July 27, 2020

Lucy Dilworth, Foreperson
Marin County Civil Grand Jury
3501 Civic Center Drive, Room #275
San Rafael, CA 94903

Dear Foreperson Dilworth:

The City of Mill Valley has received the Grand Jury Report "Cyberattacks: A Growing Threat to Marin Government" dated May 11, 2020. The Grand Jury has requested a response to Findings F3-F10 and Recommendations R4-R9. The report was reviewed and considered by the Mill Valley City Council at the July 20, 2020 regular meeting. Enclosed please find the City's response.

Should the members of the Grand Jury require any additional information, please contact City Manager Alan Piombo, at apiombo@cityofmillvalley.org.

Sincerely,

Sashi McEntee,
Mayor

Enclosure

Cc: Judge Sweet

Response to Grand Jury Report

Report Title: Cyberattacks: A Growing Threat to Marin Government

Report Date: May 11, 2020

Respondent/Agency Name: Mill Valley City Council

Response Date: July 20, 2020

FINDINGS

The City agrees with findings **F3, F7, F8, and F10.**

The City disagrees wholly or partially with findings **F4, F5, F6 and F9.**

RECOMMENDATIONS

Recommendations numbered **R4, R5, R7 (2 of the 4 Best Practices)** and **R8 (2 of the 8 of the Other Best Practices)** have been implemented.

Recommendation **R8 (3 of the 8 of the Other Best Practices)** have been partially implemented.

Recommendations numbered**, R6, R9** have not yet been implemented, but will be implemented in the future.

Recommendations numbered **R7 (2 of the 4 best practices)** and **R8 (three of the 8 of the Other Best Practices)** require further analysis.

Signed: Sashi McEntee
Sashi McEntee, Mayor

Date: 7/20/2020

Number of pages attached: 9

Attachment A

Report Title: Cyberattacks: A Growing Threat to Marin Government

Respondent/Agency Name: City of Mill Valley

PART I - FINDINGS AND RESPONSES

Note - The responses below have been made from the perspective of the City of Mill Valley's experience with cybersecurity. We do not have full insight on the cybersecurity practices of other Cities and Towns in Marin County.

F3. **Transparency is lacking regarding cybersecurity because past breaches have not been publicly disclosed, and city and town councils have not facilitated public discussion of cybersecurity issues.**

Response: Agree.

F4. **Most elected officials in Marin's cities and towns are not sufficiently engaged in ensuring robust cybersecurity policies and procedures are in place.**

Response: Disagree. The Mill Valley City Council has and continues to support, through its annual budget, managed IT services that address cybersecurity measures.

F5. **County and municipal officials and managers have been generally unaware of breaches that have occurred outside their own agencies in Marin and therefore have not felt the need to collaborate on measures to improve cybersecurity.**

Response: Disagree partially. The City of Mill Valley has not consistently been made aware of breaches outside of our agency, however issues of cybersecurity have been discussed by the Marin Managers Association.

F6. **Municipalities have been lax in following FBI guidance that cybersecurity breaches be reported to federal law enforcement.**

Response: Disagree. The City has not experienced a cybersecurity breach that would have been required to be reported to federal law enforcement. The City maintains Department of Justice compliant network connectivity to serve our Police Department.

F7. **Marin's cities and towns have not made a concerted effort to standardize around a common set of best practices with respect to cybersecurity.**

Response: Agree

F8. **The Marin County Council of Mayors & Councilmembers has not made cybersecurity a priority, which has minimized the awareness and engagement of elected officials in cybersecurity matters.**

Response: Agree

F9. **The Marin Managers Association has not done enough to facilitate the sharing of cybersecurity information and resources among its members.**

Response: Disagree. In December 2019, the City of San Rafael made a presentation to the Marin Managers Association about a recent overhaul of their IT service delivery model (including cybersecurity). Their presentation included a consultant they hired to conduct an assessment of their service model and the president of the company who manages their cybersecurity.

F10. **Various low-cost best practices exist that could, if implemented, significantly improve the cybersecurity posture of Marin's cities and towns.**

Response: Agree

PART II - RECOMMENDATIONS AND RESPONSES

R4. **Starting in fiscal year 2020–2021, the county board of supervisors and the city and town councils should request their managers report, at least annually, regarding their cybersecurity profile and any measures being taken to improve it.**

Response: The recommendation has been implemented.

See summary attached - City of Mill Valley Annual Cybersecurity Review and Report, July 2020.

R5. **Starting in fiscal year 2020–2021, the county, cities, and towns should convene periodic discussions, at least annually, in a public forum such as a board or council meeting, regarding the importance of good cybersecurity practices for our government, residents, and other organizations.**

Response: The recommendation has been implemented.

