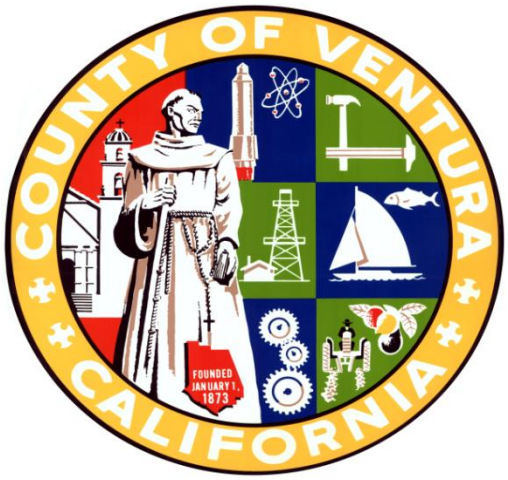
2019 - 2020
Ventura County Grand Jury



Final Report

Cybersecurity Strategies for Cities in Ventura County

April 17, 2020

This page intentionally blank

Cybersecurity Strategies for Cities in Ventura County

Summary

During 2019 targeted cyberattacks on local governments increased across the nation. Half resulted in ransomware demands. As the reports of these attacks on cities unfolded, it became clear that better preparation could have assisted those cities to avoid major and costly data breaches.

Due to the challenges of limited budgets, increasing cybersecurity attacks, the digital revolution and a competitive recruiting environment, cities would benefit from free or low–cost federal government backed assistance to defend against these challenges.

Within Ventura County (County) there are 10 incorporated cities (Cities). The 2019-2020 Ventura County Grand Jury (Grand Jury) investigated cybersecurity strategies of the Cities to assess the degree each City was prepared to defend against data breaches and ransomware and identify opportunities to implement improvements. The Grand Jury is mindful of the need not to disclose vulnerabilities of, or otherwise increase the potential for an attack on, an information technology system of a City. Therefore, this report does not detail any specific cybersecurity vulnerabilities that may have been discovered during the Grand Jury's investigation.

Since each City has varying circumstances, resources and readiness, the Grand Jury recognizes there is no perfect solution to cybersecurity or defense against cyberattacks. The Grand Jury recommends the following measures be adopted to bolster the Cities' cybersecurity and potentially decrease cybersecurity expenditures:

- Implement trustworthy website addresses
- Use free federal services for cyber risk assessments, cybersecurity evaluations, incident assistance coordination and cyber exercises/training
- Use cooperative group purchase programs
- Partner with local educational institutions and federal programs to recruit cybersecurity interns or graduating students
- Require cyber liability insurance of the Cities' IT vendors
- Develop and test cyber incident response, disaster recovery and business continuity plans
- Implement federal cybersecurity best practices
- Implement the California Cyber Security Integration Guidance for Teleworkers

While the Grand Jury investigation focused on the Cities, it suggests that similar strategies be considered by the County government and its agencies as well as independent districts. These include libraries, community colleges, county hospitals, schools and harbor, airport and water districts.

Background

Recent national and local news reporting alerted the Grand Jury to cities across the United States falling victim to hacking attacks with increasing frequency. Often attackers used malware to block access to a city's computer systems and demanded payment to unblock them. (Ref-01)

Cyberattacks

Attackers often target small organizations that have few resources to defend themselves. This can apply to cities, school districts, libraries, water districts, harbors and airports. (Ref-02, Ref-03) In 2019 at least 140 local government agencies nationwide were hit by ransomware. (Ref-04)

One published study reported more than 50 ransomware attacks against cities between January and June of 2019. Half of the victims were cities with fewer than 50,000 residents. (Ref-01) Cyberattacks against cities increased during the latter half of the year. In December alone malware attacks resulted in disruption of essential services in the cities of Pensacola, Florida; New Orleans, Louisiana; Galt, California; and St. Lucie, Florida. (Ref-05)

Nationally, 44% of local governments reported that they experienced cyberattacks on an hourly or daily basis. However, 28% of local governments did not know how often they were attacked, 41% did not know how often they were breached and 54% did not catalog or count attacks. (Ref-02)

Cities and attackers are in a never-ending game of cat and mouse as malware techniques constantly change to evade defenses.

