County Water District

cc: Board of Directors
Adrianne Carr, General Manager

PACIFICA
SCHOOL DISTRICT

Pacifica School District

375 Reina Del Mar Avenue ★ Pacifica, California ★ 94044
(650) 738-6600 ★ (650) 557-9672 (fax)

Preparing Students for an Evolving World

www.pacificasd.org

District Administration
Heather Olsen, Ed.D.
Superintendent
Julie Carrillo
Director,
Special Education, and Student Services
Will Lucey
Director,
Educational Support Services
Alexis O'Flaherty
Director,
Human Resources
Josephine Peterson
Chief Business Official

November 19, 2020

Via Email (grandjury@sanmateocourt.org)

The Honorable Danny Y. Chou
Judge of the Superior Court
c/o Jenarda Dubois
Hall of Justice
400 County Center; 2nd Floor
Redwood City, CA 94063-1655

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

Dear Judge Chou:

The Pacifica School District (the "District") has received and reviewed the 2019-2020 Grand Jury Report entitled "Ransomware: It Is Not Enough To Think You Are Protected." We appreciate the Grand Jury's interest in this matter. Having reviewed and considered the Grand Jury's Findings and Recommendations, the District responds below pursuant to section 933.05 of the California Penal Code.

Please be advised that the District presented the Grand Jury Report to its Board of Trustees, and the District's Board approved these responses, on November 18, 2020.

Findings:

1. *Ransomware is a real and growing threat to public entities including those in San Mateo County.*

   The District agrees with this Finding.

2. *Across the country, local governments and schools represent 12% of all Ransomware attacks.*

   The District lacks information to fully agree or disagree with this Finding given that it did not conduct the research related to this Report. The District, however, accepts the Grand Jury's Finding for the purposes of this Response.

3. *The direct and indirect costs of Ransomware can be significant.*

   The District agrees with this Finding.

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

   The District agrees with this Finding.

5. *A comprehensive Cybersecurity 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.

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.

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

   The District lacks information to fully agree or disagree with this Finding given that it did not conduct the research related to this Report. The District, however, accepts the Grand Jury's Finding for the purposes of this Response.

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.

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:*

1. *System Security (Firewalls, Anti-malware/Antivirus software, use of subnets, strong password policies, updating/patching regularly)*
2. *Backup & Recovery (In the event of an attack, 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?)*
3. *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)*

The District implemented this Recommendation on November 10, 2020 by directing the District's IT Department to prepare a confidential report which addresses the three concerns specifically identified above.

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 this Recommendation, 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.

3. *Given the results of their internal reports, governmental entities may choose to request further guidance by means of a Cybersecurity review from the U.S. Department of Homeland Security and/or a cyber hygiene assessment from the County Controller's Office.*

   The District will implement this Recommendation if warranted and appropriate based on the results of the District's confidential internal report.

4. *Given the results of their internal reports, governmental entities may choose to ask their IT departments to review their own Cybersecurity Plan with the detailed template provided by the FCC's Cybersecurity Planning Guide and consider customizing it using FCC's Create Custom Cybersecurity Planning Guide tool (see footnote 52).*

   The District will implement this Recommendation if warranted and appropriate based on the results of the District's confidential internal report.

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

Sincerely,

Heather Olsen, Ed.D.
Superintendent
Pacifica School District

Peninsula Health Care District

SINCE 1948 MAKING A DIFFERENCE

March 25, 2021

Mr. Neal Taniguchi
Court Executive Officer
San Mateo Superior Court
400 County Center
Redwood City, CA 94063

RE: Grand Jury Report: "Ransomware: It Is Not Enough to Think You Are Protected." Response of Peninsula Health Care District

Dear Mr. Taniguchi:

The Board of Directors and staff of the Peninsula Health Care District (the "District) have been provided with a copy of the above-referenced report from the San Mateo County Civil Grand Jury. We appreciated the thorough research and recommendations in the report.

In general, the Board agrees with the findings and recommendations in the report. The specific responses are set forth below.

The District employs an outside consultant to advise on cybersecurity and ransomware protections. As requested by the report, we reviewed the status of the District's security and backup storage with the consultant. The District was found to have robust security measures in place due to the consultant's annual review of the District's system and current knowledge of trends and technologies. He is consulted annually as part of the budget process and with the Board's approval of the budget, funding is made available to ensure the system remains "state-of-the-art". The consultant's assessment in response to the Grand Jury's "Ransomware" report found the District to be compliant with the Grand Jury's recommendations.

The District has also consulted with our bank to ensure maximum protections are in place against fraudulent check writing and hacking into wire transfer information. The bank recommended to install its "Positive Pay" system which tracks every check coming into the bank for processing against the list by date and check number provided by the District when issuing the check.

Against this background, the District responds to the findings and recommendations as follows:

FINDINGS

Finding F1. The District agrees with this finding.

Finding F2. The District agrees that local governments and school districts are frequent targets of ransomware attacks but does not have sufficient information to verify the percentage stated in the report.

Finding F3. The District agrees with this finding.

Finding F4. The District agrees with this finding.

Finding F5. The District agrees with this finding.

Finding F6. The District agrees with this finding.

Finding F7. The District agrees with this finding.

Finding F8. The District agrees with this finding.

RECOMMENDATIONS

Recommendation R1. The District agrees with this recommendation and has complied with it as of December 31, 2020.

Recommendation R2. The District agrees with this recommendation. The internal report has been provided to the Board and accepted at its regular Meeting on March 25, 2021.

Recommendation R3. In view of the responses to the first two recommendations, the District believes that this step is unnecessary.

Recommendation R4. In view of the responses to the first two recommendations, the District believes that this step is unnecessary.

This response was presented to the Board at its regular meeting on March 25, 2021 and approved.

Please let us know if there are any questions regarding the foregoing response.

Sincerely,

Lawrence W. Cappel, Chair
PHCD Board of Directors

Portola Valley School District

Ormondale School (K-3) • Corte Madera School (4-8)

Board of Trustees: Brooke Day, Anne Fazioli-Khiari, Gary Hanning, Jeff Klugman, Kimberley Morris Rosen

Roberta Zarea, Superintendent

December 18, 2020

Via Email (grandjury@sanmateocourt.org)

The Honorable Danny Y. Chou
Judge of the Superior Court
c/o Jenarda Dubois
Hall of Justice
400 County Center; 2nd Floor
Redwood City, CA 94063-1655

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

Dear Judge Chou:

The Portola Valley Elementary School District (the "District") has received and reviewed the 2019-2020 Grand Jury Report entitled "Ransomware: It Is Not Enough To Think You Are Protected." We appreciate the Grand Jury's interest in this matter. Having reviewed and considered the Grand Jury's Findings and Recommendations, the District responds below pursuant to section 933.05 of the California Penal Code.

Please be advised that the District presented the Grand Jury Report to its Board of Trustees, and the District's Board approved these responses, on December 17, 2020.

Findings:

1. ***Ransomware is a real and growing threat to public entities including those in San Mateo County.***

The District agrees with this Finding.

2. ***Across the country, local governments and schools represent 12% of all Ransomware attacks.***

The District lacks information to fully agree or disagree with this Finding given that it did not conduct the research related to this Report. The District, therefore, defers to the Grand Jury's with regard to this Finding.

3. ***The direct and indirect costs of Ransomware can be significant.***

The District agrees with this Finding.

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

The District agrees with this Finding.

5. ***A comprehensive Cybersecurity 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.

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.

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

The District lacks information to fully agree or disagree with this Finding given that it did not conduct the research related to this Report. The District, however, accepts the Grand Jury's Finding for the purposes of this Response.

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.

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:***

2. ***Backup & Recovery (In the event of an attack, 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?)***
3. ***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)***

The District implemented this Recommendation on November 1, 2020 by directing the District's IT Department to prepare a confidential report which addresses the three concerns specifically identified above.

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 this Recommendation, 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.

3. ***Given the results of their internal reports, governmental entities may choose to request further guidance by means of a Cybersecurity review from the U.S. Department of Homeland Security and/or a cyber hygiene assessment from the County Controller's Office.***

The District will implement this Recommendation if warranted and appropriate based on the results of the District's confidential internal report.

4. ***Given the results of their internal reports, governmental entities may choose to ask their IT departments to review their own Cybersecurity Plan with the detailed template provided by the FCC's Cybersecurity Planning Guide and consider customizing it using FCC's Create Custom Cybersecurity Planning Guide tool (see footnote 52).***

The District will implement this Recommendation if warranted and appropriate based on the results of the District's confidential internal report.

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

Sincerely,

Roberta Zarea

Roberta Zarea
Superintendent
Portola Valley School District

"OUR CHILDREN – OUR FUTURE"

Ravenswood City School District
ADMINISTRATIVE OFFICE
2120 Euclid Avenue, East Palo Alto, California 94303
(650) 329-2800 Fax (650) 325-3015

December 11, 2020

To: The Honorable Danny Y. Chou
Judge of the Superior Court
c/o Jenarda Dubois
Hall of Justice
400 County Center; 2nd Floor
Redwood City, CA 94063-1655

From: Gina Sudaria, Superintendent
Ravenswood City School District
2120 Euclid Avenue
East Palo Alto, CA 94303

Re: *Response to the 2019-2020 Grand Jury Report entitled "Ransomware: It Is Not Enough To Think You Are Protected."*

Attached please find the Ravenswood City School District's *Response to the 2019-2020 Grand Jury Report entitled "Ransomware: It Is Not Enough To Think You Are Protected."*

Note, the response was presented and approved by the Ravenswood City School Board during the November 19, 2020 Regular Board Meeting that is open to the public.

The response and cover memo were sent via regular mail to the address above and emailed to grandjury@sanmateocourt.org on December 11, 2020.

Thank you,

Gina Sudaria
Superintendent

"OUR CHILDREN – OUR FUTURE"

Ravenswood City School District
ADMINISTRATIVE OFFICE
2120 Euclid Avenue, East Palo Alto, California 94303
(650) 329-2800 Fax (650) 325-3015

November 20, 2020

Via Email (grandjury@sanmateocourt.org)

The Honorable Danny Y. Chou
Judge of the Superior Court
c/o Jenarda Dubois
Hall of Justice
400 County Center; 2nd Floor
Redwood City, CA 94063-1655

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

Dear Judge Chou:

The Ravenswood City School District ("District") has received and reviewed the 2019-2020 Grand Jury Report entitled "Ransomware: It Is Not Enough To Think You Are Protected." We appreciate the Grand Jury's interest in this matter. Having reviewed and considered the Grand Jury's Findings and Recommendations, the District responds below pursuant to section 933.05 of the California Penal Code.

Please be advised that the District presented the Grand Jury Report to its Board of Trustees, and the District's Board approved these responses, on November 19, 2020.

Findings:

1. Ransomware is a real and growing threat to public entities including those in San Mateo County.

The District agrees with this Finding.

2. Across the country, local governments and schools represent 12% of all Ransomware attacks.

The District lacks information to fully agree or disagree with this Finding given that it did not conduct the research related to this Report. The District, however, accepts the Grand Jury's Finding for the purposes of this Response.

3. The direct and indirect costs of Ransomware can be significant.

The District agrees with this Finding.

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

The District agrees with this Finding.

5. A comprehensive Cybersecurity 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.

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.

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

The District lacks information to fully agree or disagree with this Finding given that it did not conduct the research related to this Report. The District, however, accepts the Grand Jury's Finding for the purposes of this Response.

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.

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 attack, 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)

The District implemented this Recommendation on November 19, 2020 by directing the District's IT Department to prepare a confidential report which addresses the three concerns specifically identified above.