By bringing this item to Council on July 20, 2020, we are initiating the first annual public meeting item on cybersecurity. See summary attached - City of Mill Valley Annual Cybersecurity Review and Report, July 2020.

Also, starting in October 2020, the County of Marin will host a National Cyber Security

Awareness Month event that is open to members of the public to facilitate a discussion on cybersecurity. As a member of the recently formed Marin Information Security Collaboration (MISC), the City of Mill Valley will help promote this event to our residents and organizations.

R6. **The county and each city and town should adopt a policy to report to federal law enforcement any cybersecurity intrusion that results in financial fraud or unauthorized disclosure of information and make that intrusion public.**

Response: This recommendation has not yet been implemented, but will be implemented in the future. City staff will commit to developing a policy in Fiscal Year 20/21.

The County of Marin has access to existing security policy templates that have been developed in collaboration with the California Counties Information Services Director's Association (CCISDA) Information Security Council (ISC). These templates will be shared with the members of the recently formed Marin Information Security Collaboration (MISC) and will be considered in the development of the City of Mill Valley's own security policies.

R7. **Within 180 days of the date of this report, cities and towns should implement the first four practices described in the Best Practices section of this report, regarding (1) mandatory user training, (2) email flagging and filtering, (3) password management, and (4) backup.**

Response:

These recommendations have been implemented: (2) Email flagging and filtering, (4) backup. The City has recently implemented email flagging/filtering and has conducted daily backups and monthly testing for years.

These recommendations require further analysis: (1) Mandatory user training, (3) password management. Staff will need to review the practices and determine if the timeframe is feasible and resources are available. The City is committed to implementing as many of the best practices as is financially feasible. Staff will make a recommendation to the City Manager on the feasibility of full implementation of R7 in in Fiscal Year 20/21.

R8. **In fiscal year 2020–2021, cities and towns should complete an analysis of the feasibility of implementing the remainder of the practices described in the Best Practices section of this report.**

Response:

These recommendations have been implemented: Automated malware detection and removal, Monitoring systems.

These recommendations have been partially implemented: Use of expert resources, Firewalls, Hardware and patching

These recommendations require further analysis: Management of mobile devices, Documentation, Vulnerability assessments

Staff will need to review the practices and determine if the timeframe is feasible and resources are available. The City is committed to implementing as many of the best practices as is financially feasible. Staff will make a recommendation to the City Manager on the feasibility of the full implementation of R8 in Fiscal Year 20/21.

R9. In fiscal year 2020–2021, cities and towns should, through the Marin Managers Association, complete an analysis of the feasibility of contracting with a cybersecurity expert to be available to cities and towns on a shared basis, in order to raise the overall level of cybersecurity in Marin's cities and towns.

Response: This recommendation has not yet been implemented, but will be implemented in the future.

The Mill Valley City Manager will work with the Marin Managers Association to add the consideration of hiring a cybersecurity firm to the list of potential shared services that is currently in development.

City of Mill Valley
Annual Cybersecurity Review and Report
July 2020

2020 Scorecard

Implemented = 6

Partially Implemented =3

Not Implemented = 7

Review of Cybersecurity Best Practices

This review is based on the Marin County Civil Grand Jury Report: Cyberattacks: A Growing Threat to Marin Government: https://tinyurl.com/yazumw2e

1. Employee training. The Grand Jury recommends regular, mandatory employee training to educate and motivate employees.

   The City does not currently conduct Information Security employee training. This is an inexpensive measure that would strengthen security, and the City will initiate implementation in the upcoming 20/21 Fiscal Year.

2. Email Flagging and Filtering. The Grand Jury recommends a flag system to notify employees that an email is sent by someone from outside the organization. All email systems should also have spam filters, that identify suspicious emails.

   The City has implemented email flagging and filtering.

3. Password and User Account Management. The Grand Jury recommends:
   a. Password policies that require users to use complex passwords to avoid sharing passwords or using the same password on multiple systems, and to change passwords periodically, at least every six months.
   b. User account management which includes documented security procedures to inventory user accounts and ensure conformity with password policies.
   c. Use of "password managers" where feasible.
   d. Two-factor authentication.

Workstations are programmed to require users to change their passwords every 2 weeks, however, there is no function to make them complex and disallow repeating the same passwords. The other recommendations on this list are not currently implemented by the City. This is an inexpensive measure that would strengthen security, and the City will initiate implementation in the upcoming 20/21 Fiscal Year.

4. Data and System Backups – The Grand Jury recommends the City conduct daily backups and tests the system regularly

The City conducts daily backups and monthly system tests.