- As local governments increasingly back-up electronic files to defend against ransomware, more attacks involve Trojan horse malware. Trojan horse malware lies dormant on networks and sets itself up to cause as much damage as possible when the attack is triggered. The latent attack often destroys the back-ups along with the targeted data, requiring IT personnel to rebuild their systems.
- For some attackers, the Trojan horse attack is used as a diversionary tactic. The malware enters a victim's network, remaining undetected for weeks, while secretly stealing data and information. Then, the malware launches a ransomware attack to distract incident response teams regarding the attackers other activities. (Ref-06)

Attackers are expanding their targets to include the managed service providers that many smaller communities use to supply their technology needs. (Ref-07)

In 2017 and 2018, an online bill payment services vendor for two Cities was compromised by an outside attacker using malware. As a result, credit card information was stolen and used for fraudulent charges. (Ref-08)

Some attackers target electronic devices directly, infecting USB drives during production. When users buy the infected products and plug them into their computers, malware is automatically installed.

If a person can physically access a computer, they may use their own USB drive to steal information directly from that computer. Another security risk related to the use of USB drives is they are easily lost or stolen. If the information on the drive was not encrypted, anyone in possession of the USB drive would have access to the data on it. (Ref-09)

Costs of Cyberattacks

Costs of cyberattacks to victimized cities arise in numerous ways: operational downtime to government services (e.g. police, emergency response, fire and tax collection), citizen frustration with lack of services and financial impact. (Ref-10)

With no options left for recovery, some victimized public entities resorted to paying the attackers. The largest known single payout in a ransomware attack in 2019 was by the city of Riviera Beach, Florida. Officials approved a $600,000 payment in Bitcoins to an attacker who seized control of its computers. (Ref-04)

In addition to ransom, there can be significant recovery costs. In just one example, Pensacola, Florida was hit with a ransomware attack in early December 2019. Although most of the data was quickly recovered, fearing a Trojan horse malware, city officials paid a professional services firm $140,000 to assess how the attack occurred, whether malware remained in the city's network and if data was compromised during the incident. (Ref-11)

As insurance companies for local governments pay ransom demands, attacker ransomware demand amounts are increasing. Higher insurance premiums are expected to follow. (Ref-12)

Local taxpayers are concerned. An IBM Security Study in 2019 found that a majority of polled taxpayers throughout the United States see ransomware as a threat to their personal data and their city's data. At the same time, nearly 60% of U.S. citizens surveyed are against their local governments using tax dollars to pay ransoms. (Ref-13)

Cyber Defenses

Appendix-04 to this report itemizes federal government recommendations for preventative measures to protect local government computer networks from falling victim to a malware infection. The Federal Government also recommends taking preventative measures for handling USB drives. (Ref-09)

Cyber Risk Management

Many local government agencies operate in a server environment. As they seek to improve government functions by using state-of-the-art platforms and tools such as cloud computing, mobile devices and big data initiatives, there can be increased exposure to attacks and additional public privacy risks. Local government leaders will need to balance the risks and rewards of adopting cloud, mobile and big data technologies. They also will need adequate cybersecurity defenses if they are attacked, keeping public services running and avoiding paying hefty ransom demands. (App-05)

With these issues in mind, the Grand Jury elected to focus on examining the cybersecurity readiness of the Cities as they increasingly digitize government services and functions. The circumstances and challenges for each City are unique, so the solutions will vary.