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 this Recommendation, 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, and any delays necessitated by the ongoing COVID-19 pandemic.

3. Given the results of their internal reports, governmental entities may choose to request further guidance by means of a Cybersecurity review from the U.S. Department of Homeland Security and/or a cyber hygiene assessment from the County Controller's Office.

The District will implement this Recommendation if warranted and appropriate based on the results of the District's confidential internal report.

4. Given the results of their internal reports, governmental entities may choose to ask their IT departments to review their own Cybersecurity Plan with the detailed template provided by the FCC's Cybersecurity Planning Guide and consider customizing it using FCC's Create Custom Cybersecurity Planning Guide tool (see footnote 52).

The District will implement this Recommendation if warranted and appropriate based on the results of the District's confidential internal report.

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

Sincerely,

Gina Sudaria
Superintendent
Ravenswood City School District

1017 MIDDLEFIELD ROAD
Redwood City, California 94063
Telephone (650) 780-7220
www.redwoodcity.org

December 21, 2020

Honorable Danny Y. Chou
Judge of the Superior Court
c/o Jenarda Dubois
Hall of Justice
400 County Center, 8th Floor
Redwood City, CA 94063-1655

Subject: City of Redwood City's response to 2019-2020 Civil Grand Jury Report entitled "Cybersecurity – It Is Not Enough To Think you Are Protected"

Dear Judge Chou:

After reviewing the 2019-2020 Grand Jury report entitled "Cybersecurity – It Is Not Enough To Think you Are Protected", the following are the City of Redwood City's responses to the Grand Jury's findings. Redwood City Council approved this response letter at its public meeting on December 21, 2020.

FINDINGS AND CITY RESPONSES:

F1. Ransomware is a real and growing threat to public entities including those in San Mateo County.

City response: We agree with the Jury's findings.

F2. Across the country, local governments and schools represent 12% of all Ransomware attacks.

City response: We agree with the Jury's findings although City staff did not substantiate the statistics.

F3. The direct and indirect costs of Ransomware can be significant.

City response: We agree with the Jury's findings.

F4. Cybersecurity reviews and assessments, and an updated, well-executed Cybersecurity plan, are critical components of IT security strategy.

City response: We agree with the Jury's findings.

F5. A comprehensive Cybersecurity plan should include, at a minimum, information concerning prevention steps, spam and malware software, and backups and full recovery testing.

City response: We agree with the Jury's findings.

F6. The identification of phishing attempts, including the use of spam filters, is an important component to protecting an IT system from Ransomware attacks.

City response: We agree with the Jury's findings.

F7. Testing a full restore of a server to ensure that backups are reliable should be undertaken regularly as part an entity's backup plan to recover lost information.

City response: We agree with the Jury's findings.

F8. Training of new employees, and the recurring training of existing is an important component of defense against Ransomware.

City response: We agree with the Jury's findings.

RECOMMENDATIONS AND CITY RESPONSES

R1. 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:

City Response: The City requested a written response to this recommendation from its IT management team, in lieu of a separate report addressing these concerns, so that management could develop a response to the final three recommendations of the report.

R1.1 System Security (Firewalls, Anti-malware/ Antivirus software, use of subnets, strong password policies, updating/patching regularly).

City response: The recommendation has been implemented. Following is a summary of what has been implemented.

The City of Redwood City utilizes several strategies for protecting against nefarious acts including but not limited to:

- Industry recognized leaders' dedicated firewall appliances at all electronic entry points into the City. On each firewall all ports are blocked by default. Only known needed ports are opened; thus limiting the type of traffic coming into the City network infrastructure.
- All servers and desktops run an industry leader endpoint protection software which is automatically updated. It provides key protections including: endpoint detection and response (EDR) which detects and investigates suspicious activity with AI-driven analysis; anti-ransomware from sources including browsers, multi-media, MS Office applications, and email; behavioral analysis (acting on many files in a short period) issuing warnings, stopping errant processes, and notifying IT of such activity; malicious macros and other forms of code detections and protections; and exploit prevention techniques which detect and stop common and known

key vulnerabilities including zero-day attacks. The software communicates with the manufacturer's cloud site which continuously updates the local software with the latest protections.

- VLAN's, or virtual segmented networks, are used strategically throughout the organization to limit end-point access to servers and networks in which access is needed.
- Password policies meet generally accepted industry recommendations that are considered very strong and include required periodic changing which includes disallowing reuse of recent passwords.
- All servers are patched as appropriate, generally after a short while once a patch has been released and tested by others as bug free.
- Two Factor Authentication is being researched and expected to be implemented City-wide once the best solution for the City is determined.

R1.2 Backup & Recovery (In the event of an attack, 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?)

City response: The recommendation has been implemented. Following is a summary of what has been implemented.

More than 60 TB of user data is backed up in multiple ways. A shadow copy is created twice daily on the server to allow for easy rollback of deleted or changed files. In addition, files are backed up to an on-premise dedicated appliance. The appliance replicates itself to the manufacturers' cloud on a daily basis. In the event the on-premise device becomes infected with mal-ware, including ransomware, the device can be wiped clean and the data restored from the cloud's back up. If the backup device itself fails, within three business days a new appliance will be shipped, which is pre-loaded with our backed up data. Data can also be recovered directly from the manufacturer's cloud storage. Daily backups are preserved for a week, weekly backups are preserved for four weeks, monthly backups are saved for twelve months, and yearly revisions are kept for no less than two years. The process is continuously being tested in normal operations via requests from users asking IT to restore data from one of the previous day's backups.

All databases in the City's robust database infrastructure are included in all backup processes. As new databases are brought online, the requesting department is involved in determining the acceptable number of transactions they would be willing to re-enter from the previous full backup, usually nightly. If the number of daily transactions is great and the department desires, database backups are scheduled more often.

The City runs in a robust, industry best virtual environment. This not only allows the City to realized cost savings by having many virtual servers running on fewer physical servers, it allows the City to maintain hot-standby servers in the Police Department data center.

In addition to data backups, the City runs a sophisticated recovery tool which can shut one or more critical servers down and switch their function to hot stand-by servers located at our second data center, located in Police headquarters, from any recovery point within the last 24 hours. Communication between the two data centers is via dedicated fiber, keeping access limited to just the two firewalls at each end of the fiber.

The City's IT Manager recommends against the testing of a system wide recovery as it is not a practical approach to Redwood City's mix of different technology functions, services, and protections. The

technology architecture is designed with redundancy and failover capabilities such that no single event short of a natural disaster could bring down the entire infrastructure at one time. The different functions/components are generally tested during the normal course of business as functions fail, servers patched, or requested data restored. Nevertheless, the City has planned for such a circumstance, and recovery processes are documented in the City's secure internal systems.

All network devices have their configurations backed up nightly in the event of an equipment failure or breach.

R1.3. 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)

City response: The recommendation has been partially implemented. Following is a summary of what has been implemented and what is planned.

The City utilizes both cloud and an on premise dedicated SPAM prevention appliance and software which all email is first run though before being delivered to recipients. The appliance continuously communicates with the manufacturer's secure site to update its protections to the latest known threats. In addition, the appliance wraps all links within an email with a path which, when clicked, first go through the manufacturer's secure cloud services to confirm as best as possible that the link is legitimate and not a known hacking site.

The City prepends the subject of certain emails with [suspect] when an email contains one of many known to be trouble phrases such as "gift cards." Every external email prepends the body of the email with a warning the email is from an external source and to use caution when responding or clicking on any links contained within.

The City is currently in the process of implementing employee required cyber security and awareness training and will have it implemented by March 2021. It will include best practices for handling Personal Identifying Information (PID) among other topics requiring vigilance.

Additional City security strategies

The City carries cyber security insurance in the event of a data breach which provides the City with resources to assist in the cost of recovery, including notifications to those whose personal information was likely breached.

As cloud services become more a part of the City's infrastructure, City IT strives to connect cloud services to its internal Active Directory security model, often referred to as "Single Sign On." This allows IT staff to manage access to internal and hosted (cloud) applications from a single secure source.

Some high risk data, such as credit card information, is never stored, **in any format**, on City equipment or premise. Credit card processing is always done through third party providers who must be Payment Card Industry (PCI) compliant. PCI standards and requirements are well documented and only vendors meeting PCI compliance are considered and used by the City.

City IT staff is investigating the implementation of multi-factor authentication. This effort has been ramped up given the current pandemic environment in which the majority of the workforce is located outside of a City facility. Whereas in the past security was focused on keeping people out, the pandemic has turned that upside down in which now the strategy is to secure endpoints theoretically located

anywhere in the world. Multi-factor authentication is one of the predominant methods of securing access from outside our firewalls.

R2. 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.

City response: The recommendation is partially implemented through the creation of this response, which provides to the City's governing body a high level look at City cyber security policies and procedures without providing explicit details publicly. Staff will also offer confidential briefings to City Councilmembers prior to June 30, 2021 regarding the City's cybersecurity measures.

R3. Given the results of their internal reports, governmental entities may choose to request further guidance by means of a Cybersecurity review from the U.S. Department of Homeland Security and/or a cyber hygiene assessment from the County Controller's Office.

City response: This recommendation will be further analyzed by City staff as to whether one or both of the recommended assisting agencies, the Department of Homeland Security and/or the County Controllers Office, are the preferred fit for the City and what resources will be needed in order to consult with them. This analysis will inform the City Manager's fiscal year 2021-22 budget.

R4. Given the results of their internal reports, governmental entities may choose to ask their IT departments to review their own Cybersecurity Plan with the detailed template provided by the FCC's Cybersecurity Planning Guide and consider customizing it using FCC's Create Custom Cybersecurity Planning Guide tool (see footnote 52).

City response: City staff proposes to undertake an analysis of the level of effort required to convert its current cyber security documentation into a more formal, single source Cybersecurity Plan using the FCC's Cybersecurity Planning Guide as a template. If additional resources are required, staff may seek funding in the City Manager's proposed Fiscal Year 2021-22 budget.

Sincerely,

Diane Howard

Diane Howard
Mayor

REDWOOD CITY SCHOOL DISTRICT
750 Bradford Street • Redwood City • CA 94063 (650) 423-2200 FAX: (650) 423-2204

December 4, 2020

Via Email (grandjury@sanmateocourt.org)

The Honorable Danny Y. Chou
Judge of the Superior Court
c/o Jenarda Dubois
Hall of Justice
400 County Center; 2nd Floor
Redwood City, CA 94063-1655

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

Dear Judge Chou:

The Redwood City School District (the "District") has received and reviewed the 2019-2020 Grand Jury Report entitled "Ransomware: It Is Not Enough To Think You Are Protected." We appreciate the Grand Jury's interest in this matter. Having reviewed and considered the Grand Jury's Findings and Recommendations, the District responds below pursuant to section 933.05 of the California Penal Code.

Please be advised that the District presented the Grand Jury Report to its Board of Trustees, and the District's Board approved these responses, on December 9, 2020.

Findings:

1. *Ransomware is a real and growing threat to public entities including those in San Mateo County.*

The District agrees with this Finding.

2. *Across the country, local governments and schools represent 12% of all Ransomware attacks.*

The District lacks information to fully agree or disagree with this Finding given that it did not conduct the research related to this Report. The District, however, accepts the Grand Jury's Finding for the purposes of this Response.

3. *The direct and indirect costs of Ransomware can be significant.*

The District agrees with this Finding.

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

The District agrees with this Finding.

5. *A comprehensive Cybersecurity 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.

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.

