

**Regular Meeting of the Board of Directors  
November 19, 2020  
4:00 pm – 6:00 pm, via Zoom teleconference**

If you are using a computer to join the meeting please click [this link](https://us02web.zoom.us/j/89675733636)<sup>1</sup>. A computer video camera is not required to participate. If you do not have access to a computer or internet during this meeting, or if your computer does not have audio, you can call in by phone: (669) 900-6833 and enter the meeting ID 896 7573 3636 when prompted. If participating by phone only, you will not be able to see presentations or other participants. The teleconference will begin 10 minutes before the meeting is scheduled to begin for those who may need assistance or orientation to the technology.

<b>1. Call to Order</b>
<b>2. Approval of Agenda</b>
<b>3. Introduction of Guests and Staff</b>
<b>4. Public Comment-</b> The Board will hear comments on items that are not on the agenda. The Board cannot act on an item unless it is an emergency as defined under Government Code Sec. 54954.2.
<b>5. Consent Agenda</b> The Board of Directors approves: <b>5.1. <a href="#">Fiscal Year 2021 Draft First Quarter Financial Statements</a></b> The Board of Directors receives into record: <b>5.2. <a href="#">January 6, 2020 Bay Nature Magazine article: <i>What Stewardship Looks Like in the Santa Cruz Mountains</i></a></b> <b>5.3. <a href="#">August 17, 2020 California Environmental Water Network article: <i>Meet Jarrad Fisher - Oakland</i></a></b> <b>5.4. <a href="#">September 30, 2020 Half Moon Bay Review article: <i>Midcoast eucalyptus create growing concern for wildfire</i></a></b> <b>5.5. <a href="#">October 1, 2020 Bay Nature Magazine article: <i>As Fires Continue, Land Managers Start to Survey Ecological Damage and Recovery in Bay Area Parks</i></a></b>
<b>6. Regular Agenda</b> <b>6.1. Executive Director's report</b> <b>6.2. NRCS report</b> <b>6.3. Directors' reports</b> <b>6.4. <a href="#">Board will consider appointment of Kevin Watt as Associate Director.</a></b> <b>6.5. <a href="#">Discuss October 7, 2020 Grand Jury Report: "Ransomware: It is Not Enough To Think You Are Protected" and RCD response.</a></b> <b>6.6. <a href="#">Board will consider Resolution 2020-7: Approval to Enter into Agreement with the California Wildlife Conservation Board for the Mindego Creek Fish Passage Project.</a></b> <b>6.7. <a href="#">Board will consider Resolution 2020-8: Approval to Enter into Agreement with the California Wildlife Conservation Board for the San Pedro Creek Fish Passage Project at Adobe Bridge.</a></b> <b>6.8. <a href="#">Board will consider Resolution 2020-9: Approval to Enter into Agreement with the California Wildlife Conservation Board for the Butano Creek Channel Stabilization and Habitat Enhancement at the Cloverdale Road Bridge Project.</a></b>
<b>7. Adjourn Meeting</b> The next Regular Meeting of the Board of Directors will be December 17, 2020

*Public records that relate to any item on the open session agenda for a regular board meeting are available for public inspection. Those records that are distributed less than 72 hours prior to the meeting are available for public inspection at the same time they are distributed to all members, or a majority of the members of the Board.*

<sup>1</sup> <https://us02web.zoom.us/j/89675733636>

**Minutes of the Regular Meeting of the Board of Directors  
November 19, 2020  
4:00 pm – 6:00 pm  
via Zoom teleconference**

Directors present: Barbara Kossy, TJ Glauthier, Adrienne Etherton, Jim Reynolds

RCD staff present: Kellyx Nelson, Lau Hodges, Amy Kaeser, Joe Issel

Guests present: Eric Schmidt, Melissa Krause

**1. Call to Order**

Kossy called the meeting to order at 4:02 p.m.

**2. Approval of Agenda**

Etherton moved to approve the agenda, Glauthier seconded. Motion passed unanimously.

**3. Introductions of Guests and Staff**

All in attendance introduced themselves.

**4. Public Comment**

There was no public comment.

**5. Consent Agenda**

- Glauthier noted that the RCD's finances were in good shape and vendors were being paid prior to receiving money from funders.
- Nelson noted that Diversity, Equity & Inclusion had been pulled from the agenda while the Board formulated a plan regarding the most appropriate way to discuss it.
- Glauthier moved to approve the consent agenda, Etherton seconded. Motion passed unanimously. Etherton abstained.

**6. Regular Agenda**

**6.1 Executive Director's Report**

- Ten thousand coho salmon released into Pescadero Creek on November 17; over a decade of restoration work had led up to the release. Kaeser did excellent working planning the event with NOAA. CBS News and Half Moon Bay Review attended the event.
- First Rain (previously First Flush) was also on November 17. Noah Katz, the RCD's Water Quality Program Manager, did a great job with safety and outreach despite COVID restrictions. 20 volunteers collected water samples during the storm.
- Post-fire recovery assistance continues: 150 responses to help, 43 site visits, 13 follow up efforts moving forward (ag irrigation to hazardous tree removal to creek protection and more). Replaced 11 burned out culverts on Old Womans Creek Road last week.

Repairs implemented in near record time thanks to partnerships, collaborative funders, and trusting relationships within the community. Ramping up hazard tree assistance.

