

RESPONSE TO GRAND JURY REPORT FORM

Report Title: Cyberattacks: A Growing Threat to Marin Government

Report Date: May 11, 2020

Response By: San Rafael City Council

Title: Mayor and City Council

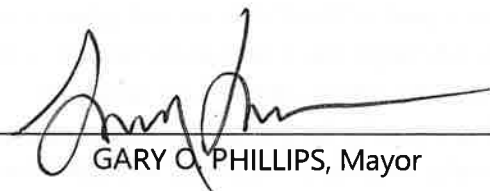
FINDINGS:

- We agree with the findings numbered F3, F7, F8, and F10
- We disagree wholly or partially with the findings numbered F4, F5, F6, and F9
(See Attachment A)

RECOMMENDATIONS:

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

DATED: 7/14/20

Signed: 
GARY O. PHILLIPS, Mayor

ATTEST: B. Nurmi

for Lindsay Lara, City Clerk

Number of pages attached: 4

**ATTACHMENT A: RESPONSE OF THE CITY OF SAN RAFAEL 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 San Rafael'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

The City of San Rafael has not experienced a security breach that would require public disclosure. We will develop a mechanism and policy that clarifies public reporting of breaches, should one occur.

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 San Rafael City Council 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 Mayor and City Manager have received periodic updates on the status of the City's cybersecurity goals and programs. These updates include past, ongoing, in-progress, and upcoming efforts regarding security for network infrastructure, desktop, mobile devices, users, internal processes, and disaster recovery. They also include information about known attempted ransomware attacks.

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 San Rafael 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 San Rafael maintains Department of Justice compliant network connectivity to serve our Police Department and has 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

We agree 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. The City of San Rafael will work with the recently formed Marin Information Security Collaboration (MISC) between Marin County regional agencies to develop and share best practices for cybersecurity.

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

While the Marin County Council of Mayors & Councilmembers (MCCMC) have not made cybersecurity a major focus over other pressing regional issues, the San Rafael City Council has made cybersecurity a priority through the City's annual goals. We are not aware of all topics (including cybersecurity) that may have been considered by MCCMC subcommittees. For the past several years, the City Manager and Mayor 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 December 2019, the City of San Rafael made an hour-and-a-half presentation to the Marin Managers Association's Strategic Retreat about a recent overhaul of our IT service delivery model (including cybersecurity). Our presentation included a consultant we hired to conduct an assessment of our 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.

Response: Agree

While the City of San Rafael has implemented or is in progress of implementing many low-cost best practices already, we recognize this finding to be generally true.

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 has been implemented.

Historically, the City of San Rafael's Information Technology Division, now the Digital Service and Open Government Department, has provided periodic reports to the City Manager and the Mayor on current cybersecurity risk and threat assessments and actions underway by City staff to combat these threats. City staff will continue to provide these reports at the request of the Mayor and City Manager on a periodic basis.

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 has not yet been implemented, but will be implemented in the future.

City of San Rafael employees, elected officials, and anyone with access to the City network are required to participate in regular cybersecurity training and receive email updates to current and trending security threats. The City periodically sends out public communications about known scams and prevention measures. The City will continue to explore additional means for educating the public about cybersecurity and work with the County of Marin to promote countywide public awareness campaigns.

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.

The City of San Rafael has not had any recent cybersecurity breaches, financial fraud, or unauthorized disclosure of information that have required the reporting to federal law enforcement. If the City of San Rafael were to become victim to any of the above attacks staff would work closely with all law enforcement personnel, including federal law enforcement, as required to properly respond to the threat. While we have a process for reporting breaches, we will develop a policy consistent with the above recommendation.

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 for updates to the City of San Rafael'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 mandatory user training, email flagging and filtering, password management, and backup.

Response: This recommendation has been implemented.

The City of San Rafael currently follows the first four practices described in this report. Network security is currently managed by the City's managed service provider, Xantrion Inc., who monitors and responds to threats, provides network backups, and manages cybersecurity training. Staff is required to participate in annual security training including email updates on current threats, phishing simulations, regular password changes. We also have measures in place for email flagging, spam filtering, and regular backups of City files and servers. Mobile

device management has been implemented in our Police Department and we are currently working to expand mobile device security and management throughout the organization. We have started requiring multi-factor authentication for City staff who have access to City networks and documents, and plan to have this rolled out to all users by the end of the summer.

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 of San Rafael is committed to protecting information and data from external threats. We have conducted a security analysis of the City of San Rafael network and systems and our Managed Service Provider Xantrion is working to implement recommendations on an ongoing basis. Some measures require more funding than is currently available however we are 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 has not yet been implemented, but will be implemented in the future.

The City of San Rafael currently contracts with cybersecurity experts who assist in the management of training, backup, and response. The City Manager will work with the Marin Managers Association to discuss shared resources and recommendations based on the success of our program and the consideration of shared cybersecurity services.

2020 JUL 20 P 4: 02

MARIN COUNTY
COUNSEL'S OFFICE