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

The District lacks information to fully agree or disagree with this Finding given that it did not conduct the research related to this Report. The District, however, accepts the Grand Jury's Finding for the purposes of this Response.

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.

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:*

1. *System Security (Firewalls, Anti-malware/Antivirus software, use of subnets, strong password policies, updating/patching regularly)*
2. *Backup & Recovery (In the event of an attack, 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?)*
3. *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)*

The District implemented this Recommendation on June 1, 2020 by directing the District's IT Department to prepare a confidential report which addresses the three concerns specifically identified above.

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 has implemented this Recommendation.

3. *Given the results of their internal reports, governmental entities may choose to request further guidance by means of a Cybersecurity review from the U.S. Department of Homeland Security and/or a cyber hygiene assessment from the County Controller's Office.*

The District has implemented this Recommendation.

4. *Given the results of their internal reports, governmental entities may choose to ask their IT departments to review their own Cybersecurity Plan with the detailed template provided by the FCC's Cybersecurity Planning Guide and consider customizing it using FCC's Create Custom Cybersecurity Planning Guide tool (see footnote 52).*

The District implemented this Recommendation.

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

Sincerely,

John R. Baker, Ed.D.
Superintendent
Redwood City School District

San Bruno Park School District
Innovate • Motivate • Educate

500 Acacia Avenue, San Bruno, CA 94066-4222
Tele: 650.624.3100

January 13, 2021

Via Email (grandjury@sanmateocourt.org)

The Honorable Danny Y. Chou
Judge of the Superior Court
c/o Jenarda Dubois
Hall of Justice
400 County Center; 2nd Floor
Redwood City, CA 94063-1655

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

Dear Judge Chou:

The San Bruno Park Elementary School District (the "District") has received and reviewed the 2019-2020 Grand Jury Report entitled "Ransomware: It Is Not Enough To Think You Are Protected." We appreciate the Grand Jury's interest in this matter. Having reviewed and considered the Grand Jury's Findings and Recommendations, the District responds below pursuant to section 933.05 of the California Penal Code.

Please be advised that the District presented the Grand Jury Report to its Board of Trustees, and the District's Board approved these responses, on January 13, 2021.

Findings:

1. *Ransomware is a real and growing threat to public entities including those in San Mateo County.*

The District agrees with this Finding.

2. *Across the country, local governments and schools represent 12% of all Ransomware attacks.*

The District lacks information to fully agree or disagree with this Finding given that it did not conduct the research related to this Report. The District, however, accepts the Grand Jury's Finding for the purposes of this Response.

3. *The direct and indirect costs of Ransomware can be significant.*

The District agrees with this Finding.

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

The District agrees with this Finding.

5. *A comprehensive Cybersecurity 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.

500 Acacia Avenue, San Bruno, CA 94066-4222
Tele: 650.624.3100

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.

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

The District lacks information to fully agree or disagree with this Finding given that it did not conduct the research related to this Report. The District, however, accepts the Grand Jury's Finding for the purposes of this Response.

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.

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:*

    1. *System Security (Firewalls, Anti-malware/Antivirus software, use of subnets, strong password policies, updating/patching regularly)*

The recommendation has been implemented – We are using current, next generation firewall, antivirus, content filtering. Our network consists of multiple subnets and VLANs, with strong password protection and regular updates of our servers.

    2. *Backup & Recovery (In the event of an attack, 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?)*

The recommendation has been implemented – We have implemented a hybrid Cloud/On-Premises backup solution that backs up our voice, data and virtual servers to a physical storage point house in our data center. Those backups are also uploaded to a cloud storage point, for off-premises storage. Backups have been tested and a restore can be implemented from the backup data stored locally or off-premises.

    3. *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)*

The District implemented this Recommendation starting September 2019 thru October 2020 by directing the District's IT Department to make upgrades to our systems and prepare a confidential report which addresses the three concerns specifically identified above. - Using G Suite for Education, email filtering and warnings are enabled and functional. Also, users have been informed of email safety and have been asked to report any suspicious activity to the IT Department.

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.*

San Bruno Park School District
Innovate • Motivate • Educate

500 Acacia Avenue, San Bruno, CA 94066-4222
Tele: 650.624.3100

The District intends to implement this Recommendation, 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.

3. *Given the results of their internal reports, governmental entities may choose to request further guidance by means of a Cybersecurity review from the U.S. Department of Homeland Security and/or a cyber hygiene assessment from the County Controller's Office.*

The District will implement this Recommendation if warranted and appropriate based on the results of the District's confidential internal report.

4. *Given the results of their internal reports, governmental entities may choose to ask their IT departments to review their own Cybersecurity Plan with the detailed template provided by the FCC's Cybersecurity Planning Guide and consider customizing it using FCC's Create Custom Cybersecurity Planning Guide tool (see footnote 52).*

The District will implement this Recommendation if warranted and appropriate based on the results of the District's confidential internal report.

Please be advised that Both the Grand Jury Report and the District's responses were presented to and approved by the District's Governing Board on January 13, 2021.

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

Sincerely,

Jose Espinoza
Superintendent
San Bruno Park Elementary School District

SAN CARLOS SCHOOL DISTRICT

Michelle Harmeier, Ed. D., Superintendent
Hans Barber, Assistant Superintendent
Christine Gong, Chief Financial Officer

1200 Industrial Road, Unit 9
San Carlos, CA 94070
Voice: (650) 508-7333
Fax: (650) 508-7340
www.scsdk8.org

December 3, 2020

Approved on
DEC 03 2020
Board Agenda

Via Email (grandjury@sanmateocourt.org)

The Honorable Danny Y. Chou
Judge of the Superior Court
c/o Jenarda Dubois
Hall of Justice
400 County Center; 2nd Floor
Redwood City, CA 94063-1655

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

Dear Judge Chou:

The San Carlos School District (the "District") has received and reviewed the 2019-2020 Grand Jury Report entitled "Ransomware: It Is Not Enough To Think You Are Protected." We appreciate the Grand Jury's interest in this matter. Having reviewed and considered the Grand Jury's Findings and Recommendations, the District responds below pursuant to section 933.05 of the California Penal Code.

Please be advised that the District presented the Grand Jury Report to its Board of Trustees, and the District's Board approved these responses, on December 3, 2020.

Findings:

1. ***Ransomware is a real and growing threat to public entities including those in San Mateo County.***

The District agrees with this Finding.

2. ***Across the country, local governments and schools represent 12% of all Ransomware attacks.***

The District lacks information to fully agree or disagree with this Finding given that it did not conduct the research related to this Report. The District, however, accepts the Grand Jury's Finding for the purposes of this Response.

3. ***The direct and indirect costs of Ransomware can be significant.***

The District agrees with this Finding.

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

The District agrees with this Finding.

5. ***A comprehensive Cybersecurity 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.

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.

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

The District lacks information to fully agree or disagree with this Finding given that it did not conduct the research related to this Report. The District, however, accepts the Grand Jury's Finding for the purposes of this Response.

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.

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:***
    1. ***System Security (Firewalls, Anti-malware/Antivirus software, use of subnets, strong password policies, updating/patching regularly)***
    2. ***Backup & Recovery (In the event of an attack, 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?)***
    3. ***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)***

The District implemented this Recommendation on November 24, 2020, by directing the District's IT Department to prepare a confidential report which addresses the three concerns specifically identified above.

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 this Recommendation, 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.

3. ***Given the results of their internal reports, governmental entities may choose to request further guidance by means of a Cybersecurity review from the U.S. Department of Homeland Security and/or a cyber hygiene assessment from the County Controller's Office.***

The District will implement this Recommendation if warranted and appropriate based on the results of the District's confidential internal report.

4. ***Given the results of their internal reports, governmental entities may choose to ask their IT departments to review their own Cybersecurity Plan with the detailed template provided by the FCC's Cybersecurity Planning Guide and consider customizing it using FCC's Create Custom Cybersecurity Planning Guide tool (see footnote 52).***

The District will implement this Recommendation if warranted and appropriate based on the results of the District's confidential internal report.

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

Sincerely,

Hans Barber
Assistant Superintendent
San Carlos School District

SAN MATEO COUNTY COMMUNITY COLLEGE DISTRICT

3401 CSM Drive, San Mateo, CA 94402
P: (650) 574-6550 F: (650) 574-6574
www.smccd.edu

December 21, 2020 Via Email to grandjury@sanmateocourt.org

The Honorable Danny Y. Chou
Judge
San Mateo County Superior Court
c/o Jenarda Dubois
Hall of Justice
400 County Center, 2nd Floor
Redwood City, CA 94063-1655

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

Dear Judge Chou:

The San Mateo County Community College District ("the District") has received and reviewed the 2019-2020 Grand Jury Report entitled "Ransomware: It Is Not Enough To Think You Are Protected. " We appreciate the Grand Jury's interest in this matter. Having reviewed and considered the Grand Jury's Findings and Recommendations, the District responds below pursuant to section 933.05 of the California Penal Code.

Please be advised that the District presented the Grand Jury Report to its Board of Trustees, and the District's Board approved these responses on December 14, 2020.

In its report, the Grand Jury delivered eight findings and the District provides the following responses:

Finding 1. Ransomware is a real and growing threat to public entities including those in San Mateo County.

District Response: *The District agrees with this finding.*

Finding 2. Across the country, local governments and schools represent 12% of all Ransomware attacks.

District Response: *The District lacks information to fully agree or disagree with this finding given that it did not conduct the research related to this Report. The District, however, accepts the Grand Jury's finding for the purposes of this Response.*

Finding 3. The direct and indirect costs of Ransomware can be significant.

District Response: *The District agrees with this finding.*

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

District Response: *The District agrees with this finding.*

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

District Response: *The District agrees with this finding.*

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

District Response: *The District agrees with this finding.*

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

District Response: *The District lacks information to fully agree or disagree with this finding given that it did not conduct the research related to this Report. The District, however, accepts the Grand Jury's finding for the purposes of this Response.*

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

District Response: *The District agrees with this finding.*

Further, the Grand Jury has offered the following recommendations who which it has asked the District to respond:

Recommendation 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:

1. System Security (Firewalls, Anti-malware/Antivirus software, use of subnets, strong password policies, updating/patching regularly)

2. Backup & Recovery (In the event of an attack, 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?)

3. 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)

District Response: *The Chancellor has directed the District's Chief Technology Officer to prepare a confidential report which addresses the issues outlined above.*

Recommendation 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.

> ***District Response:*** *The District intends to prepare and provide a confidential report to the District's Board of Trustees by June 30, 2021.*

Recommendation 3. Given the results of their internal reports, governmental entities may choose to request further guidance by means of a Cybersecurity review from the U.S. Department of Homeland Security and/or a cyber hygiene assessment from the County Controller's Office.

> ***District Response:*** *The District will implement this Recommendation if warranted and appropriate based on the results of the District s confidential internal report.*

Recommendation 4. Given the results of their internal reports, governmental entities may choose to ask their IT departments to review their own Cybersecurity Plan with the detailed template provided by the FCC's Cybersecurity Planning Guide and consider customizing it using FCC's Create Custom Cybersecurity Planning Guide tool (see footnote 52).

> ***District Response:*** *The District will implement this Recommendation if warranted and appropriate based on the results of the District s confidential internal report.*

The District appreciates the work of the Grand Jury and the opportunity to respond to the findings and recommendations of its report. Should the Grand Jury have any questions regarding the District's responses, or need additional information, please let me know.