- The repairs to the Dark Gulch crossing on Old Haul Road were completed end of October.
- Fire Prevention work continues. Working on programmatic or streamlined permitting through Coastal Commission and County. El Granada chipper event Oct 26 and 27. Chipper events Montara Moss Beach Nov 6. La Honda, Loma Mar, Dearborn Park with assistance from local volunteers. Working through relationship with FireSafe Council, likely developing MOU.
- Strategic plan in an early draft and expected to be completed by the end of the year.
  - Etherton said she felt good about the direction the strategic plan was heading. Nelson noted that the communications plan would be started soon and would tie directly into the strategic plan.
- Cutting Green Tape paper scheduled for release on November 30. Nelson will present it at the California Association of RCD's (CARCD). The RCD also sponsored the 2020 CARCD Conference.
- On November 18 the Local Area Formation Commission (LAFCo) voted unanimously to move to a public hearing regarding the RCD's sphere of influence and potential change the RCDs boundaries. Nelson offered a note of thanks the Glauthier for all of his support.

## 6.2 NRCS report

- Jim Howard was unable to attend the meeting therefore no report was given.

## 6.3 Directors' reports

- Etherton participated in First Rain, enjoyed the opportunity, and was interested to learn the results. She had joined a new group, Coastside Families Taking Action, and was on the environmental committee where she had met other members with concerns about water quality; she suggested the RCD reach out.
- Reynolds shared how proud he was of the RCD, specifically of the work in Pescadero.
- Glauthier attended the coho salmon release and expressed enthusiasm. He attended a San Mateo County Harbor District Board of Commissioners meeting, which included a lengthy discussion about water quality and what can be done about it; they were pleased with their partnership with the RCD. He attended the recent LAFCo meeting and was pleased with their decision; Glauthier further noted that it would be a long process but worth it for the reliable revenue.
- Kossy will represent the RCD at the CARCD conference and was giving a lot of thought to the diversity, equity and inclusions themes running throughout it. She recently left her position on the Sequoia Audubon Society Board.

## 6.4 Board will consider appointment of Kevin Watt as Associate Director.

- **ACTION:** Glauthier moved to appoint Kevin Watt as Associate Director, Etherton seconded. Motion passed unanimously.

**6.5 Discuss October 7, 2020 Grand Jury Report: “Ransomware: It is Not Enough To Think You Are Protected” and RCD response.**

- There was discussion of the recommendations and that staff had asked the RCD’s IT consultant to review and help comment.
- Glauthier suggested that the letter, noting the Board had given approval, come from Nelson.

**6.6 Board will consider Resolution 2020-7: Approval to Enter into Agreement with the California Wildlife Conservation Board for the Mindogo Creek Fish Passage Project.**

- There was discussion about the project and the funder’s requirement for this resolution.
- **ACTION:** Glauthier moved to approve Resolution 2020-7, Etherton seconded. Motion passed unanimously.

**6.7 Board will consider Resolution 2020-8: Approval to Enter into Agreement with the California Wildlife Conservation Board for the San Pedro Creek Fish Passage Project at Adobe Bridge.**

- There was discussion about previous efforts to secure funding for this project, partnership with the local watershed coalition; description of the site; and where it is located.
- **ACTION:** Etherton moved to approve Resolution 2020-8, Glauthier seconded. Motion passed unanimously.

**6.8 Board will consider Resolution 2020-9: Approval to Enter into Agreement with the California Wildlife Conservation Board for the Butano Creek Channel Stabilization and Habitat Enhancement at the Cloverdale Road Bridge Project.**

- There was discussion about the project site, potential benefits and the partnerships.
- **ACTION:** Glauthier moved to approve Resolution 2020-9, Reynolds seconded. Motion passed unanimously.

**7 Adjourn Meeting**

- Kossy adjourned the meeting at 5:30 p.m.



# REVENUE

	FY 21	9.30.20	
	Budget	Actual	Remaining
<u>Program Revenue</u>			
Agricultural Ombudsman	\$ 40,866	13,161.99	27,704.01
Climate Mitigation and Adaptation	\$ 196,482	32,783.91	163,697.69
Conservation Technical Assistance	\$ 25,667	8,383.93	17,283.47
Erosion and Sediment Management	\$ 2,839,941	711,490.48	2,128,450.33
Fire and Forestry	\$ 1,499,881	91,824.07	1,408,056.63
Habitat Enhancement	\$ 1,347,176	225,396.49	1,121,779.28
Santa Cruz Mountains Stewardship Network	\$ 1,228,180	36,478.54	1,191,701.46
Stream Gage		5,000.00	(5,000.00)
Water Resources & Conservation	\$ 1,310,977	134,933.42	1,176,043.58
Water Quality	\$ 291,504	27,030.17	264,473.83
Billing Rate Adjustments			-
<b>Subtotal Program Revenue</b>	<b>\$ 8,780,673</b>	<b>\$ 1,286,483</b>	<b>\$ 7,494,190</b>
<u>Other Revenue</u>			
County Contributions	\$ 200,000	200,000.00	-
Individual Contributions	\$ 10,000	5,790.50	4,209.50
Interest Income		549.11	(549.11)
Misc. Income		7,643.74	(7,643.74)
Property Tax	\$ 65,000	6,773.75	58,226.25
<b>Subtotal Other Revenue</b>	<b>\$ 275,000</b>	<b>\$ 220,757</b>	<b>\$ 54,243</b>
<b>Total Revenue</b>	<b>\$ 9,055,673</b>	<b>1,507,240.10</b>	<b>7,548,433.18</b>

