CYBERSECURITY FOR SPECIAL DISTRICTS AND COUNTY SERVICE AREAS IN SANTA BARBARA COUNTY

SUMMARY

The 2021 Santa Barbara County Grand Jury (Jury) has prepared a report on the subject of cybersecurity for special districts and county service areas following the 2019-20 Santa Barbara County Grand Jury report titled "Cyber-Attacks Threaten Santa Barbara County," which focused on the broader County issues. This report encourages the 53 special districts in Santa Barbara County (County) to review their cyber-systems in order to identify cybersecurity threats. This Jury urges the special districts and service areas to take all necessary measures to protect their operational data and computer systems. This Jury has proposed a list of best practices for Santa Barbara County special districts to consider identifying, protecting, and, if necessary, upgrading their cybersecurity activities to advance the best interests of their consumers.

INTRODUCTION

> "With but a few lines of well-crafted code, a mobile phone or laptop computer can be convinced to betray its owner's most closely guarded secrets - and continue betraying them for months and even years. The machines are perfect spies. They do not require money or validation or love. Their motives are beyond question, for they have none of their own. They are reliable, dependable, and willing to work extraordinarily long hours. They do not become depressed or drink too much. They do not have spouses who berate them or children who disappoint them. They do not become lonely or frightened. They do not burn out. Obsolescence is their only weakness. More often than not they are discarded merely because something better comes along." Daniel Silva, *The Rembrandt Affair*

There are three types of special districts within Santa Barbara County. One is an Independent Special District, another is a Dependent Special District, and the third is a County Service Area. An Independent Special District has its own board of directors, either elected directly or appointed; they make their decisions on activities and budgets independent of any city or county oversight. A Dependent Special District is actually run by its respective city council or county board of supervisors. County Service Areas (CSA) are different from "Special Districts" in that they are also governed by the County Service Area Law (Cal. Govt. Code §§ 25210 et seq)[1] in addition to Cortese-Knox-Hertzberg Local Government Reorganization Act of 2000.[2] There are currently 39 Independent Special Districts, eight Dependent Special Districts, and six Community Service Areas within the County. (See Appendix I, II & III)

Recent press accounts report cybersecurity breaches across the United States.[3] Restoration of these services often requires the payment of ransom and reconstruction costs. The two-day

[1] California Government Code Section 25210.3 (2016)
[2] www.sbcounty.gov/uploads/LAFCO/Publications/CKH_2018.pdf
[3] https://thehill.com/policy/cybersecurity/576835-agencies-warn-of-cyber-threats-to-water-wastewater-systems

shutdown of a part of Colonial Pipeline's oil distribution system on the East Coast in early 2021, which reportedly cost the company more than $2 million dollars in ransom payments, is one example. Costly or potentially even deadly cyber-attacks also impacted, among many other business and government entities, police departments, water distribution systems, a major national meatpacking company, and hospital systems. Health care systems are particularly targeted. California had the highest percentage of attempted health-care system hacks, with 21 percent of the nationwide total.[4]

These intrusions can be very expensive to correct. Even when ransoms are paid, the breached or maliciously encrypted systems must be reconfigured or even rebuilt entirely. Moreover, there remain potential financial liabilities for critical infrastructure businesses like utilities, as well as financial institutions, to their customers. For example, Ally Bank (formerly known as GMAC) presently is the defendant in a class-action lawsuit in Federal Court in New York for its alleged negligence in allowing hackers to breach several of its customer accounts and steal names and passwords.[5]

Unfortunately, as the special district officials and consultants whom the Jury interviewed candidly admitted, no system is foolproof and precautions may vary greatly from district to district. It, therefore, is incumbent upon the special districts to take whatever proactive steps possible to reduce the threats and thereby mitigate the damaging consequences of the intrusions which inevitably will occur despite diligent efforts to prevent them.

METHODOLOGY

In an effort to assess the readiness of special districts in Santa Barbara County, the Jury interviewed a representative sampling of Santa Barbara County special districts and municipal officials, as well as private industry internet technology and cybersecurity experts. The Jury also reviewed many informative articles, reports, and official publications dealing with the subject of cybersecurity.