Sincerely,

Michael E. Claire
Chancellor

SAN MATEO COUNTY
MOSQUITO & VECTOR
CONTROL DISTRICT
Protecting public health since 1916

1351 Rollins Road
Burlingame, CA 94010

phone (650) 344-8592
fax (650) 344-3843

www.smcmvcd.org

February 8, 2021

Honorable Danny Y. Chou
Judge of the Superior Court
C/O Jenarda Dubois
Hall of Justice
400 County Center, 8th Floor
Redwood City, CA 94063-1655

Subject: October 7, 2020 Grand Jury Report: "Ransomware: It Is Not Enough To Think You Are Protected"

Dear Honorable Judge Chou:

The San Mateo County Mosquito and Vector Control District Board of Trustees reviewed the following responses at its November 12, 2020. The District Board subsequently approved the following responses to the San Mateo County Civil Grand Jury 2019-2020 Report entitled "Ransomware: It is Not Enough To Think You Are Protected."

Findings:

F1. Ransomware is a real and growing threat to public entities including those in San Mateo County.

The District agrees with this Finding.

F2. Across the country, local governments and schools represent 12% of all Ransomware attacks.

The District accepts the Grand Jury's Finding that appears to be based on 2020 first quarter data from the Coveware Report.

F3. The direct and indirect costs of Ransomware can be significant.

The District agrees with this Finding.

F4. Cybersecurity reviews and assessments, and an updated, well-executed Cybersecurity plan, are critical components of IT security strategy.

The District agrees with this Finding.

F5. A comprehensive Cybersecurity 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.

F6. 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.

F7. Testing a full restore of a server to ensure that backups are reliable should be undertaken regularly as part an entity's backup plan to recover lost information.

The District agrees with this Finding.

F8. 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.

Recommendations:

R1. 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:

1. *System Security (Firewalls, Anti-malware/Antivirus software, use of subnets, strong password policies, updating/patching regularly)*
2. *Backup & Recovery (In the event of an attack, 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?)*
3. *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)*

The District received this report from its IT staff on these three areas of concern to the Board of Trustees at its November 12, 2020 meeting.

R2. 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's IT staff have received this request and is working on completing the Recommended confidential internal report by June 30, 2021.

R3. Given the results of their internal reports, governmental entities may choose to request further guidance by means of a Cybersecurity review from the U.S. Department of Homeland Security and/or a cyber hygiene assessment from the County Controller's Office.

The District will consider requesting further guidance based on the internal reports.

R4. Given the results of their internal reports, governmental entities may choose to ask their IT departments to review their own Cybersecurity Plan with the detailed template provided by the FCC's Cybersecurity Planning Guide and consider customizing it using FCC's Create Custom Cybersecurity Planning Guide tool.

The District's IT staff will utilize the FCC Cybersecurity Planning Guide to review and update the District's cybersecurity plan.

We appreciate the research and awareness brought forth by the Grand Jury. We thank the members of the Grand Jury for their work and contributions toward this important issue.

Sincerely,

Brian Weber
District Manager

SAN MATEO COUNTY OFFICE OF EDUCATION
Excellence and Equity in Education
Nancy Magee • County Superintendent of Schools

December 2, 2020

Via Email (grandjury@sanmateocourt.org)

The Honorable Danny Y. Chou
Judge of the Superior Court
c/o Jenarda Dubois
Hall of Justice
400 County Center; 2nd Floor
Redwood City, CA 94063-1655

Re: Response to the 2019-2020 Grand Jury Report entitled "Ransomware: It Is Not Enough to Think You Are Protected."

Dear Judge Chou:

The San Mateo County Office of Education ("the SMCOE") has received and reviewed the 2019-2020 Grand Jury Report entitled "Ransomware: It Is Not Enough to Think You Are Protected." We appreciate the Grand Jury's interest in this matter. Having reviewed and considered the Grand Jury's Findings and Recommendations, the SMCOE responds below pursuant to section 933.05 of the California Penal Code.

Findings:

1. Ransomware is a real and growing threat to public entities including those in San Mateo County.

The SMCOE agrees with this Finding.

2. Across the country, local governments and schools represent 12% of all Ransomware attacks.

The SMCOE lacks information to fully agree or disagree with this Finding given that it did not conduct the research related to this Report. The SMCOE, however, accepts the Grand Jury's Finding for the purposes of this Response.

3. The direct and indirect costs of Ransomware can be significant.

The SMCOE agrees with this Finding.

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

The SMCOE agrees with this Finding.

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

The SMCOE agrees with this Finding.

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 SMCOE agrees with this Finding.

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 SMCOE lacks information to fully agree or disagree with this Finding given that it did not conduct the research related to this Report. The SMCOE, however, accepts the Grand Jury's Finding for the purposes of this Response.

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

The SMCOE agrees with this Finding.

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 attack, 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)

The SMCOE implemented this Recommendation on October 7, 2020, by directing the SMCOE IT Department to prepare a confidential report which addresses the three concerns specifically identified above.

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 SMCOE intends to implement this Recommendation, provided that the SMCOE 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.

3. *Given the results of their internal reports, governmental entities may choose to request further guidance by means of a Cybersecurity review from the U.S. Department of Homeland Security and/or a cyber hygiene assessment from the County Controller's Office.*

The SMCOE will implement this Recommendation if warranted and appropriate based on the results of our confidential internal report.

4. *Given the results of their internal reports, governmental entities may choose to ask their IT departments to review their own Cybersecurity Plan with the detailed template provided by the FCC's Cybersecurity Planning Guide and consider customizing it using FCC's Create Custom Cybersecurity Planning Guide tool (see footnote 52).*

The SMCOE will implement this Recommendation if warranted and appropriate based on the results of our confidential internal report.

Sincerely,

Nancy Magee

Nancy Magee
San Mateo County Superintendent of Schools

C: San Mateo County Board of Supervisors

SAN MATEO-FOSTER CITY
SCHOOL DISTRICT

LIVE • LEAD • LEARN

November 20, 2020

Via Email (grandjury@sanmateocourt.org)

The Honorable Danny Y. Chou
Judge of the Superior Court
c/o Jenarda Dubois
Hall of Justice
400 County Center; 2nd Floor
Redwood City, CA 94063-1655

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

Dear Judge Chou:

The San Mateo-Foster City School District (the "District") has received and reviewed the 2019-2020 Grand Jury Report entitled "Ransomware: It Is Not Enough To Think You Are Protected." We appreciate the Grand Jury's interest in this matter. Having reviewed and considered the Grand Jury's Findings and Recommendations, the District responds below pursuant to section 933.05 of the California Penal Code.

Please be advised that the District presented the Grand Jury Report to its Board of Trustees, and the District's Board approved these responses, on November 19, 2020.

Findings:

1. *Ransomware is a real and growing threat to public entities including those in San Mateo County.*

The District agrees with this Finding.

2. *Across the country, local governments and schools represent 12% of all Ransomware attacks.*

1170 Chess Drive
Foster City, California 94404
650.312.7700 Tel
650.312.7779 Fax
www.smfcsd.net

The District lacks information to fully agree or disagree with this Finding given that it did not conduct the research related to this Report. The District, however, accepts the Grand Jury's Finding for the purposes of this Response.

3. *The direct and indirect costs of Ransomware can be significant.*

The District agrees with this Finding.

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

The District agrees with this Finding.

5. *A comprehensive Cybersecurity 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.

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.

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 lacks information to fully agree or disagree with this Finding given that it did not conduct the research related to this Report. The District, however, accepts the Grand Jury's Finding for the purposes of this Response.

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.

Recommendations:

1170 Chess Drive
Foster City, California 94404
650.312.7700 Tel
650.312.7779 Fax
www.smfcsd.net

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:*
    1. *System Security (Firewalls, Anti-malware/Antivirus software, use of subnets, strong password policies, updating/patching regularly)*
    2. *Backup & Recovery (In the event of an attack, 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?)*
    3. *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)*

The District implemented this Recommendation on October 30, 2020 by directing the District's IT Department to prepare a confidential report which addresses the three concerns specifically identified above.

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 this Recommendation, 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.

3. *Given the results of their internal reports, governmental entities may choose to request further guidance by means of a Cybersecurity review from the U.S. Department of Homeland Security and/or a cyber hygiene assessment from the County Controller's Office.*

The District will implement this Recommendation if warranted and appropriate based on the results of the District's confidential internal report.

1170 Chess Drive
Foster City, California 94404
650.312.7700 Tel
650.312.7779 Fax
www.smfcsd.net

4. *Given the results of their internal reports, governmental entities may choose to ask their IT departments to review their own Cybersecurity Plan with the detailed template provided by the FCC's Cybersecurity Planning Guide and consider customizing it using FCC's Create Custom Cybersecurity Planning Guide tool (see footnote 52).*

The District will implement this Recommendation if warranted and appropriate based on the results of the District's confidential internal report.

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

Sincerely,

Joan Rosas Ed.D.
Superintendent
San Mateo-Foster City School District

1170 Chess Drive
Foster City, California 94404
650.312.7700 Tel
650.312.7779 Fax
www.smfcsd.net

December 21, 2020

Hon. Danny Y. Chou
Judge of the Superior Court
c/o Jenarda Dubois
Hall of Justice
400 County Center; 8th Floor
Redwood City, CA 94063-1655

Dear Hon. Chou:

The San Mateo County Harbor District (District) approved the following responses to the Grand Jury Report "Ransomware: It Is Not Enough To Think You Are Protected" at its Regularly Scheduled Board Meeting held on December 16, 2020.

Response to Findings:

F1. Ransomware is a real and growing threat to public entities including those in San Mateo County.
The District agrees with the finding.

F2. Across the country, local governments and schools represent 12% of all Ransomware attacks.
The District does not have enough information to agree or disagree with the percentage that local governments and schools represent.

F3. The direct and indirect costs of Ransomware can be significant.
The District agrees with the finding.

F4. Cybersecurity reviews and assessments, and an updated, well-executed Cybersecurity plan, are critical components of IT security strategy.
The District agrees with the finding.

F5. A comprehensive Cybersecurity plan should include, at a minimum, information concerning prevention steps, spam and malware software, and backups and full recovery testing.
The District agrees with the finding.

F6. 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 the finding.

F7. Testing a full restore of a server to ensure that backups are reliable should be undertaken regularly as part an entity's backup plan to recover lost information.
The District agrees with the finding.

504 Avenue Alhambra, Ste. 200, P.O. Box 1449, El Granada, CA 94018
(650) 583-4400 T F (650) 583-4614

F8. Training of new employees, and the recurring training of existing employees, is an important component of defense against Ransomware.
The District agrees with the finding.

Response to Recommendations:

R1. 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:

1. System Security (Firewalls, Anti-malware/Antivirus software, use of subnets, strong password policies, updating/patching regularly)
2. Backup & Recovery (In the event of an attack, 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 Sever from a backup?)
3. 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)

The recommendation has been implemented. The District made a request to its outsourced IT consultant on November 9, 2020.

R2. 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 recommendation has not yet been implemented, but will be implemented in the future, with a time no later than June 30, 2021.

R3. Given the results of their internal reports, governmental entities may choose to request further guidance by means of a Cybersecurity review from the U.S. Department of Homeland Security and/or a cyber hygiene assessment from the County Controller's Office.

The recommendation has not yet been implemented but may be implemented in the future if the results of the IT consultant's internal report warrants such review.

R4. Given the results of their internal reports, Governmental entities may choose to ask their IT departments to review their own Cybersecurity Plan with the detailed template provided by the FCC's Cybersecurity Planning Guide and consider customizing it using FCC's Create Custom Cybersecurity Planning Guide tool.

The recommendation has not yet been implemented but will be implemented in the future if the results of the IT consultant's internal report warrants such review.