# EXPENSES

<u>Operating Expenses</u>			
Personnel (Salaries & Fringe)	\$ 1,671,414	369,370.03	1,302,044.02
Other	\$ 188,000	36,598.37	151,401.63
<b>Subtotal Operating Expenses</b>	<b>\$ 1,859,414</b>	<b>\$ 405,968</b>	<b>\$ 1,453,446</b>
<u>Program Expenses</u>			
Agricultural Ombudsman	\$ 1,000	22.49	977.51
Climate Mitigation and Adaptation	\$ 52,404	636.76	51,767.24
Conservation Technical Assistance	\$ 925	73.68	851.32
Erosion and Sediment Management	\$ 2,725,595	868,706.64	1,856,888.36
Fire and Forestry	\$ 1,158,550	38,105.59	1,120,444.41
Habitat Enhancement	\$ 903,319	131,781.75	771,537.07
Santa Cruz Mountains Stewardship Network	\$ 1,086,715	64,377.86	1,022,337.14
Stream Gage		3,400.00	(3,400.00)
Water Resources & Conservation	\$ 1,170,786	98,846.97	1,071,939.03
Water Quality	\$ 112,871	59,258.65	53,612.35
<b>Subtotal Program Expenses</b>	<b>\$ 7,212,165</b>	<b>\$ 1,265,210</b>	<b>\$ 5,946,954</b>
<b>Total Expenses</b>	<b>\$ 9,071,579</b>	<b>\$ 1,671,179</b>	<b>\$ 7,400,400</b>
<b>NET</b>	<b>\$ (15,906)</b>	<b>\$ (163,939)</b>	<b>\$ 148,033</b>
<b>Operating Reserve Allocation</b>	<b>\$ 100,000</b>		

# San Mateo Resource Conservation District

## Balance Sheet

As of September 30, 2020

Sep 30, 20

### ASSETS

#### Current Assets

##### Checking/Savings

1030 - Checking Account (5269) 1,564,934.97

1031 - Restricted State Funds (5012) (Butano Channel) 2,997.08

1032 - Operating Reserve (0202) 350,025.89

Total Checking/Savings 1,917,957.94

##### Accounts Receivable

1200 - Accounts Receivable 2,524,297.80

Total Accounts Receivable 2,524,297.80

Total Current Assets 4,442,255.74

**TOTAL ASSETS 4,442,255.74**

### LIABILITIES & EQUITY

#### Liabilities

##### Current Liabilities

##### Accounts Payable

2000 - Accounts Payable 422,827.57

Total Accounts Payable 422,827.57

##### Credit Cards

2025 - Visa - Nelson - 1952 62.49

2035 - Visa - Issel - 0129 201.43

Total Credit Cards 263.92

##### Other Current Liabilities

2045 - Accrued Payroll 110,158.43

2060 - Accrued Time Off 73,473.50

##### 2400 - Deferred Revenue

2401 - NFWF - San Bruno Mtn Butterfly 8,665.00

2405 - NFWF - Bonde Weir 3,263.86

2406 - CARCD - Pesc. Water Monitoring 2,500.00

2409 - SCMSN- Regional Climate Action 39,011.53

2410 - Santa Cruz Mountain Stewardship 139,868.33

2411 - SCMSN - Atlas Project 133,332.24

2412 - SCMSN-Spotlight Stewardship 10,608.88

2413 - SCMSN-Permitting 165.64

2414 - SCMSN - Veg Gen 169,807.52

2415 - SCMSN - DEI 28,364.54

2416 - SCMSN - COVID 2,429.20

2420 - MROSD - Driscoll Ranch 7,386.95

2421 - MROSD - Apple Orchard 13,569.75

2425 - Randtron Antenna 3,184.32

2430 - PG&E - Butano Mitigation Proj. 790,419.16

2431 - PG&E - Project Development 33,668.57

2432 - PG&E Foundation - Hedge Rows 4,227.07

2433 - PG&E - Tree Planting 90,091.00

2434 - PG&E - San Bruno Mountain 161,513.52

# San Mateo Resource Conservation District

## Balance Sheet

As of September 30, 2020

	<u>Sep 30, 20</u>
2435 - Cloverdale Ponds	75,132.38
2451 - SMC - Butano Channel	533,313.52
2470 - SVCF - Carbon Farm Planning	4,229.29
2471 - SVCF - Mobile Laundry Grant	30,000.00
2473 - RLF - TMDL Pescadero Butano	42,982.63
2475 - SAM - First Flush	18,457.79
2476 - SAM - Mitigation	11,228.54
2490 - POST - DR Match Funds	52,717.23
2491 - POST - Rangeland Compost	5,845.65
Total 2400 - Deferred Revenue	<u>2,415,984.11</u>
Total Other Current Liabilities	<u>2,599,616.04</u>
Total Current Liabilities	3,022,707.53
Long Term Liabilities	
2500 - Recoverable Grants	
2520 - Silicon Valley Foundation	<u>100,000.00</u>
Total 2500 - Recoverable Grants	<u>100,000.00</u>
Total Long Term Liabilities	<u>100,000.00</u>
Total Liabilities	3,122,707.53
Equity	
3500 - Net Assets	1,483,486.90
Net Income	<u>-163,938.69</u>
Total Equity	<u>1,319,548.21</u>
TOTAL LIABILITIES & EQUITY	<u><u>4,442,255.74</u></u>