There are at least three U.S. agencies that address cybersecurity crime. Special districts are encouraged to access these and strengthen their own websites:

1. U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency (CISA) https://www.cisa.gov/
2. U.S. Department of Commerce, National Institute of Standards and Technology (NIST) https://www.nist.gov/cyberframework
3. U.S. Department of Justice, Federal Bureau of Investigation, Internet Crime Complaint Center (IC3) https://www.ic3.gov

OBSERVATIONS

While there appear to have been no known successful cyberattacks of special districts within Santa Barbara County, the Jury learned that an extensive number of cyber incursions have been

[4] https://www.comparitech.com/blog/information-security/ransomware-attacks-hospitals-data/
[5] *Medicis v. Ally Bank*, Case No.7:27-CV-06799 (U.S.D.C., So. Dist. N.Y., 2021

attempted in the United States, often with success. These intrusions severely disrupted governmental and private company operations, costing billions of dollars in ransom payments, system repairs, and additional defensive measures. Following a 2021 White House meeting[6] on the problem and in an effort to meet the challenge, Microsoft announced it is allocating $150 million for cybersecurity technical services to assist Federal, State, and local government agencies. In addition, it has committed to invest $20 billion over a period of five years to develop improved cybersecurity programs. Google has committed to spend $10 billion for that same purpose, and major corporations like Amazon and IBM will be greatly increasing their investment in employee training programs**.**

How Can Special Districts Protect Themselves?

The Jury has neither the staff nor the technical expertise to analyze the cyber-readiness of the special districts or to suggest specific defenses to cyberattacks. That work should be done by expert consultants and security firms devoted to such activities. The Jury offers a list of "Best Practices" based upon the sources consulted:

BEST PRACTICES

- Create "strong" passwords and change them often, or at least periodically
- Install and regularly update "encryption" software
- Install and regularly update "firewall" software (intrusion detection systems)
- Update computer systems as necessary
- Install and regularly update virus protection software
- Secure data by limiting access
- Safely dispose of all unwanted documents
- Limit remote internet access to the extent possible
- Limit physical access to system equipment (access cards, ID cards, etc.)
- Wipe data from equipment to be disposed of
- Monitor employee use of all systems
- Periodically test security measures and immediately remediate weaknesses
- Report to the appropriate internal security all malfunctions, anomalies or any other "out-of-ordinary" events no matter how insignificant they may appear to be
- Conduct training for all employees periodically on security policies and procedures, certify attendance, and teach staff how to prevent, detect, contain, and eliminate breaches
- Hire an outside security consulting firm to conduct a "risk analysis" at least annually and consider the possibility of pooling resources with other special districts to hire such expertise

[6] "Biden Presses CEO'S to Boost Cyber Security," *Wall Street Journal*, August 28, 2021, p.4A.

- Consider adequate cybersecurity insurance and the possibility of creating or joining an existing insurance pool to reduce premium cost
- Create and securely maintain back-up data separate from the "live" system
- Create a comprehensive Security Policy Manual to centralize information in one place and make it accessible to all staff
- Classify and prioritize all district hardware, software, devices, data, etc. in accordance with their critical nature
- Adopt easy to follow protocols for detecting and reporting known or suspected incursions and explain the exact duties and responsibilities of different staff levels in case an incident occurs. Create and maintain a current incident log designed to immediately document, analyze, and catalog incursions and explain how best to respond
- Immediately eliminate all access to data systems and emails upon an employee's departure

CONCLUSION

The Jury determined that it is important to keep this critical issue before the public; it now addresses this concern in more general terms to the County's many special districts and service areas. It is the Jury's hope that these agencies will become more fully aware of cyber-threats and will take all necessary measures to protect their confidential data.

Like all other government and business entities, special districts and service areas are vulnerable to cyber-attacks. Given its concern over the unfortunate increase in serious intrusions by criminal groups or individuals into data systems maintained by these governmental agencies and major publicly owned companies, the 2021 Santa Barbara County Grand Jury reminds all special districts in the County that they too potentially are targets for such criminal activity.