Respectfully,

James Pruett
General Manager

SAN MATEO RESOURCE CONSERVATION DISTRICT

PHONE: 650.712.7765

80 STONE PINE ROAD, SUITE 100
HALF MOON BAY, CA 94019

SANMATEORCD.ORG

December 22, 2020

Hon. Danny Y. Chou
Judge of the Superior Court
c/o Jenarda Dubois
Hall of Justice
400 County Center, 8th Floor
Redwood City, CA 94063-1655

Re: Response to Grand Jury Report: "Ransomware: It Is Not Enough To Think You Are Protected"

Dear Honorable Danny Y. Chou,

At the November 19, 2020 RCD Regular Meeting of the Board of Directors, the Board approved Executive Director, Kellyx Nelson, to respond. Due to the small size of the San Mateo Resource Conservation District (RCD), many of the "Best Practices" as outlined in the report do not apply or have been implemented in a scaled down fashion more appropriate to the RCD situation. Please find the RCD's responses to the Grand Jury Report below.

1. Office network is protected with a business class firewall with no external resources exposed to the internet. All computers and servers are setup to install updates automatically as they are released by Microsoft. Ancillary software such as Adobe Acrobat also updates automatically. On site computer patching is monitored at the server level. Network and email accounts share the same credentials, and all accounts require strong passwords. 2-Factor authentication for email is being implemented and should be complete by early 2021.

2. All RCD data is stored on the server. The server is backed up daily with an offsite backup solution. A second local backup is configured to allow rapid recovery of the server to new hardware should a catastrophic failure occur. A small amount of ancillary data is kept on the shared Geographic Information System mapping (GIS) workstation related to GIS projects. The GIS machine is backed up with an offsite backup solution. Workstations are not backed up and are considered expendable. RCD has a policy for users to never store important data on their laptops. All data is kept on the server network shares.

   Subnetting does not apply to RCD. Backups are monitored but full server recovery is not tested due to limited hardware resources.

3. Basic Email Spam and Malware filtering is provided via Office 365 tools. More sophisticated filtering is available and is currently under consideration. The cost of the expanded filtering functionality is a limiting factor. Currently we have no planned structured employee training on avoiding security issues. Frequent casual guidance given on an individual basis.

Sincerely,

Kellyx Nelson, Executive Director
San Mateo Resource Conservation District

San Mateo Union High School District

Kevin Skelly, Ph.D., Superintendent
Elizabeth McManus, Deputy Superintendent Business Services
Kirk Black, Ed.D., Deputy Superintendent Human Resources and Student Services
Julia Kempkey, Ed.D. Assistant Superintendent of Curriculum and Instruction

December 17, 2020

APPROVED BY
BOARD OF TRUSTEES
Ana
INITIALS

Via Email (grandjury@sanmateocourt.org)

The Honorable Danny Y. Chou
Judge of the Superior Court
c/o Jenarda Dubois
Hall of Justice
400 County Center; 2nd Floor
Redwood City, CA 94063-1655

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

Dear Judge Chou:

The San Mateo Union High School District has received and reviewed the 2019-2020 Grand Jury Report entitled "Ransomware: It Is Not Enough To Think You Are Protected." We appreciate the Grand Jury's interest in this matter. Having reviewed and considered the Grand Jury's Findings and Recommendations, the District responds below pursuant to section 933.05 of the California Penal Code.

Please be advised that the District presented the Grand Jury Report to its Board of Trustees, and the District's Board of Trustees approved these responses, on December 17, 2020

Findings:

1. *Ransomware is a real and growing threat to public entities including those in San Mateo County.*

The District agrees with this Finding.

2. *Across the country, local governments and schools represent 12% of all Ransomware attacks.*

The District lacks information to fully agree or disagree with this Finding given that it did not conduct the research related to this Report. The District, however, accepts the Grand Jury's Finding for the purposes of this Response.

3. *The direct and indirect costs of Ransomware can be significant.*

The District agrees with this Finding.

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

The District agrees with this Finding.

5. *A comprehensive Cybersecurity 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.

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.

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

The District lacks information to fully agree or disagree with this Finding given that it did not conduct the research related to this Report. The District, however, accepts the Grand Jury's Finding for the purposes of this Response.

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.

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 attack, 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 stronger password policy.

SMUHSD backups use CBT (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 up 30TB of district data which includes the SIS, and various other file servers.

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.

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.

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.

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.

3. *Given the results of their internal reports, governmental entities may choose to request further guidance by means of a Cybersecurity review from the U.S. Department of Homeland Security and/or a cyber hygiene assessment from the County Controller's Office.*

The District will implement this Recommendation if warranted and appropriate based on the results of the District's confidential internal report.

4. *Given the results of their internal reports, governmental entities may choose to ask their IT departments to review their own Cybersecurity Plan with the detailed template provided by the FCC's Cybersecurity Planning Guide and consider customizing it using FCC's Create Custom Cybersecurity Planning Guide tool (see footnote 52).*

The District will implement this Recommendation if warranted and appropriate based on the results of the District's confidential internal report.

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

Sincerely,

Kevin Skelly Digitally signed by Kevin Skelly Date: 2020.12.11 14:56:23 -08'00'

Kevin Skelly, Ph.D.
Superintendent

San Mateo Union High School District

Sequoia
Healthcare
District
525 Veterans Blvd.
Redwood City, CA 94063

650-421-2155 Phone
650-421-2159 Fax

www.seqhd.org

December 2, 2020

Mr. Neal Taniguchi
Court Executive Officer
San Mateo Superior Court
400 County Center
Redwood City, CA 94063

Re: Grand Jury Report: "Ransomware: It Is Not Enough To Think You Are Protected."
Response of Sequoia Healthcare District

Dear Mr. Taniguchi:

The Board of Directors and staff of the Sequoia Healthcare District (the "District") have been provided with a copy of the above-referenced report from the San Mateo County Civil Grand Jury. We appreciated the thorough research and recommendations in the report.

In general, the Board agrees with the findings and recommendations in the report. The specific responses are set forth below.

The District employs an outside consultant to advise on cybersecurity and ransomware protections. As requested by the report, we reviewed the status of the District's security and backup storage with the consultant. Although the District has robust security measures in place, the consultant has recommended additional "state of the art" protections to guard against ransomware attacks. The Board has authorized these measures and they will be implemented by December 31, 2020.

Against this background, the District responds to the findings and recommendations as follows:

FINDINGS

Finding F1. The District agrees with this finding.

Finding F2. The District agrees that local governments and school districts are frequent targets of ransomware attacks but does not have sufficient information to verify the percentage stated in the report.

Finding F3. The District agrees with this finding.

Finding F4. The District agrees with this finding.

Finding F5. The District agrees with this finding.

Finding F6. The District agrees with this finding.

Finding F7. The District agrees with this finding.

Finding F8. The District agrees with this finding.

RECOMMENDATIONS

Recommendation R1. The District agrees with this recommendation and has complied with it as of November 30, 2020.

Recommendation R2. The District agrees with this recommendation. The internal report has been provided to the Board and the Board has authorized expenditure for additional cybersecurity measures. The District expects to implement these measures by December 31, 2020.

Recommendation R3. In view of the responses to the first two recommendations, the District believes that this step is unnecessary.

Recommendation R4. In view of the responses to the first two recommendations, the District believes that this step is unnecessary.

This response was presented to the Board at its regular meeting on December 2, 2020 and approved unanimously.

Please let us know if there are any questions regarding the foregoing response.

Kim Griffin, RN
President of the Board of Directors

Pamela Kurtzman
Chief Executive Officer

SEQUOIA UNION HIGH SCHOOL DISTRICT

480 James Avenue, Redwood City, California 94062-1098
Administrative Offices (650) 369-1411

December 7, 2020

Via Email (grandjury@sanmateocourt.org)

The Honorable Danny Y. Chou
Judge of the Superior Court
c/o Jenarda Dubois
Hall of Justice
400 County Center; 2nd Floor
Redwood City, CA 94063-1655

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

Dear Judge Chou:

The Sequoia Union High School District (the "District") has received and reviewed the 2019-2020 Grand Jury Report entitled "Ransomware: It Is Not Enough To Think You Are Protected." We appreciate the Grand Jury's interest in this matter. Having reviewed and considered the Grand Jury's Findings and Recommendations, the District responds below pursuant to section 933.05 of the California Penal Code.

Please be advised that the District presented the Grand Jury Report to its Board of Trustees, and the District's Board approved these responses, on December 16, 2020.

Findings:

1. *Ransomware is a real and growing threat to public entities including those in San Mateo County.*

The District agrees with this Finding.

2. *Across the country, local governments and schools represent 12% of all Ransomware attacks.*

The District lacks information to fully agree or disagree with this Finding given that it did not conduct the research related to this Report. The District, however, accepts the Grand Jury's Finding for the purposes of this Response.

3. *The direct and indirect costs of Ransomware can be significant.*

The District agrees with this Finding.

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

The District agrees with this Finding.

5. *A comprehensive Cybersecurity 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.

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.

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

The District lacks information to fully agree or disagree with this Finding given that it did not conduct the research related to this Report. The District, however, accepts the Grand Jury's Finding for the purposes of this Response.

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.

Recommendations:

[NOTE: In responding to each Recommendation, the District must indicate that either: (1) the Recommendation has been implemented, with a summary regarding the implemented action, (2) the Recommendation has not yet been implemented, but will be implemented in the future, with a timeframe for implementation; (3) that the Recommendation requires further analysis, with an explanation and the scope and parameters of an analysis or study, and a time frame (not

to exceed six months) for the matter to be prepared for discussion by the governing body of the public agency when applicable; or (4) the Recommendation will not be implemented because it is not warranted or reasonable, with an explanation therefore.]

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:*
    1. *System Security (Firewalls, Anti-malware/Antivirus software, use of subnets, strong password policies, updating/patching regularly)*
    2. *Backup & Recovery (In the event of an attack, 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?)*
    3. *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)*

The District implemented this Recommendation on December 16, 2020 by directing the District's IT Department to prepare a confidential report which addresses the three concerns specifically identified above.

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 this Recommendation, 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.

3. *Given the results of their internal reports, governmental entities may choose to request further guidance by means of a Cybersecurity review from the U.S. Department of Homeland Security and/or a cyber hygiene assessment from the County Controller's Office.*

The District will implement this Recommendation if warranted and appropriate based on the results of the District's confidential internal report.

4. *Given the results of their internal reports, governmental entities may choose to ask their IT departments to review their own Cybersecurity Plan with the detailed template provided by the FCC's Cybersecurity Planning Guide and consider customizing it using FCC's Create Custom Cybersecurity Planning Guide tool (see footnote 52).*

The District will implement this Recommendation if warranted and appropriate based on the results of the District's confidential internal report.

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

Sincerely,

Crystal Leach
Interim Superintendent
Sequoia Union High School District

December 11, 2020

Via Email (grandjury@sanmateocourt.org)
The Honorable Danny Y. Chou
Judge of the Superior Court
c/o Jenarda Dubois
Hall of Justice
400 County Center; 8th Floor
Redwood City, CA 94063-1655

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

Dear Judge Chou:

The South San Francisco Unified School District ("SSFUSD") has received and reviewed the 2019-2020 Grand Jury Report entitled "Ransomware: It Is Not Enough To Think You Are Protected." We appreciate the Grand Jury's interest in this matter. Having reviewed and considered the Grand Jury's Findings and Recommendations, the District responds below pursuant to section 933.05 of the California Penal Code.