# San Mateo Resource Conservation District

## Profit & Loss

July through September 2020

	<u>TOTAL</u>
Ordinary Income/Expense	
Income	
4010 • Contracts	1,289,013.75
4020 • Donations	
4030 • General Support Donations	2,590.50
4035 • Individual Donation	3,200.00
Total 4020 • Donations	<u>5,790.50</u>
4040 • Interest	549.11
4050 • SMC Contributions	
4055 • SMC Property Tax	6,443.75
4065 • SMC Operating Support	200,000.00
Total 4050 • SMC Contributions	<u>206,443.75</u>
4070 • Legal Settlements	5,442.99
Total Income	<u>1,507,240.10</u>
Gross Profit	1,507,240.10
Expense	
5100 • Personnel	
5110 • Salary	312,407.84
5120 • Benefits	56,962.19
Total 5100 • Personnel	<u>369,370.03</u>
5200 • Operating Expense	
5205 • Bank Fees	78.67
5210 • Communications	2,031.52
5215 • Dues-Membership-Subscriptions	9,375.00
5220 • Equipment	3,687.53
5225 • Information Technology	1,886.02
5235 • Office Supplies	244.89
5240 • Rent	11,368.80
5245 • Accounting Services	3,495.00
5270 • Prof. Development & Meetings	336.89
Total 5200 • Operating Expense	<u>32,504.32</u>
5300 • Program Expenses	
5310 • Project Implementation	1,269,304.44
Total 5300 • Program Expenses	<u>1,269,304.44</u>
Total Expense	<u>1,671,178.79</u>
Net Ordinary Income	<u>-163,938.69</u>
Net Income	<u><u>-163,938.69</u></u>



# San Mateo Resource Conservation District

## Profit & Loss

July through September 2020

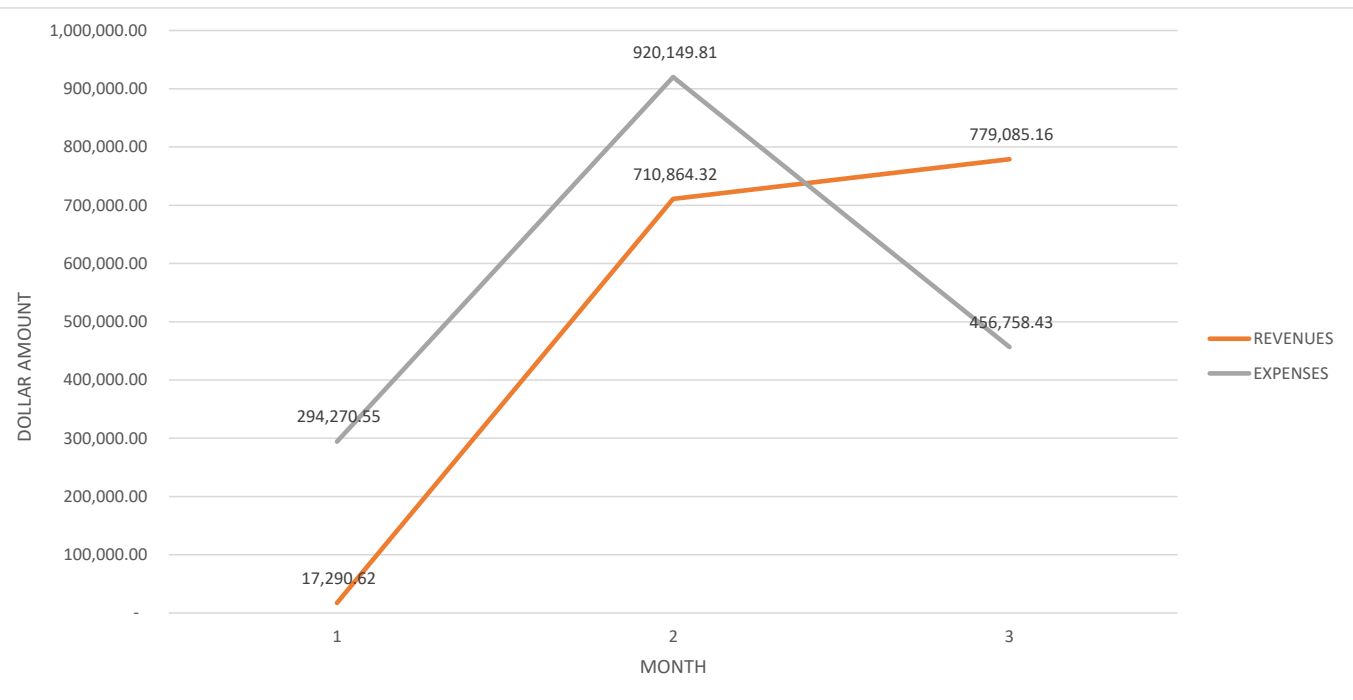
	<u>Jul 20</u>	<u>Aug 20</u>	<u>Sep 20</u>
Ordinary Income/Expense			
Income			
4010 • Contracts	9,917.01	702,290.22	576,806.52
4020 • Donations			
4030 • General Support Donations	1,890.50	700.00	0.00
4035 • Individual Donation	2,200.00	0.00	1,000.00
Total 4020 • Donations	4,090.50	700.00	1,000.00
4040 • Interest	119.27	145.52	284.32
4050 • SMC Contributions			
4055 • SMC Property Tax	3,163.84	2,285.59	994.32
4065 • SMC Operating Support	0.00	0.00	200,000.00
Total 4050 • SMC Contributions	3,163.84	2,285.59	200,994.32
4070 • Legal Settlements	0.00	5,442.99	0.00
Total Income	17,290.62	710,864.32	779,085.16
Gross Profit	17,290.62	710,864.32	779,085.16
Expense			
5100 • Personnel			
5110 • Salary	111,254.05	98,477.04	102,676.75
5120 • Benefits	15,860.91	21,604.87	19,496.41
Total 5100 • Personnel	127,114.96	120,081.91	122,173.16
5200 • Operating Expense			
5205 • Bank Fees	0.00	0.00	78.67
5210 • Communications	413.48	450.85	1,167.19
5215 • Dues-Membership-Subscriptions	4,775.00	2,100.00	2,500.00
5220 • Equipment	581.41	1,158.63	1,947.49
5225 • Information Technology	301.88	565.64	1,018.50
5235 • Office Supplies	244.89	0.00	0.00
5240 • Rent	480.00	0.00	10,888.80
5245 • Accounting Services	0.00	1,890.00	1,605.00
5270 • Prof. Development & Meetings	238.89	75.00	23.00
Total 5200 • Operating Expense	7,035.55	6,240.12	19,228.65
5300 • Program Expenses			
5310 • Project Implementation	160,120.04	793,827.78	315,356.62
Total 5300 • Program Expenses	160,120.04	793,827.78	315,356.62
Total Expense	294,270.55	920,149.81	456,758.43
Net Ordinary Income	-276,979.93	-209,285.49	322,326.73
Net Income	<u>-276,979.93</u>	<u>-209,285.49</u>	<u>322,326.73</u>