Methodology

The Grand Jury obtained information from the following sources:

- Internet research to gather relevant information from a variety of authoritative sources
- Interviews with local IT subject matter experts from September through November 2019
- Interviews with City officials and IT personnel within the County from October through November 2019
- Related documents provided by City officials

The Grand Jury's interview questions and document requests focused on the "Five Functions of the Cybersecurity Framework" (Cybersecurity Framework). This framework represents five key pillars of a successful and holistic cybersecurity program as developed by the U.S. Department of Commerce and used throughout the Federal government.

The Five Functions of the Cybersecurity Framework

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

(Ref-14)

The California Public Records Act Government Code Section 6254.19 protects from public disclosure a record that would reveal vulnerabilities to, or otherwise increase the potential for an attack on, an information technology system of a public agency. Therefore, the Grand Jury's report does not detail any specific cybersecurity vulnerabilities that may have been discovered during the Grand Jury's investigation. (Ref-15)

The Grand Jury appreciates the cooperation of local subject matter experts and City staff interviewed in the course of the investigation.

Facts

City Cybersecurity Awareness & Preparation in the County

FA-01. Attackers often target small organizations and cities that have few resources to defend themselves. (Ref-02, Ref-03)

FA-02. Cities are aware of the threat of cyberattacks and, to a varying degree, take active measures to reduce the risk in accordance with the Cybersecurity Framework. (Ref-14)

FA-03. On March 13, 2020, the California Cyber Security Integration Center issued a cybersecurity advisory titled Teleworking Quick Reference Guide. The guide highlights some security concerns and best practices end-users and network administrators should consider when implementing a teleworking program. (App-01)

FA-04. Not all Cities are implementing the teleworking best practices recommended by the California Cyber Security Integration Center. (Ref-16) (App-01)

FA-05. City managers and IT personnel provide ongoing cyber safety training and encourage personnel to take advantage of that training.

Collaboration within the County

FA-06. The Ventura County Executive Office created an informal network of City IT managers, thereby collectively elevating the level of the Cities' IT performance.

FA-07. City managers and IT personnel meet with their counterparts from other Cities on a regular basis to collaborate regarding cyberattacks.

City Web Addresses (URLs)

FA-08. The California Department of Technology and the National League of Cities recommend using .gov domain names and secure internet protocols. (App-01)

FA-09. Nine out of ten Cities use HTTPS (Hypertext Transfer Protocol Secure). Two out of ten Cities have .gov domain names. (App-03)

Cybersecurity Resources

FA-10. Cybersecurity and Infrastructure Agency

- The Department of Homeland Security (DHS) designated the Cybersecurity and Infrastructure Agency (CISA) to be the lead federal department to provide cybersecurity assistance to State, Local, Tribal and Territorial (SLTTs) government organizations. (App-02)
- CISA provides SLTTs with a "one-stop shop" of free services for cyber risk assessments, cybersecurity evaluations, incident assistance coordination, cyber exercises/training and recommended best practices. (App-02)

FA-11. Only one City uses any of the free CISA resources. That City uses only one of the available resources.

FA-12. Among its many services, CISA operates the Protective Security Advisor (PSA) Program. PSAs are DHS-trained critical infrastructure protection and vulnerability mitigation subject matter experts. Upon request, these experts provide free cybersecurity advice and assistance to SLTTs. (App-02)

FA-13. Nine of the 10 Cities maintain their cyber infrastructure through the use of internal staff and/or hiring vendors, in each case without taking advantage of CISA assistance.

FA-14. By using just one free CISA service, the remaining City saved at least $1,000 per month over five years. That City was not aware of the other available free CISA services.

