Attachment A

COUNTY OF SANTA BARBARA

BOARD OF SUPERVISORS
County Administration Building
105 East Anapamu Street
Santa Barbara, CA 93101
Telephone: (805) 568-2190
www.countyofsb.org

June, 2, 2020

Honorable Michael J. Carrozzo
Presiding Judge
Santa Barbara Superior Court
County Courthouse
1100 Anacapa Street
Santa Barbara CA 93101

Reference: Response to Santa Barbara Civil Grand Jury report titled, "Cyber-Attacks Threaten Santa Barbara County" published March 2020.

Judge Carrozzo:

Please find attached the Santa Barbara County Board of Supervisors (Board) response to the above referenced Civil Grand Jury Report. As directed by the Grand Jury, all responses are provided in accordance with Section 933.05 of the California Penal Code.

The Board appreciates the work conducted by the Risk Management Division of the County Executive Office and Information Technology and Communications Division of General Services for their assistance in responding to this matter.

Sincerely,

Gregg Hart, Chair
Santa Barbara County Board of Supervisors

CC: Santa Barbara County Board of Supervisors

Attachment

Santa Barbara County Board of Supervisors
Response to the Santa Barbara County Grand Jury 2018-2019 Report
"Cyber-Attacks Threaten Santa Barbara County"

Finding 1

Ensuring critical cyber security tasks and activities are properly executed on a timely basis requires a designated individual to be accountable and responsible.

The Board of Supervisors agrees with the finding.

Recommendation 1

That each public entity within Santa Barbara County designate an individual to be accountable and responsible to oversee cyber security.

The County has implemented this recommendation for only the County of Santa Barbara. The County does not have jurisdiction over other public agencies in the County on this matter. In 2018, the County hired its first Chief Information Security Officer (CISO) who is assigned to the Risk Management Division of the County Executive Office. The position is responsible for the professional guidance, advice, and assistance with the development and implementation of County policies and procedures aimed at ensuring the integrity of County data systems and private data that County departments must adhere to.

Finding 2

Most public entities within Santa Barbara County have an inadequate understanding of what communication and electronic systems they use and what data they maintain, and do not fully understand the risks, security issues and costs associated with the destruction of systems or loss of data.

The Board of Supervisors agrees with the finding.

Recommendation 2

That each public entity within Santa Barbara County complete a full inventory of their data, electronic and communication systems and determine the related security risks.

The County has implemented this recommendation for only the County of Santa Barbara. The County does not have jurisdiction over other public agencies in the County on this matter. In November of 2019, the County's General Services Department received a full Information Technology Inventory from WTC Consulting in an effort to fully document all data, electronic and communication systems and resources. Additionally, to determine the related security risks, the County has contracted to have a security audit completed in the next fiscal year.

Finding 3
Some public entities within Santa Barbara County do not have a written cyber security plan.

The Board of Supervisors agrees with the finding.

Recommendation 3
That each public entity within Santa Barbara County establish a written cyber security plan.

The recommendation has not yet been implemented, but will be implemented in the future for the County of Santa Barbara. The County does not have jurisdiction over other public agencies in the County on this matter. The County is in the process of implementing this recommendation. Beginning in December of 2019, the County secured 3rd party consulting firm Insight Security (formally PCMG) to conduct a full-scale IT Security Audit that as a promised deliverable will produce documented cyber security plans and scorecards specific to each department. The audit is expected to run 60 weeks.

Finding 4
Nationally, cyber-attacks on governmental organizations have been successful for many years and are occurring with more frequency and sophistication.

The Board of Supervisors agrees with the finding.

Recommendation 4
That each public entity within Santa Barbara County take substantial steps to protect data from internal and external attacks or threats.

The recommendation has not yet been implemented, but will be implemented in the future for the County of Santa Barbara. The County does not have jurisdiction over other public agencies in the County on this matter. Beginning in December of 2019, the County secured 3rd party consulting firm Insight Security (formally PCMG) to conduct a full-scale IT Security Audit that as a promised deliverable will produce documented cyber security plans and scorecards specific to each department. The audit is expected to run 60 weeks.