Please be advised that the District presented the Grand Jury Report to its Board of Trustees, and the District's Board approved these responses, on December 10, 2020.

FINDINGS

1. *Ransomware is a real and growing threat to public entities including those in San Mateo County.*

   The District agrees with this Finding.

2. *Across the country, local governments and schools represent 12% of all Ransomware attacks.*

The District lacks information to fully agree or disagree with this Finding given that it did not conduct the research related to this Report. The District, however, accepts the Grand Jury's Finding for the purposes of this Response.

3. *The direct and indirect costs of Ransomware can be significant.*

   The District agrees with this Finding.

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

   The District agrees with this Finding.

5. *A comprehensive Cybersecurity 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.

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.

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

   The District lacks information to fully agree or disagree with this Finding given that it did not conduct the research related to this Report. The District, however, accepts the Grand Jury's Finding for the purposes of this Response.

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.

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:

1. *System Security (Firewalls, Anti-malware/Antivirus software, use of subnets, strong password policies, updating/patching regularly)*
2. *Backup & Recovery (In the event of an attack, 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?)*
3. *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)*

The District implemented this Recommendation on October 19, 2020 by directing the District's IT Department to prepare a confidential report which addresses the three concerns specifically identified above.

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 this Recommendation, 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.

3. *Given the results of their internal reports, governmental entities may choose to request further guidance by means of a Cybersecurity review from the U.S. Department of Homeland Security and/or a cyber hygiene assessment from the County Controller's Office.*

   The District will implement this Recommendation if warranted and appropriate based on the results of the District's confidential internal report.

4. *Given the results of their internal reports, governmental entities may choose to ask their IT departments to review their own Cybersecurity Plan with the detailed template provided by the FCC's Cybersecurity Planning Guide and consider customizing it using FCC's Create Custom Cybersecurity Planning Guide tool (see footnote 52).*

   The District will implement this Recommendation if warranted and appropriate based on the results of the District's confidential internal report.

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

Sincerely,

Shawnterra Moore, Ed.D.
Superintendent
South San Francisco Unified School District

TOWN OF ATHERTON

ADMINISTRATIVE OFFICES
150 WATKINS AVENUE
ATHERTON, CALIFORNIA 94027
(650) 752-0500

December 18, 2020

Hon. Danny Y. Chou
Judge of Superior Court
C/o Jenarda Dubois
Hall of Justice
400 County Center; 8th Floor
Redwood City, CA 94063-1655

VIA EMAIL: grandjury@sanmateocourt.org

SUBJECT: RESPONSE TO GRAND JURY REPORT: "Ransomware: It Is Not Enough To Think You Are Protected"

Honorable Judge Chou,

Attached please find the Town of Atherton's response to the above Grand Jury Report. The response to both the findings and recommendations are listed below. Pursuant to California Penal Code Section 933.05, the response was considered by the City Council at a public meeting on December 16, 2020.

Should you have any questions concerning the response, please contact City Manager George Rodericks at (650) 752-0504 or grodericks@ci.atherton.ca.us.

Respectfully,

TOWN OF ATHERTON

Elizabeth Lewis
Mayor

Response to Grand Jury Report Findings and Recommendations

Report Title: “Ransomware: It Is Not Enough To Think You Are Protected"

Report Date: October 7, 2020

Response by: Town of Atherton

From: Elizabeth Lewis, Mayor

The Town of Atherton is responding to each Finding solely with respect to itself and not regarding any other City.

Response to Grand Jury Findings:

F1. Ransomware is a real and growing threat to public entities including those in San Mateo County.
Response: The Town of Atherton agrees with this finding

F2. Across the country, local governments and schools represent 12% of all Ransomware attacks.
Response: The Town of Atherton agrees with this finding

F3. The direct and indirect costs of Ransomware can be significant.
Response: The Town of Atherton agrees with this finding.

F4. Cybersecurity reviews and assessments, and an updated, well-executed Cybersecurity plan, are critical components of IT security strategy.
Response: The Town of Atherton agrees with this finding.

F5. A comprehensive Cybersecurity plan should include, at a minimum, information concerning prevention steps, spam and malware software, and backups and full recovery testing.
Response: The Town of Atherton agrees with this finding.

F6. The identification of phishing attempts, including the use of spam filters, is an important component to protecting an IT system from Ransomware attacks.
Response: The Town of Atherton agrees with this finding.

F7. Testing a full restore of a server to ensure that backups are reliable should be undertaken regularly as part an entity’s backup plan to recover lost information.
Response: The Town of Atherton agrees with this finding.

F8. Training of new employees, and the recurring training of existing employees, is an important component of defense against Ransomware.
Response: The Town of Atherton agrees with this finding.

Response to Grand Jury Recommendations:

The Grand Jury recommends that each governing body undertake its own confidential effort to protect against Ransomware attacks. Specifically:

R1. 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:

1. System Security (Firewalls, Anti-malware/Antivirus software, use of subnets, strong password policies, updating/patching regularly)
2. Backup & Recovery (In the event of an attack, 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?)
3. 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)

Response: This recommendation has been implemented

The Town of Atherton City Manager's Office made this request of the Town's IT Department upon receipt of the Grand Jury Report. The IT Department will prepare a study session report for City Council which will, at a minimum, address the concerns listed in R1.1, R1.2, and R1.3.

R2. 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.

Response: This recommendation will be implemented by the June deadline

The Town of Atherton's IT Department will prepare a comprehensive study session report for City Council, planned for Q1 calendar year 2021, that addresses the concerns identified in the report. This report will include actions taken and plans for future enhancements.

R3. Given the results of their internal reports, governmental entities may choose to request further guidance by means of a Cybersecurity review from the U.S. Department of Homeland Security and/or a cyber hygiene assessment from the County Controller's Office.

Response: This recommendation will be implemented on or before June 30, 2021

The Town of Atherton IT Department will make a request with the Department of Homeland Security, Cybersecurity & Infrastructure Security Agency, for cyber-hygiene services before June 30, 2021.

R4. Given the results of their internal reports, governmental entities may choose to ask their IT departments to review their own Cybersecurity Plan with the detailed template provided by the FCC's Cybersecurity Planning Guide and consider customizing it using FCC's Create Custom Cybersecurity Planning Guide tool (see footnote 52).

Response: This recommendation will be implemented on or before June 30, 2021

The Town of Atherton IT Department will utilize the Federal Communications Commission Cyber Security Planning Guide and the FCC Cyber Security Planner to review and update our cyber-security plans. This work will be completed on or before June 30, 2021.

TOWN OF COLMA
1198 El Camino Real • Colma, California • 94014-3212
Tel 650.997.8300 • Fax 650.997.8308

December 9, 2020

Honorable Danny Y. Chou
Judge of the Superior Court
Hall of Justice
400 County Center, 2nd Floor
Redwood City, CA 94063-1655

Re: Grand Jury Report: "Ransomware: It Is Not Enough To Think You Are Protected."

Dear Judge Chou:

The City Council received the San Mateo Civil Grand Jury report titled, "Ransomware: It Is Not Enough To Think You Are Protected."

The Town was requested to submit comments regarding the findings and recommendations within 90 days and no later than January 5, 2020. The Town of Colma's response to both the findings and recommendations are listed below.

The Grand Jury instructed each agency in San Mateo County to respond to findings F1 - F8 and recommendations R1 - R4.

For the "findings", the Town was to indicate one of the following;

1. The respondent agrees with the finding.
2. The respondent disagrees wholly or partially with the finding, in which case the response shall specify the portion of the finding that is disputed and shall include an explanation of the reasons therefore.

Additionally, for each Grand Jury "recommendation", the Town was requested to report one of the following actions;

1. The recommendation has been implemented, with a summary regarding the implemented action.
2. The recommendation has not yet been implemented, but will be implemented in the future, with a time frame for implementation.
3. The recommendation requires further analysis, with an explanation and the scope and parameters of an analysis or study, and a time frame for the matter to be prepared for

discussion by the officer or director of the agency or department being investigated or reviewed, including the governing body of the public agency when applicable. This time frame shall not exceed six months from the date of publication of the Grand Jury report.

4. The recommendation will not be implemented because it is not warranted or reasonable, with an explanation therefore.

The following are responses to findings F1-8;

F1. Ransomware is a real and growing threat to public entities including those in San Mateo County.

Town Response: The Town of Colma agrees with this finding.

F2. Across the country, local governments and schools represent 12% of all Ransomware attacks. 2019-2020 San Mateo County Civil Grand Jury 13

Town Response: The Town of Colma agrees with this finding.

F3. The direct and indirect costs of Ransomware can be significant.

Town Response: The Town of Colma agrees with this finding.

F4. Cybersecurity reviews and assessments, and an updated, well-executed Cybersecurity plan, are critical components of IT security strategy.

Town Response: The Town of Colma agrees with this finding.

F5. A comprehensive Cybersecurity plan should include, at a minimum, information concerning prevention steps, spam and malware software, and backups and full recovery testing.

Town Response: The Town of Colma agrees with this finding.

F6. The identification of phishing attempts, including the use of spam filters, is an important component to protecting an IT system from Ransomware attacks.

Town Response: The Town of Colma agrees with this finding.

F7. Testing a full restore of a server to ensure that backups are reliable should be undertaken regularly as part an entity's backup plan to recover lost information.

Town Response: The Town of Colma agrees with this finding.

F8. Training of new employees, and the recurring training of existing employees, is an important component of defense against Ransomware.

Town Response: The Town of Colma agrees with this finding.

The following are responses to recommendations R1-4;

R1. 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:

1. System Security (Firewalls, Anti-malware/Antivirus software, use of subnets, strong password policies, updating/patching regularly)

2. Backup & Recovery (In the event of an attack, 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?)

3. 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)

Town Response: This recommendation has been implemented. The Town requested this report from the Town's IT Support contractor, Stepford, on October 30, 2020.

R2. 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.

Town Response: This recommendation has been implemented. The Town received this report from the Town's IT Support contractor, Stepford, on November 14, 2020. The report describes what actions have already been taken and which will be given timely consideration for future enhancements to the existing cybersecurity plan. It will be presented to the City Council by June 30, 2021.

R3. Given the results of their internal reports, governmental entities may choose to request further guidance by means of a Cybersecurity review from the U.S. Department of Homeland Security and/or a cyber hygiene assessment from the County Controller's Office.

Town Response: This recommendation requires further analysis. The Town will conduct a thorough review of the provided report and will make this request if it is deemed appropriate, no later than April 7, 2021

R4. Given the results of their internal reports, governmental entities may choose to ask their IT departments to review their own Cybersecurity Plan with the detailed template provided by the FCC's Cybersecurity Planning Guide and consider customizing it using FCC's Create Custom Cybersecurity Planning Guide tool.

Town Response: This recommendation requires further analysis. The Town will conduct a thorough review of the provided report and will make this request if it is deemed appropriate, no later than April 7, 2021

This response was approved by the City Council at the December 9, 2020 public meeting.

On behalf of the Town of Colma, I would like to thank the Grand Jury for their work on this report.

Sincerely,

Diana Colvin

Diana Colvin
Mayor

TOWN OF HILLSBOROUGH
California

December 14, 2020

Hon. Danny Y. Chou
Judge of the Superior Court
c/o Jenarda Dubois
Hall of Justice
400 County Center, 8th Floor
Redwood City, CA 94063-1655

Re: Civil Grand Jury Report: "Ransomware: It Is Not Enough To Think You Are Protected"

Honorable Judge Chou:

Thank you for the opportunity to review and comment on the above referenced Grand Jury Report filed on October 7, 2020. The Town of Hillsborough's response to both the findings and recommendations are listed below.