The Jury has suggested several "Best Practices" that those agencies should consider incorporating into their cyber-security programs. This would help protect them from unwanted intrusions, possible public disclosure of personal information, and having to pay ransoms. Although the Jury assumes that many districts have implemented many of these and other cyber-measures, some may not have done so, or have failed to test in a timely manner and upgrade existing protections to counter the increasingly sophisticated techniques employed by hackers.

Although the Jury did not interview representatives from all special districts, it is hoped they will review and adopt, as appropriate, the "Best Practices" listed in the report for their respective special districts. It is suggested that the districts take such remedial action as may be needed to safeguard their confidential personal, financial, and operational data against cyber-attacks to the greatest extent possible within their ability to do so.

FINDINGS and RECOMMENDATIONS

Finding 1

The Santa Barbara County Board of Supervisors has oversight over all dependent special districts and community service areas and their respective cybersecurity operations.

Recommendation 1

That the Santa Barbara County Board of Supervisors review and adopt, as appropriate, the "Best Practices" listed in the report for its dependent special districts and community service areas.

REQUEST FOR RESPONSE

Pursuant to *California Penal Code Section 933 and 933.05*, the Santa Barbara County Grand Jury requests each entity or individual named below to respond to the enumerated findings and recommendations within the specified statutory time limit:

Responses to Findings shall be either:

- Agree
- Disagree wholly
- Disagree partially with an explanation

Responses to Recommendations shall be one of the following:

- Has been implemented, with brief summary of implementation actions taken
- Will be implemented, with an implementation schedule
- Requires further analysis, with analysis completion date of no more than six months after the issuance of the report
- Will not be implemented, with an explanation of why

Santa Barbara County Board of Supervisors – 90 days

Findings: 1

Recommendation: 1

Note: A courtesy copy of this Report is being sent to all special districts within Santa Barbara County.

APPENDIX I

Independent Special Districts Within Santa Barbara County

- Cachuma Resource Conservation District
- Carpinteria Cemetery District
- Carpinteria Sanitary District
- Carpinteria/Summerland Fire Protection District
- Carpinteria Valley Water District
- Casmalia Community Services District
- Cuyama Basin Water District
- Cuyama Community Services District
- Cuyama Valley Recreation and Park District
- Embarcadero Municipal Improvement District
- Goleta Cemetery District
- Goleta Sanitary District
- Goleta Water District
- Goleta West Sanitary District
- Guadalupe Cemetery District
- Isla Vista Recreation and Park District
- Isla Vista Community Services District
- Lompoc Cemetery District
- Lompoc Valley Medical Center (Health Care District)
- Los Alamos Cemetery District
- Los Alamos Community Services District
- Los Olivos Community Services District
- Mission Hills Community Services District
- Montecito Fire Protection District
- Montecito Sanitary District
- Montecito Water District
- Oak Hill Cemetery District
- Mosquito and Vector Management District of Santa Barbara County
- San Antonio Basin Water District
- Santa Barbara County Fire Protection District
- Santa Maria Public Airport District
- Santa Maria Cemetery District
- Santa Maria Valley Water Conservation District
- Santa Rita Hills Community Services District
- Santa Ynez Community Services District
- Santa Ynez River Water Conservation District
- Santa Ynez River Water Conservation District, Improvement District #1
- Summerland Sanitary District
- Vandenberg Village Community Services District

APPENDIX II

Dependent Special Districts Within Santa Barbara County

- Guadalupe Lighting District
- Laguna County Sanitation District
- Mission Canyon Lighting District
- North County Lighting District Santa Barbara County Flood Control & Water Conservation District
- Santa Barbara County Water Agency
- Santa Barbara Metropolitan Transit District

APPENDIX III

County Service Areas Within Santa Barbara County

- County Service Area No. 3 (Goleta Valley)
- County Service Area No. 4 (North Lompoc)
- County Service Area No. 5 (Orcutt)
- County Service Area No. 11 (Carpinteria Valley)
- County Service Area No. 12 (Mission Canyon)
- County Service Area No. 31 (Isla Vista)
- County Service Area No. 32 (Unincorporated police services)
- County Service Area No. 41 (Rancho Santa Rita)