# San Mateo Resource Conservation District

## Profit & Loss

July through September 2020

	<u>TOTAL</u>
Ordinary Income/Expense	
Income	
4010 • Contracts	1,289,013.75
4020 • Donations	
4030 • General Support Donations	2,590.50
4035 • Individual Donation	3,200.00
Total 4020 • Donations	5,790.50
4040 • Interest	549.11
4050 • SMC Contributions	
4055 • SMC Property Tax	6,443.75
4065 • SMC Operating Support	200,000.00
Total 4050 • SMC Contributions	206,443.75
4070 • Legal Settlements	5,442.99
Total Income	1,507,240.10
Gross Profit	1,507,240.10
Expense	
5100 • Personnel	
5110 • Salary	312,407.84
5120 • Benefits	56,962.19
Total 5100 • Personnel	369,370.03
5200 • Operating Expense	
5205 • Bank Fees	78.67
5210 • Communications	2,031.52
5215 • Dues-Membership-Subscriptions	9,375.00
5220 • Equipment	3,687.53
5225 • Information Technology	1,886.02
5235 • Office Supplies	244.89
5240 • Rent	11,368.80
5245 • Accounting Services	3,495.00
5270 • Prof. Development & Meetings	336.89
Total 5200 • Operating Expense	32,504.32
5300 • Program Expenses	
5310 • Project Implementation	1,269,304.44
Total 5300 • Program Expenses	1,269,304.44
Total Expense	1,671,178.79
Net Ordinary Income	-163,938.69
Net Income	<u><u>-163,938.69</u></u>



Superior Court of California, County of San Mateo  
Hall of Justice and Records  
400 County Center  
Redwood City, CA 94063-1655

NEAL TANIGUCHI  
COURT EXECUTIVE OFFICER  
CLERK & JURY COMMISSIONER

(650) 261-5066  
FAX (650) 261-5147  
[www.sanmateocourt.org](http://www.sanmateocourt.org)

October 7, 2020

Governing Board  
San Mateo County Resource Conservation District  
625 Miramontes Street, Suite 103  
Half Moon Bay, CA 94019

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

Dear Governing Board:

The 2019-2020 Grand Jury filed a report on October 7, 2020 which contains findings and recommendations pertaining to your agency. Your agency must submit comments, within 90 days, to the Hon. Danny Y. Chou. Your agency's response is due no later than January 5, 2021. **Please note that the response should indicate that it was approved by your governing body at a public meeting.**

For all findings, your responding agency shall 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, as to each Grand Jury recommendation, your responding agency shall 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.

Please submit your responses in all of the following ways:

**1. Responses to be placed on file with the Clerk of the Court by the Court Executive Office.**

- Prepare original on your agency's letterhead, indicate the date of the public meeting that your governing body approved the response address and mail to Judge Chou.

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

**2. Responses to be placed at the Grand Jury website.**

- Copy response and send by e-mail to: [grandjury@sanmateocourt.org](mailto:grandjury@sanmateocourt.org). (Insert agency name if it is not indicated at the top of your response.)

**3. Responses to be placed with the clerk of your agency.**

- File a copy of the response directly with the clerk of your agency. Do not send this copy to the Court.

For up to 45 days after the end of the term, the foreperson and the foreperson's designees are available to clarify the recommendations of the report. To reach the foreperson, please call the Grand Jury Clerk at (650) 261-5066.

If you have any questions regarding these procedures, please do not hesitate to contact Paul Okada, Chief Deputy County Counsel, at (650) 363-4761.