Response to Grand Jury Findings:

F1. Ransomware is a real and growing threat to public entities including those in San Mateo County.

Response: The Town of Hillsborough agrees with this finding.

F2. Across the country, local governments and schools represent 12% of all Ransomware attacks.

Response: The Town of Hillsborough agrees with this finding.

F3. The direct and indirect costs of Ransomware can be significant.

Response: The Town of Hillsborough agrees with this finding.

F4. Cybersecurity reviews and assessments, and an updated, well-executed Cybersecurity plan, are critical components of IT security strategy.

Response: The Town of Hillsborough agrees with this finding.

F5. A comprehensive Cybersecurity plan should include, at a minimum, information concerning prevention steps, spam and malware software, and backups and full recovery testing.

Response: The Town of Hillsborough agrees with this finding.

F6. The identification of phishing attempts, including the use of spam filters, is an important component to protecting an IT system from Ransomware attacks.

Response: The Town of Hillsborough agrees with this finding.

F7. Testing a full restore of a server to ensure that backups are reliable should be undertaken regularly as part an entity's backup plan to recover lost information.

Response: The Town of Hillsborough agrees with this finding.

F8. Training of new employees, and the recurring training of existing employees, is an important component of defense against Ransomware.

Response: The Town of Hillsborough agrees with this finding.

Response to Grand Jury Recommendations:

The Grand Jury recommends that each governing body undertake its own confidential effort to protect against Ransomware attacks. Specifically:

R1. 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:

1. System Security (Firewalls, Anti-malware/Antivirus software, use of subnets, strong password policies, updating/patching regularly)
2. Backup & Recovery (In the event of an attack, 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?)
3. 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)

Response: This recommendation has been implemented. The Town of Hillsborough's City Manager's Office made this request of the Town's IT provider upon receipt of the Grand Jury Report. The Town will award a new contract for Managed IT services in February 2021 and the contract for services requires the new provider to address the concerns listed in R1.1, R1.2, and R1.3.

R2. 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.

Response: This recommendation will be implemented by the June deadline. The Town of Hillsborough's Managed IT Service provider will prepare a report for the City Council that addresses the concerns identified in the report. This report will include actions taken and plans for future enhancements.

R3. Given the results of their internal reports, governmental entities may choose to request further guidance by means of a Cybersecurity review from the U.S. Department of Homeland Security and/or a cyber hygiene assessment from the County Controller's Office.

Response: This recommendation will be implemented on or before June 30, 2021. The Town of Hillsborough may choose to make a request with the Department of Homeland Security, Cybersecurity & Infrastructure Security Agency, for cyber-hygiene services before June 30, 2021.

R4. Given the results of their internal reports, governmental entities may choose to ask their IT departments to review their own Cybersecurity Plan with the detailed template provided by the FCC's Cybersecurity Planning Guide and consider customizing it using FCC's Create Custom Cybersecurity Planning Guide tool (see footnote 52).

Response: This recommendation will be implemented on or before June 30, 2021. The Town of Hillsborough's Managed IT Service provider will utilize the Federal Communications Commission Cybersecurity Planning Guide and the FCC Cybersecurity Planner to review and update our cybersecurity plans. This work will be completed on or before June 30, 2021.

This response to the Grand Jury was approved at a public meeting on December 14, 2020.

Respectfully,

Alvin L. Royse
Mayor, Town of Hillsborough

Town of Portola Valley

Town Hall: 765 Portola Road, Portola Valley, CA 94028 Tel: (650) 851-1700 Fax: (650) 851-4677

December 9, 2020

Hon. Danny Chou
Judge of the Superior Court
c/o ChJenarda Dubois
Hall of Justice
400 County Center, 8th Floor
Redwood City, CA 94063

Dear Judge Chou,

Thank you for the opportunity to respond to the Grand Jury report entitled “Ransomware: It’s Not Enough To Think You Are Protected”.

Below are the Town’s responses to the report’s findings and recommendations.

Findings

F1. Ransomware is a real and growing threat to public entities including those in San Mateo County.

Response: The Town agrees with this finding.

F2. Across the country, local governments and schools represent 12% of all Ransomware attacks.

Response: The Town cannot independently confirm this finding, but does not disagree.

F3. The direct and indirect costs of Ransomware can be significant.

Response: The Town agrees with this finding.

F4. Cybersecurity reviews and assessments, and an updated, well-executed Cybersecurity plan, are critical components of IT security strategy.

Response: The Town agrees with this finding.

F5. A comprehensive Cybersecurity plan should include, at a minimum, information concerning prevention steps, spam and malware software, and backups and full recovery testing.

Response: The Town agrees with this finding.

F6. The identification of phishing attempts, including the use of spam filters, is an important component to protecting an IT system from Ransomware attacks.

Response: The Town agrees with this finding.

F7. Testing a full restore of a server to ensure that backups are reliable should be undertaken regularly as part an entity's backup plan to recover lost information.

Response: The Town agrees with this finding.

F8. Training of new employees, and the recurring training of existing employees, is an important component of defense against Ransomware.

Response: The Town agrees with this finding.

Recommendations

R1. 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: 1. System Security (Firewalls, Anti-malware/Antivirus software, use of subnets, strong password policies, updating/patching regularly) 2. Backup & Recovery (In the event of an attack, 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?) 3. 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)

Response: Recommendations 1 and 3 have been implemented fully over the last two years. Recommendation 2 has been implemented by way of a 2015 server crash that utilized backup systems that have subsequently been improved.

R2. 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.

Response: The recommendation has not been implemented at the Town Council level at this time, but the Council has been informed of multiple improvements to the Town's IT infrastructure. A full report will be provided to the Council by June 30, 2021.

R3. Given the results of their internal reports, governmental entities may choose to request further guidance by means of a Cybersecurity review from the U.S. Department of Homeland Security56 and/or a cyber hygiene assessment from the County Controller's Office.

Response: The recommendation has not been implemented, but the Town will request a cyber hygiene assessment from the County Controller's Office by the end of the fiscal year

R4. Given the results of their internal reports, governmental entities may choose to ask their IT departments to review their own Cybersecurity Plan with the detailed template provided by the

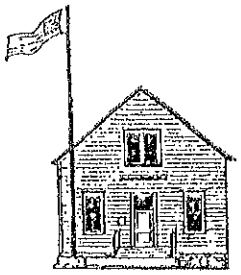
FCC's Cybersecurity Planning Guide and consider customizing it using FCC's Create Custom Cybersecurity Planning Guide tool (see footnote 52).

Response: The recommendation has not been implemented, but will be by June 30, 2021 which will be based on our annual auditor's enhanced cybersecurity audit.

Thank you,

Mayor, Town of Portola Valley

cc: Members of the Town Council



The Town of
Woodside

December 16, 2020

Hon. Danny Y. Chou
Judge of the Superior Court
c/o Jenarda Dubois
Hall of Justice
400 County Center; 8th Floor
Redwood City, CA 94063-1655

Dear Judge Chou:

The Woodside Town Council has had an opportunity to review the 2020 Grand Jury report entitled *"Ransomware: It is Not Enough to Think You Are Protected."* The Council after reviewing the report and allowing for public comment at its Town Council meeting on December 15, 2020 offers the following responses:

P.O. Box 620005
2955 Woodside Road
Woodside CA 94062

Responses to Findings

Finding F1. Ransomware is a real and growing threat to public entities including those in San Mateo County.

Response: The respondent agrees with the finding.

Finding F2. Across the country, local governments and schools represent 12% of all Ransomware attacks.

Response: The respondent agrees with the finding.

Finding F3. The direct and indirect costs of Ransomware can be significant.

Response: The respondent agrees with the finding.

Finding F4. Cybersecurity reviews and assessments, and an updated, well-executed Cybersecurity plan, are critical components of IT security strategy.

Response: The respondent agrees with the finding.

650-851-6790
Fax: 650-851-2195
townhall@woodsidetown.org

Finding F5. A comprehensive Cybersecurity plan should include, at a minimum, information concerning prevention steps, spam and malware software, and backups and full recovery testing.

Response: The respondent agrees with the finding.

Finding F6. The identification of phishing attempts, including the use of spam filters, is an important component to protecting an IT system from Ransomware attacks.

Response: The respondent agrees with the finding.

Finding F7. Testing a full restore of a server to ensure that backups are reliable should be undertaken regularly as part an entity's backup plan to recover lost information.

Response: The respondent agrees with the finding.

Finding F8. Training of new employees, and the recurring training of existing employees, is an important component of defense against Ransomware.

Response: The respondent agrees with the finding.

Response to Recommendations

R1. 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:

1. System Security (Firewalls, Anti-malware/Antivirus software, use of subnets, strong password policies, updating/patching regularly)

2. Backup & Recovery (In the event of an attack, 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?)

3. 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)

Response: The recommendation has been implemented.

R2. 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.

Response: The recommendation will be implemented within the requested timeframe.

R3. Given the results of their internal reports, governmental entities may choose to request further guidance by means of a Cybersecurity review from the U.S. Department of Homeland Security and/or a cyber hygiene assessment from the County Controller's Office.

Response: The recommendation will be implemented within the requested timeframe.

R4. Given the results of their internal reports, governmental entities may choose to ask their IT departments to review their own Cybersecurity Plan with the detailed template provided by the FCC's Cybersecurity Planning Guide and consider customizing it using FCC's Create Custom Cybersecurity Planning Guide tool (see footnote 52).

Response: The recommendation will be implemented.

Respectfully submitted,

Brian Dombkowski
Mayor, Town of Woodside

Cc: grandjury@sanmateocourt.org

WEST BAY
SANITARY DISTRICT

Serving Our Community Since 1902

500 Laurel Street, Menlo Park, California 94025-3486 (650) 321-0384 (650)321-4265 FAX

SERGIO RAMIREZ
District Manager

In reply, please refer to our File No.

December 22, 2020

The Honorable Danny Y. Chou
Judge of the Superior Court
c/o Jenarda Dubois
Hall of Justice
400 County Center, 2nd Floor
Redwood City, CA 94063-1655

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

Honorable Judge Chou,

Thank you for the opportunity to review and comment on the above reference Grand Jury Report filed on October 7, 2020. The West Bay Sanitary District's response to both the findings and the recommendations are listed below.

FINDINGS:

F1. **Ransomware is a real and growing threat to public entities including those in San Mateo County.**

West Bay agrees with this finding.

F2. **Across the country, local governments and schools represent 12% of all Ransomware attacks.**

West Bay lacks information to fully agree or disagree with this Finding given that it did not conduct the research related to this Report. West Bay, however, accepts the Grand Jury's Finding for the purpose of this Response.

F3. **The direct and indirect costs of Ransomware can be significant.**

West Bay agrees with this finding.

F4. **Cybersecurity reviews and assessments, and an updated, well-executed Cybersecurity plan, are critical components of IT security strategy.**

West Bay agrees with this finding.

F5. A comprehensive Cybersecurity plan should include, at a minimum, information concerning prevention steps, spam and malware software, and backups and full recovery testing.

West Bay agrees with this finding.

F6. The identification of phishing attempts, including the use of spam filters, is an important component to protecting an IT system from Ransomware attacks.

West Bay agrees with this finding.

F7. Testing a full restore of a server to ensure that backups are reliable should be undertaken regularly as part an entity's backup plan to recover lost information.

West Bay agrees with this finding.

F8. Training of new employees, and the recurring training of existing employees, is an important component of defense against Ransomware.

West Bay agrees with this finding.