Other Best Practices

5. Management of mobile devices. An agency should ensure that it has a platform to manage mobile devices. This system should include (1) enabling password management controls, (2) requiring two-factor authentication, (3) requiring use of a virtual private network, (4) encrypting all information stored on the mobile device, and (5) enabling "remote wipe" so that when a device is lost, its data can be deleted remotely.

Mill Valley does not currently have a platform to manage mobile devices. This measure would strengthen security, but it may be expensive and require staff resources beyond the City's current capacity. Staff will assess the feasibility of implementing these recommendations.

6. Automated malware detection and removal. Antivirus software on the servers and personal computers can detect and remove malware before it does any damage.

The City has malware detection and removal on all City servers and personal computers.

7. Monitoring systems. Despite best efforts, most systems will end up being penetrated. It is important to have a monitoring system enabling the manager to see what is happening on the system and be alerted immediately when hackers have gained access.

The City has malware/virus protection on all workstations.

8. Use of expert resources. Cyber threats are constantly evolving, and it is difficult for the average IT professional to stay current. It is critical to have access to an expert outside resource, especially when performing vulnerability assessments. Free resources such as the

MS-ISAC alerts and newsletters can keep city and town managers (or their outside consultants) aware of new threats and risk-reduction techniques.

The City contracts with a Managed IT Services provider to assist the City with information security. However, they do not get MS-ISAC alerts to make staff aware of new threats and risk-reduction techniques. This is an inexpensive measure that would strengthen security, and the City will initiate implementation in the upcoming 20/21 Fiscal Year.

9. Firewalls. A firewall is a hardware device or software element that can block and filter outside access to a network. Firewalls should be up to date and deployed with security settings that are as strong as feasible, blocking, for example, all access from outside the United States.

The City has firewalls and they are up to date. However, they do not block foreign IP addresses. This measure would strengthen security, but it may be expensive and require staff resources beyond the City's current capacity. Staff will assess the feasibility of implementing these recommendations.

10. Hardware and patching. Many attacks happen because older computer operating systems are no longer supported and cannot be patched with up-to-date software. It is common to replace computers every three to four years to minimize this problem. Grand Jury interviews revealed that many cities and towns lack any policy on how frequently they replace their equipment.

The City does have older hardware that cannot be patched and is at greater risk. The City's Managed IT Services contractor regularly notifies the City of these risks and advises replacement. This measure would strengthen security, but it may be expensive and require staff resources beyond the City's current capacity. Staff will assess the feasibility of implementing these recommendations.

11. Documentation. All security measures and policies should be adequately documented and disseminated to ensure that (1) the policies and procedures are understood and capable of being followed, (2) users understand the expectations placed on them, and (3) when employee turnover occurs, critical information about information security is not lost.

The City does not currently have security measures and policies, and does not currently conduct documentation. This measure would strengthen security, but it may be expensive and require staff resources beyond the City's current capacity. Staff will assess

the feasibility of implementing these recommendations.

12. Vulnerability assessments. For organizations that can afford this extra step, a vulnerability assessment involves inventorying all systems, hardware, and software and assessing the points of vulnerability. A vulnerability report typically includes a list of recommended modifications. These assessments are usually performed every few years. Assessments can also include a "probe" element, where a deliberate attempt to gain unauthorized access to a system is made in order to educate users about vulnerabilities.

The City does not currently conduct vulnerability assessments. This measure would strengthen security, but it may be expensive and require staff resources beyond the City's current capacity. Staff will assess the feasibility of implementing these recommendations.

Other Recommendations in the Report

13. City staff should report, at least annually, regarding the City's cybersecurity profile and any measures being taken to improve it.

This report satisfies this recommendation.

14. The City should convene annual discussions, in a public forum such as a council meeting, regarding the importance of good cybersecurity practices for our government, residents, and other organizations.

By bringing this item to Council in July 2020, the City is initiating the first annual public meeting item on cybersecurity.

15. Adopt a policy to report to federal law enforcement any cybersecurity intrusion that results in financial fraud or unauthorized disclosure of information and make that intrusion public.

The City does not have a policy to report to federal law enforcement cybersecurity intrusion. City staff will develop a policy in Fiscal Year 20/21.

16. Complete an analysis of the feasibility of contracting with a cybersecurity expert to be available to cities and towns on a shared basis, in order to raise the overall level of cybersecurity in Marin's cities and towns.

The City does not have an analysis of the feasibility of contracting with a cybersecurity expert. The Mill Valley City Manager is a member of the Marin Managers

Association and will add the consideration of hiring cybersecurity firm to the list of potential shared services that is currently in development.