Very truly yours,



Neal Taniguchi  
Court Executive Officer

Enclosure

cc: Hon. Danny Y. Chou  
Paul Okada



## **Ransomware: It Is Not Enough To Think You Are Protected**

### **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,<sup>1</sup> 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 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

---

<sup>1</sup> See Appendix F: Public Entities in San Mateo County (Cities, County, School Districts, Special Districts)

that only limited training is provided for new employees with little or no recurring training provided for current employees.<sup>2</sup>

Ransomware and other malware attacks are a test to an organization's backup and restoration procedures.<sup>3</sup> 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 than owning their own computing infrastructure or data centers, companies can rent access to

---

<sup>2</sup> Grand Jury interviews

<sup>3</sup> Epicor Corporation, *Protecting Yourself From Ransomware*, January 2020

anything from applications to storage from a cloud service provider.<sup>4</sup> Some examples of this are Yahoo Mail, services like Google Docs, and customer relationship management software.<sup>5</sup>

## 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.<sup>6</sup>

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.<sup>7</sup> By planting the malware but delaying its activation, Ransomware 2.0 can infect backups thus defeating their value.

---

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

<sup>5</sup> Pearson Education, Ubuntu Unleashed 2015 Edition: Covering 14.10 and 15.04, page 655

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

<sup>7</sup> <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.<sup>8</sup> 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,<sup>9</sup> when organizations are seeking to avoid embarrassment, or when the attacks were simply undetected or untraceable.<sup>10</sup> This has been true even in San Mateo County where local public governing entities have had Ransomware attacks that were not publicly reported.<sup>11</sup>

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.”<sup>12</sup> The cost to the city of Atlanta to recover from its Ransomware breach was estimated at \$17 million.<sup>13</sup> Similarly, a recent Baltimore Ransomware breach is estimated to have cost over \$18 million.<sup>14</sup> In 2020, the UC San Francisco School of Medicine paid \$1.14 million in ransom to recover its own data.<sup>15</sup> 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:<sup>16</sup>

- Direct Costs:
  - Paying the ransom to obtain an encryption key and hoping that it works;
  - Expenditures for outside IT professionals and new systems providers to plan and implement improved breach security based on new Ransomware strategies;

---

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

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

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

<sup>11</sup> Grand Jury survey responses

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

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

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

<sup>15</sup> San Jose Mercury News, David Wu, “UCSF pays \$1.14 million ransom to recover data”, July 4, 2020

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

- 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,<sup>17</sup> 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.<sup>18</sup> 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.<sup>19</sup> 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

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.

---

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

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

<sup>19</sup> Appendix F

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.<sup>20</sup>

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.<sup>21</sup>
- 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"<sup>22</sup>: 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 infected server units followed by the application of the incremental backups of the database to complete the restore.

---

<sup>20</sup> Grand Jury Interview

<sup>21</sup> These services include onsite and offsite backup and recovery services which are usually located outside the immediate locale.

<sup>22</sup> Management Wire, *The 3-2-1 Backup Rule and Effective Cybersecurity Strategy*, January 7, 2020.

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:<sup>23</sup> *“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.<sup>24</sup> 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:<sup>25</sup>

*“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<sup>26</sup>, a lack of understanding of the complexity of a well-written, well-executed Cybersecurity Plan.<sup>27</sup> 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”.<sup>28</sup>

#### Investigation Results Regarding Backup/Restore/Maintenance

The Grand Jury survey and follow-up interviews revealed that, while many local agencies have backup plans,<sup>29</sup> only a portion of those same agencies had successfully recovered lost files from backups and none of the survey responders had ever done a full restore of a server.<sup>30</sup> When an

---

<sup>23</sup> Appendix A – Question #1

<sup>24</sup> Grand Jury Interview

<sup>25</sup> Appendix A – Question #2

<sup>26</sup> Grand Jury Interviews

<sup>27</sup> Federal Communications Commission, *Cyber Security Planning Guide*, October 2012.

<sup>28</sup> National League of Cities report, *Protecting Our Data: What Cities Should Know About Cybersecurity*, page 8

<sup>29</sup> Appendix A – Question #3

<sup>30</sup> Appendix A – Question #4

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.<sup>31</sup> 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<sup>32</sup> 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<sup>33</sup> provide the most complete backup and the fastest restore option.<sup>34</sup>

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.”<sup>35</sup>

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.”<sup>36</sup>

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 needing improvements.<sup>37</sup> As one survey responder commented, “The answer is yes, but a lot more needs to be done.”

---

<sup>31</sup> Structured Query Language (SQL) is a programming language

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

<sup>33</sup> Image backup consists of block by block storing of the contents of a hard drive

<sup>34</sup> <https://www.itnow.com/file-backup-vs-image-backup-which-is-best/>

<sup>35</sup> Zerto, Raj Samani, *Ransomware – Mitigating the Threat of Cyber Attacks*, 2019

<sup>36</sup> Epicor, *Protecting Yourself from Ransomware*, January 2020

<sup>37</sup> Grand Jury Survey responses

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.”<sup>38</sup> The article concluded that even with the best training programs and defenses, the human element may never be completely overcome.<sup>39</sup> 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.”<sup>40</sup> 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.<sup>41</sup>

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.<sup>42</sup> “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.”<sup>43</sup>

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 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.