RECOMMENDATIONS:

R1. 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:

1. System Security (Firewalls, Anti-malware/Antivirus software, use of subnets, strong password policies, updating/patching regularly)
2. Backup & Recovery (In the event of an attack, 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?)
3. 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)

This recommendation has been implemented. While the West Bay Sanitary District has had these three concerns specifically identified above in place prior to this report with the exception of providing employee training on phishing, the District has requested that a report be prepared by a District consultant.

R2. 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 West Bay Sanitary District intends to implement this Recommendation and any recommended actions and/or enhancements from this Recommendation by June 30, 2021.

R3. Given the results of their internal reports, governmental entities may choose to request further guidance by means of a Cybersecurity review from the U.S. Department of Homeland Security and/or a cyber hygiene assessment from the County Controller's Office.

The West Bay Sanitary District will make a request with the Department of Homeland Security, Cybersecurity & Infrastructure Security Agency, for cyber-hygiene services before June 30, 2021 if warranted.

R4. Given the results of their internal reports, government entities may choose to ask their IT departments to review their own Cybersecurity Plan with the detailed template provided by the FCC's Cybersecurity Planning Guide and consider customizing it using FCC's Create Custom Cybersecurity Planning Guide tool (see footnote 52).

The West Bay Sanitary District will utilize the Federal Communications Commission Cyber Security Planning Guide and the FCC Cyber Security Planner to review and update our cyber-security plans, if warranted. This work will be completed on or before June 30, 2021.

Thank you again for your efforts on this matter and allowing the District to respond to the Grand Jury report and share the District's thoughts and opinions.

This response was approved by the West Bay Sanitary District Board of Directors at a special meeting on December 22, 2020.

Sincerely,

Fran Dehn
President of the District Board of the West Bay Sanitary District

cc: West Bay Sanitary District Board
Sergio Ramirez, District Manager

Westborough Water District
P.O. Box 2747 | 2263 Westborough Blvd. | South San Francisco, CA 94080
Phone: 650-589-1435 Fax: 650-589-5167
Email: WWD@WestboroughWater.org Web: WestboroughWater.org

December 10, 2020

Hon. Danny Y. Chou
Judge of Superior Court
c/o Jenarda Dubois
Hall of Justice
400 County Center, 8th Floor
Redwood City, CA 94063-1655

Re: Grand Jury Report on Ransomware

Dear Judge Chou:

I am writing on behalf of the Board of Directors (Board) of the Westborough Water District (WWD). This letter will serve as WWD's formal response to San Mateo Grand Jury's October 7, 2020 report entitled "Ransomware: It Is Not Enough To Think You Are Protected." WWD's Board reviewed and approved (on December 10, 2020) this response to the Grand Jury report's with findings (numbered F1-F8) and four recommendations (R1-R4). Please see the following:

Findings

WWD agrees with findings F1-F8.

Recommendations

The Grand Jury requested that WWD respond to the following four recommendations:

R1. 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:

1. ***System Security (Firewalls, Anti-malware/Antivirus software, use of subnets, strong password policies, updating/patching regularly) '***
2. ***Backup & Recovery (In the event of an attack, 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?)***

3. ***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)***

WWD has requested a report from its IT organization that addresses the concerns identified in the Grand Jury report with respect to system security, backup and recovery, and prevention.

R2. 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.

See response to R1. No later than June 30, 2021, WWD will provide the Board with a comprehensive confidential report describing what actions have been taken and which will be given timely consideration for future enhancements to the existing cybersecurity plan.

R3. Given the results of their internal reports, governmental entities may choose to request further guidance by means of a Cybersecurity review from the U.S. Department of Homeland Security and/or a cyber hygiene assessment from the County Controller's Office.

If necessary, WWD will request further guidance by means of a Cybersecurity review from the U.S. Department of Homeland Security and/or a cyber hygiene assessment from the County Controller's Office.

R4. Given the results of their internal reports, governmental entities may choose to ask their IT departments to review their own Cybersecurity Plan with the detailed template provided by the FCC's Cybersecurity Planning Guide and consider customizing it using FCC's Create Custom Cybersecurity Planning Guide tool (see footnote 52).

Once the results of our internal reports are completed, WWD will consider asking its IT department to review its own Cybersecurity Plan with the detailed template provided by the FCC's Cybersecurity Planning Guide.

Thank you for the opportunity to respond to your report; I trust you will find our comments helpful.

Sincerely,

Darryl A. Barrow

Darryl Barrow
General Manager, Westborough Water District
cc: Board of Directors
via email as a Word document to: grandjury@sanmateocourt.org

WOODSIDE FIRE PROTECTION DISTRICT

3111 WOODSIDE ROAD
WOODSIDE, CALIFORNIA 94062
650.851.1594
FAX 650.851.3960

January 26th, 2021

Hon. Danny Y. Chou

Judge of the Superior Court

c/o Jenarda Dubois

Hall of Justice

400 County Center, 8th Floor

Redwood City, CA 94063-1665

Re: Woodside Fire Protection District Comments and Response to the 2019-2020 Grand Jury Report: "Ransomware: It Is Not Enough To Think You Are Protected

Hon. Judge Chou:

The Woodside Fire Protection District is pleased to respond to the Court's October 7, 2020 letter transmitting the Grand Jury's findings and recommendations on "Ransomware: It Is Not Enough To Think You Are Protected". This report was discussed at the October 26th, 2020 Board of Directors Meeting and was approved by the Board of Directors at the Woodside Fire Protection District Board of Directors meeting on January 25th, 2021.

Responses to Findings:

F1. Ransomware is a real and growing threat to public entities including those in San Mateo County.

Response: The Fire District agrees with the finding.

F2. Across the country, local governments and schools represent 12% of all Ransomware attacks.

Response: The Fire District agrees with the finding.

F3. The direct and indirect costs of Ransomware can be significant.

Response: The Fire District agrees with the finding.

F4. Cybersecurity reviews and assessments, and an updated, well-executed Cybersecurity plan, are critical components of IT security strategy.

Response: The Fire District agrees with the finding.

F5. A comprehensive Cybersecurity plan should include, at a minimum, information concerning prevention steps, spam and malware software, and backups and full recovery testing.

Response: The Fire District agrees with the finding.

F6. The identification of phishing attempts, including the use of spam filters, is an important component to protecting an IT system from Ransomware attacks.

Response: The Fire District agrees with the finding.

F7. Testing a full restore of a server to ensure that backups are reliable should be undertaken regularly as part an entity's backup plan to recover lost information.

Response: The Fire District agrees with the finding.

F8. Training of new employees, and the recurring training of existing employees, is an important component of defense against Ransomware.

Response: The Fire District agrees with the finding.

Additionally, the Fire District reports the following based on the Grand Jury recommendations:

R1. 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 30th, 2020, make a request for a report from their IT organization that addresses the concerns identified in the report, specifically:

1. System Security (Firewalls, Anti-malware/Antivirus software, use of subnets, strong password policies, updating/patching regularly)

2. Backup and Recovery (In the event of an attack, can you shut down your system quickly? What is being backed up, and 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 backup?)

3. 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)

Response: The recommendation has been implemented through our private enterprise.

R2. These confidential internal reports should be provided to the governing body by June 30th, 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.

Response: The recommendation will be implemented within the requested timeframe.

R3. Given the results of their internal reports, governmental entities may choose to request further guidance by means of a Cybersecurity review from the U.S. Department of Homeland Security and/or a cyber hygiene assessment from the County Controller's Office.

Response: The recommendation will request further guidance, if necessary.

R4. Given the results of their internal reports, governmental entities may choose to ask their IT departments to review their own Cybersecurity Plan with the detailed template provided by the FCC's Cybersecurity Planning Guide and consider customizing it using FCC's Create Custom Cybersecurity Planning Guide tool

Response: The recommendation will be implemented.

If there are any questions, please feel free to contact me at (650) 851-1594.

Sincerely,

Robert Lindner

Fire Chief

Woodside School District
3195 Woodside Road Woodside, CA 94062
Office: 650.851.1571 Fax: 650.851.5577

Hon. Danny Y. Chou
Judge of the Superior Court
c/o Jenarda Dubois
Hall of Justice
400 County Center; 2nd Floor
Redwood City, CA 94063-1655
Email: grandjury@sanmateocourt.org

Dear Honorable Judge Davis:

The Woodside Elementary School District (the "District") received and reviewed the 2020-2021 Grand Jury Report entitled "Ransomware: It is Not Enough to Think You Are Protected." We appreciate the Grand Jury's interest in this matter. Having reviewed and considered the Grand Jury's Findings and Recommendations, the District responds as follows, pursuant to section 933.05 of the California Penal Code.

FINDINGS

F1. Ransomware is a real and growing threat to public entities including those in San Mateo County.

The District agrees with this finding.

F2. Across the country, local governments and schools represent 12% of all Ransomware attacks.

The District agrees with this finding.

F3. The direct and indirect costs of Ransomware can be significant.

The District agrees with this finding.

F4. Cybersecurity reviews and assessments, and an updated, well-executed Cybersecurity plan, are critical components of IT security strategy.

The District agrees with this finding.

F5. A comprehensive Cybersecurity 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.

F6. 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.

F7: 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 agrees with this finding.

F8: 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.

RECOMMENDATIONS

R1. 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:

1. *System security (Firewalls, Anti-malware/Antivirus software, use of subnets, strong password policies, updating/patching regularly)*

    - **Firewalls have been deployed on the perimeter network to inspect traffic and limit access both inbound and outbound**
    - **Additional policies have been created to detect intrusion and block access based on connection rates on specific ports**
    - **Antivirus software is deployed inline to scan for viruses and malware; these are also deployed on all client systems**
    - **Filtering software have been deployed to block access to known phishing/malware/dangerous sites to limit exposure to internal users**
    - **DNS filtering software pending deployment to prevent name resolution of sites that may contain command and control facilities**
    - **Additional ransomware/malware detection software will be deployed by 11/30/2020 to monitor and remove improperly deployed executables on servers and workstations.**
    - **Strong password policies have been enabled on the internal servers for all clients**
    - **Patches have been set to deploy frequently within 14 days of release**

2. *Backup & Recovery (In the event of an attack, 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?)*

    - **Backups are conducted to local storage systems and replicated to a cloud repository**
    - **A seven-day offline recovery is available on the cloud service should that backup be compromised**
    - **Local backup storage is locked to specific backup account**
    - **Local backup storage facility also contains Backup snapshot facility to provide block-based recovery and a roll back of corrupted data (should a Ransomware 2.0 event occur).**
    - **Server restore is tested quarterly from local backup storage media**

- **All server systems can be restored directly from local backup media and offsite backup media**

3. *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)*

   - **Additional mail filtering services are pending but rules can be currently created to mark inbound messages as possibly fraudulent.**
   - **Additional training for personnel will be conducted to identify impersonation attempts via whaling attacks and phishing attempts.**

R2. 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 above list summarizes in general terms the items deployed within the network. Providing additional details on the exact technology implemented may impose security risks to our internal network. Additional information can be provided if necessary.**

R3. Given the results of their internal reports, governmental entities may choose to request further guidance by means of a Cybersecurity review from the U.S. Department of Homeland Security[56] and/or a cyber hygiene assessment from the County Controller's Office[57].

- **If deemed necessary to secure additional parts of the infrastructure, we will request further guidance from the Department of Homeland Security.**

Both the Grand Jury Report and these responses were presented to and approved by the District's Board of Trustees at its meeting held on December 15, 2020.

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

Sincerely,

Superintendent

Approved by the Woodside Elementary School District Governing Board