RESPONSE TO GRAND JURY REPORT FORM

Report Title: **Cyberattacks: A Growing Threat to Marin Government**

Report Date: **May 11, 2020**

Response By: **Sausalito City Council**

Title: **Mayor and City Council**

FINDINGS:

- We agree with the findings numbered **F7 and F10**
- We disagree wholly or partially with the findings numbered **F3, F4, F5, F6, F8, and F9**

RECOMMENDATIONS:

- Recommendations numbered **R7, R8** have been implemented.
- Recommendations numbered **R4, R5, R6, R9** have not yet been implemented, but will be implemented in the future.
- Recommendations numbered **N/A** requires further analysis.
- Recommendations numbered **N/A** will not be implemented because they are not warranted or are not reasonable.

DATED: 7/11/2020

Signed: DocuSigned by: CF095EA91C8340C...
Susan Cleveland-Knowles, Mayor

ATTEST: DocuSigned by: 919A8B149866467...
Heidi Scoble, City Clerk

Number of pages attached: 4

ATTACHMENT A: RESPONSE OF THE CITY OF SAUSALITO TO GRAND JURY REPORT "CYBERATTACKS: A GROWING THREAT TO MARIN GOVERNMENT"

FINDINGS AND RESPONSES

The responses below have been made from the perspective of the City of Sausalito'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: Disagree

The Sausalito City Council has and continues to support, through its annual budget and managed IT services that address cybersecurity measures. In particular and as referenced in the Report on page 7, in January 2018, when Sausalito was the victim of a phishing attack in which a fake emails, purporting to be from the City Manager, was sent to a city employee, the city employee provided confidential tax filing information of all city employees and councilmembers. The City began to initiate procedures to notify both the FBI and the victims of the breach. As also referenced in the Report on page 8, Sausalito informed the persons whose information was compromised, provided identity theft protection resources to all employees, held a City Council discussion on cybersecurity on November 27, 2018 whereby the City's cybersecurity consultant, Maze and Associates, provided a presentation to the public (refer to Agenda Item 1.A of that can be found at the following link: https://docs.google.com/gview?url=https%3A%2F%2Fgranicus_production_attachments.s3.amazonaws.com%2Fsausalito%2Fca54136fa4c860d8348f5eaeff9f882a0.pdf&embedded=tru), and implemented a number of measures to strengthen its security, including mandatory training, technology for flagging external emails, and on-going monitoring of its system by a cybersecurity consultant.

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

As referenced in the Report, Sausalito has regularly made the maintenance and upgrade of cybersecurity practices a part of the City's annual goals and objectives. Over the past several years, the City Council and City Staff have receive periodic updates on the status of the City's cybersecurity programs.

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 Sausalito 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 of Sausalito maintains Department of Justice compliant network connectivity to serve our Police Department and have a process for reporting breaches to federal authorities.

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

The City of Sausalito agrees that more can be done to share cybersecurity best practices. While the strategy and approach to cybersecurity in Marin cities and towns have not been standardized amongst all jurisdictions, most of the cities and towns utilizing the MIDAS network share the network security protocols in place for MIDAS and a number of cities and towns have relied on a common service provider to implement local network security solutions through Marin IT.

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: Disagree partially

While the Marin County Council of Mayors & Councilmembers have not made cybersecurity a focus over other pressing regional issues, the Sausalito City Council has made cybersecurity a priority. Since Sausalito's phishing breach, the City Manager and councilmembers have been briefed on the status of our security program, long-term projects, and actions-to-date related to the security of the City's network.

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

Response: Disagree

In 2019, the City of San Rafael made a presentation to the Marin Managers Association about a recent overhaul of our IT service delivery model (including cybersecurity). The San Rafael presentation included a consultant that was hired to conduct an assessment of San Rafael's service model and the president of the company who manages our cybersecurity.

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

Agree.

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: This recommendation is to be implemented.

The Sausalito Information Technology Division has provided periodic reports to the City Manager and the Councilmembers on current cybersecurity risk and threat assessments and actions underway by City staff to combat these threats in November 2018 and continues to contract with a cybersecurity consultant. The City's Information Technology Division will coordinate with the Sausalito City Manager to provide an annual update on the City's cybersecurity profile and any measures that would be necessary to improve cybersecurity.

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: This recommendation is to be implemented.

The City of Sausalito will commit to providing an opportunity to convene a public discussion concurrently with the annual cybersecurity profile report and update that will be scheduled for Fiscal Year 2020-2021

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 is to be implemented.

The City of Sausalito will commit to developing a policy in Fiscal Year 2020/2021. The policy will be presented to the City Council and the public concurrently with the cybersecurity profile and public forum.

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 mandatory user training, email flagging and filtering, password management, and backup.

Response: This recommendation has been implemented.

The City of Sausalito currently follows the first four practices described in this report. Specifically, Sausalito has implemented employee training, email flagging and filtering, password management, and data and system backups.

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: This recommendation has been implemented.

The City has implemented the following other best practices: (1) Automated malware detection and removal; (2) Use of expert resources; (3) Firewalls; (4) Hardware and patching; (5) Documentation; and (6) Vulnerability assessments.

The City has not implemented Management of Mobile Devices and Monitoring Systems. The aforementioned measures require more funding than is currently available, however the City is committed to implementing as many of the best practices as is financially feasible.

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 is to be implemented.

The Sausalito 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. It is probably more feasible to share staff resources in-house than contracting with a cybersecurity expert.