---

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

<sup>39</sup> Ibid

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

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

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

<sup>43</sup> Epicor, *Protecting Yourself from Ransomware*, January 2020

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.<sup>44</sup> 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.<sup>45</sup> 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”.<sup>46</sup> 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<sup>47</sup>: “*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.”<sup>48</sup>

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;

---

<sup>44</sup> Grand Jury interviews

<sup>45</sup> Ibid

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

<sup>47</sup> Appendix A - Question #6

<sup>48</sup> Grand Jury Survey response

- 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:<sup>49</sup>

- Use Subnets<sup>50</sup> 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.<sup>51</sup>
- 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.<sup>52</sup> 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."<sup>53</sup> 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.<sup>54</sup> 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 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.<sup>55</sup>

---

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

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

<sup>51</sup> 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.

<sup>52</sup> 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>

<sup>53</sup> Ibid, page PDS-1

<sup>54</sup> eMails received from public domain accounts

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



## 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.
- 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<sup>56</sup> and/or a cyber hygiene assessment from the County Controller's Office.<sup>57</sup>

---

<sup>56</sup> <https://www.us-cert.gov/resources/assessments>

<sup>57</sup> 2018-2019 San Mateo Grand Jury Report – Security of Election Announcements

- 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 24<sup>th</sup> and 28<sup>th</sup> 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>

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](http://www.knowbe4.com)

[www.lucysecurity.com](http://www.lucysecurity.com)

[www.metacompliance.com](http://www.metacompliance.com)


[www.mediapro.com](http://www.mediapro.com)

[www.cofense.com](http://www.cofense.com)

[www.elevatesecurity.com](http://www.elevatesecurity.com)

[www.securitymentor.com](http://www.securitymentor.com)

## APPENDIX C – EMAIL MESSAGE RULE - EXTERNAL

 Send	To...	Name Hidden
	Cc...	
Account ▾	Subject:	[EXTERNAL] Setup a Conference Call to review nest steps

CAUTION: EXTERNAL EMAIL. Verify before you click links or open attachments. Questions? Contact GIS.

## 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](http://www.unitrends.com)  
[www.barracuda.com](http://www.barracuda.com)  
[www.carbonite.com](http://www.carbonite.com)  
[www.commvault.com](http://www.commvault.com)  
[www.dellemc.com](http://www.dellemc.com)  
[www.axcient.com](http://www.axcient.com)  
[www.cohesity.com](http://www.cohesity.com)  
[www.datto.com](http://www.datto.com)  
[www.infrascale.com](http://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 Lomas 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 Francisco 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

---

**RESOLUTION 2020-7****APPROVAL TO ENTER INTO AGREEMENT WITH THE CALIFORNIA WILDLIFE  
CONSERVATION BOARD FOR THE MINDEGO CREEK FISH PASSAGE PROJECT**

**WHEREAS**, the San Mateo Resource Conservation District is a Special District organized under Division 9 of the California Public Resources Code with an original petition granted on July 1, 1939;

**WHEREAS**, the San Mateo Resource Conservation District is defined in Section 3501 of the Government Code as a public agency;

**WHEREAS**, funds were made available to the Wildlife Conservation Board through the Parks, Environment, and Water Bond of 2018 (Proposition 68) for projects that enhance State and local parks, environmental protection and restoration, water infrastructure, and flood protection;

**WHEREAS**, San Mateo Resource Conservation District intends to address fish passage and instream habitat in Mindego Creek through removal of a channel-spanning dam and fish ladder, relocation of water diversion intake, channel reconstruction, and habitat enhancements;

**WHEREAS**, the California Wildlife Conservation Board may encumber \$747,488.97 through the Wildlife Corridor and Fish Passage Program for the San Mateo Resource Conservation District to implement the Mindego Creek Fish Passage Project;

**WHEREAS**, the California Wildlife Conservation Board requires a resolution from the governing body of the grant recipient authorizing its designee to sign a financial assistance agreement, and any amendments thereto;

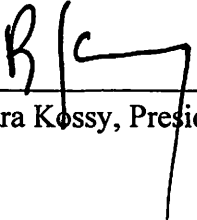
**NOW THEREFORE BE IT RESOLVED** that the San Mateo Resource Conservation District Board of Directors hereby:

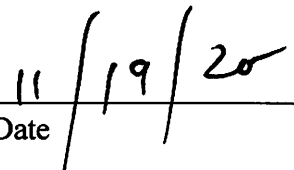
1. Approves the filing of an application for funding from the Wildlife Conservation Board;
2. Authorizes its Executive Director to conduct negotiations, execute, submit, and sign all documents including but not limited to applications, agreements, amendments, payment

requests, and other documents which may be necessary for the completion of the proposed project;

3. Certifies that the Resource Conservation District will comply with all federal, state and local environmental, public health, and other appropriate laws and regulations applicable to the project and will obtain or will ensure that the other project partners obtain all appropriate permits applicable to the project; and
4. Further commits to the terms and conditions specified in the grant agreement.

**ADOPTED** at a regular meeting of the Board of Directors of the San Mateo Resource Conservation District on November 19, 2020.