Finding 5
Cyber-attackers use a number of methods to install malicious software on systems including access through backdoors, staff or employee carelessness, and known bugs in software.

The Board of Supervisors agrees with the finding.

Recommendation 5a
That each public entity within Santa Barbara County install and maintain current antivirus software to detect malware and other threats.

The County has implemented this recommendation for the County of Santa Barbara. The County does not have jurisdiction over other public agencies in the County on this matter.

Recommendation 5b

That each public entity within Santa Barbara County install and update all operating software regularly.

The recommendation will not be implemented because it is not warranted or is not reasonable. The County agrees that it is critical to install and update all operating software regularly. However, in certain use cases there are State regulated systems and/or hardware compatibility issues that limit the County's ability to upgrade to the most current versions of operating software. The County maintains a complete inventory of all operating systems and applications and, where legacy issues exist, is working to address the update requirements with all respective parties. If possible, risk mitigating security controls will be implemented to reduce vulnerabilities associated with legacy software.

Recommendation 5c

That each public entity within Santa Barbara County periodically train employees and then test their cyber security awareness.

The County has implemented this recommendation for the County of Santa Barbara. The County does not have jurisdiction over other public agencies in the County on this matter. All County employees are required to undertake cybersecurity training upon entering County service and on a regular basis thereafter.

Recommendation 5d

That each public entity within Santa Barbara County periodically ensure electronic system-related contractors have been trained for cyber security awareness.

The County has implemented this recommendation for the County of Santa Barbara. The County does not have jurisdiction over other public agencies in the County on this matter.

Finding 6

If data is lost or compromised for any reason, including cyber-attack, mechanical failure or error, the most cost effective and expedient way to recover is to have current data backups and a plan to reinstall it.

The Board of Supervisors agrees with the finding.

Recommendation 6a

That each public entity within Santa Barbara County create and implement a full backup and recovery plan.

The County has implemented this recommendation for the County of Santa Barbara. The County does not have jurisdiction over other public agencies in the County on this matter. The County maintains offsite backup and recovery capabilities. Two (2) data centers backup data from each other and are geographically separated. These locations are separated by (60) miles and are serviced by two independent electrical utility providers (PG&E in the north and SCE in the south).

Recommendation 6b

That each public entity within Santa Barbara County regularly update and test their backup and recovery plan.

The recommendation has not yet been implemented, but will be implemented in the future for the County of Santa Barbara. The County does not have jurisdiction over other public agencies in the County on this matter. Beginning in December of 2019, the County secured 3rd party consulting firm Insight Security (formally PCMG) to conduct a full-scale IT Security Audit that as a promised deliverable will produce documented go-forward best practices for a more modernized data center/disaster recovery strategy for the County. The audit is expected to run 60 weeks.

Finding 7

Some public entities within Santa Barbara County do not have any, or adequate, cyber insurance.

The Board of Supervisors disagrees with the finding as it pertains to the County. The County maintains cyber insurance at generally acceptable risk levels of coverage. The Board of Supervisors cannot comment on the adequacy of cyber insurance for independent cities, districts and other municipalities within the County that are not under the jurisdiction of the Board.

Recommendation 7

That each public entity within Santa Barbara County secure adequate cyber insurance.

The County has already implemented this recommendation for the County of Santa Barbara. The County maintains cyber insurance at generally acceptable risk levels of coverage. The Board of Supervisors cannot comment on the adequacy of cyber insurance for independent cities, districts and other municipalities within the County that are not under the jurisdiction of the Board.

Finding 8

A cost-effective method to address cyber risks and concerns is to form an information sharing and learning consortium.

The Board of Supervisors agrees with the finding.

Recommendation 8

That each public entity within Santa Barbara County that is unable to allocate adequate funds for cyber security develop a cybersecurity working group to establish best practices and share costs for education, expertise, and insurance.

The recommendation has not yet been implemented, but will be implemented in the future for the County of Santa Barbara. Beginning in December of 2019, the County secured 3rd party consulting firm Insight Security (formally PCMG) to conduct a full-scale IT Security Audit that as a promised deliverable will produce documented go-forward strategy to develop a unified cyber security model that includes security participation across the county. The audit is expected to run 60 weeks.