  
\_\_\_\_\_  
Barbara Kossy, President

  
\_\_\_\_\_  
Date

**RESOLUTION 2020-8****APPROVAL TO ENTER INTO AGREEMENT WITH THE CALIFORNIA WILDLIFE  
CONSERVATION BOARD FOR THE SAN PEDRO CREEK FISH PASSAGE PROJECT  
AT ADOBE BRIDGE**

**WHEREAS**, the San Mateo Resource Conservation District is a Special District organized under Division 9 of the California Public Resources Code with an original petition granted on July 1, 1939;

**WHEREAS**, the San Mateo Resource Conservation District is defined in Section 3501 of the Government Code as a public agency;

**WHEREAS**, funds were made available to the Wildlife Conservation Board through the Parks, Environment, and Water Bond of 2018 (Proposition 68) for projects that enhance State and local parks, environmental protection and restoration, water infrastructure, and flood protection;

**WHEREAS**, San Mateo Resource Conservation District intends to address fish passage and instream habitat in San Pedro Creek by developing designs and permits for the remediation of a priority fish passage barrier at Adobe Bridge and riparian habitat enhancements;

**WHEREAS**, the California Wildlife Conservation Board may encumber \$170,067.24 through the Wildlife Corridor and Fish Passage Program for the San Mateo Resource Conservation District to implement the San Pedro Creek Fish Passage Project at Adobe Bridge;

**WHEREAS**, the California Wildlife Conservation Board requires a resolution from the governing body of the grant recipient authorizing its designee to sign a financial assistance agreement, and any amendments thereto;

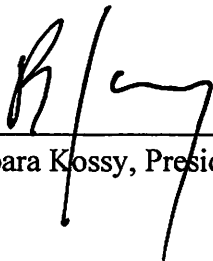
**NOW THEREFORE BE IT RESOLVED** that the San Mateo Resource Conservation District Board of Directors hereby:

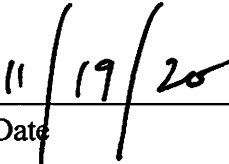
1. Approves the filing of an application for funding from the Wildlife Conservation Board;
2. Authorizes its Executive Director to conduct negotiations, execute, submit, and sign all documents including but not limited to applications, agreements, amendments, payment

requests, and other documents which may be necessary for the completion of the proposed project;

3. Certifies that the Resource Conservation District will comply with all federal, state and local environmental, public health, and other appropriate laws and regulations applicable to the project and will obtain or will ensure that the other project partners obtain all appropriate permits applicable to the project; and
4. Further commits to the terms and conditions specified in the grant agreement.

**ADOPTED** at a regular meeting of the Board of Directors of the San Mateo Resource Conservation District on November 19, 2020.

  
\_\_\_\_\_  
Barbara Kossy, President

  
\_\_\_\_\_  
Date



**RESOLUTION 2020-9****APPROVAL TO ENTER INTO AGREEMENT WITH THE CALIFORNIA WILDLIFE  
CONSERVATION BOARD FOR THE BUTANO CREEK CHANNEL STABILIZATION  
AND HABITAT ENHANCEMENT AT THE CLOVERDALE ROAD BRIDGE PROJECT**

**WHEREAS**, the San Mateo Resource Conservation District is a Special District organized under Division 9 of the California Public Resources Code with an original petition granted on July 1, 1939;

**WHEREAS**, the San Mateo Resource Conservation District is defined in Section 3501 of the Government Code as a public agency;

**WHEREAS**, funds were made available to the Wildlife Conservation Board through the Parks, Environment, and Water Bond of 2018 (Proposition 68) for projects that enhance State and local parks, environmental protection and restoration, water infrastructure, and flood protection;

**WHEREAS**, San Mateo Resource Conservation District intends to address channel incision at Cloverdale bridge, pier scour, and bank instability, while providing habitat enhancement benefits for salmonids and other aquatic species in Butano Creek through addressing the Cloverdale Road bridge and resultant stream degradation;

**WHEREAS**, the California Wildlife Conservation Board may encumber \$1,734,681 through the Wildlife Corridor and Fish Passage Program for the San Mateo Resource Conservation District to implement the Butano Creek Channel Stabilization and Habitat Enhancement at the Cloverdale Road Bridge Project;

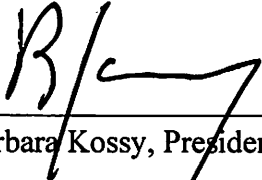
**WHEREAS**, the California Wildlife Conservation Board requires a resolution from the governing body of the grant recipient authorizing its designee to sign a financial assistance agreement, and any amendments thereto;

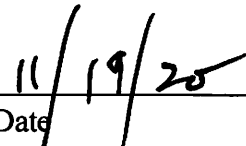
**NOW THEREFORE BE IT RESOLVED** that the San Mateo Resource Conservation District Board of Directors hereby:

1. Approves the filing of an application for funding from the Wildlife Conservation Board;

2. Authorizes its Executive Director to conduct negotiations, execute, submit, and sign all documents including but not limited to applications, agreements, amendments, payment requests, and other documents which may be necessary for the completion of the proposed project;
3. Certifies that the Resource Conservation District will comply with all federal, state and local environmental, public health, and other appropriate laws and regulations applicable to the project and will obtain or will ensure that the other project partners obtain all appropriate permits applicable to the project; and
4. Further commits to the terms and conditions specified in the grant agreement.

**ADOPTED** at a regular meeting of the Board of Directors of the San Mateo Resource Conservation District on November 19, 2020.

  
\_\_\_\_\_  
Barbara Kossy, President

  
\_\_\_\_\_  
Date