FA-15. The DHS designated the nonprofit member driven Multi-State Information Sharing & Analysis Center (MS-ISAC) as its partner for sharing cybersecurity information with the SLTT governments. (App-02)

FA-16. MISAC also provides some fee-based cybersecurity services. (App-02)

FA-17. While all IT managers for the Cities are members of MISAC, less than half are members of MS-ISAC. Furthermore, only three Cities' IT personnel attended the MISAC 2019 Annual Conference. (Ref-17)

FA-18. Representatives from MS-ISAC provided information on available Federal cybersecurity resources at the 2019 MISAC conference. (Ref-18)

FA-19. More than 90 California cities hold memberships in MS-ISAC; two Cities in the County are members. (Ref-19)

FA-20. Of those Cities that use servers, hybrid cloud and cloud platforms, few take advantage of the cost-saving FedRAMP Moderate program to contract with cloud providers. (App-02)

Partnerships with Local Educational Institutions

FA-21. Some Cities partner with local educational institutions to develop internship opportunities and create a talent pool for cybersecurity or information technology. Those that do employ cybersecurity interns reported positive experiences and personnel cost savings.

FA-22. Three County higher educational institutions offer cybersecurity and internship programs:

- California Lutheran University (Ref-20)
- California State University Channel Islands (Ref-21, Ref-22)
- Moorpark College (Ref-23)

Information Technology Department Staffing

FA-23. Some Cities have difficulty recruiting and retaining IT staff. Salaries and benefits for City IT staff are not competitive with the private sector.

Cybersecurity Liability Insurance

FA-24. All Cities have cybersecurity liability insurance through the California Joint Powers Insurance Authority or other insurers.

FA-25. In addition to recommending cyber liability insurance for cities, the MISAC Security committee encourages MISAC members require their IT vendors have cyber liability insurance. (Ref-24)

City Budgets for Information Technology Services

FA-26. In reviews of budget documents, the Grand Jury found that five Cities have Information Services/Technology Departments line items in their adopted budgets. No City has a publicly viewable budget line item specifically for cybersecurity. (App-03)

FA-27. Two of the Cities anticipate spending over $5 million on information services in the upcoming budget year. (App-03)

Cyber Incident Response and Disaster Recovery Plans

FA-28. In 2018, a major provider of cybersecurity policies conducted a survey of public and private-sector respondents. In that survey 91% of respondents were confident their companies had implemented best practices to avoid a cyber event. Yet, 55% admitted not completing a cyber-risk assessment, 62% had not developed a business continuity plan and 63% had not completed a cyber-risk assessment on vendors who have access to their data. (Ref-25)

FA-29. Not all Cities have comprehensive cyber incident response, recovery and business continuity plans.

Vendor Management

FA-30. Business and Intellectual Property Attorney Lisa M. Thompson advised in August 2019 that cities should defend against cybersecurity threats by conducting risk management assessments on all third-party vendors that have access to confidential data and interact with municipal networks and systems. In addition, she stated that cities should require all vendors provide security documentation. (Ref-26)

FA-31. Most Cities do not manage the cyber risk of third-party vendors.

Conclusions

C-01. While the Grand Jury recognizes each City is taking steps to implement cybersecurity and to defend against cyberattacks, it concludes there is no perfect solution to cybersecurity or defense against cyberattacks. (FA-01, FA-02, FA-03, FA-04, FA-05, FA-06, FA-07)

C-02. The Grand Jury concluded eight Cities are currently using suboptimal web addresses for their websites. (FA-08, FA-09)

C-03. The Grand Jury concluded generally Cities are not utilizing free federal and discounted federally aligned resources available to Cities to bolster their cybersecurity defenses. (FA-10, FA-11, FA-12, FA-13, FA-14, FA-15, FA-16, FA-17, FA-18, FA-19, FA-20)

C-04. The Grand Jury concluded cybersecurity staffing could be improved with more effective recruiting and staff retention practices. (FA-21, FA-22, FA-23)

C-05. The Grand Jury concluded Cities should manage cyber risks associated with vendors by requiring they provide annual documentation regarding cybersecurity insurance and cybersecurity practices. (FA-24, FA-25, FA-30, FA-31)

C-06. The Grand Jury concluded some Cities do not clearly identify expenditures regarding information technology or cybersecurity in their budgets. (FA-26, FA-27)

C-07. The Grand Jury concluded all Cities would benefit from comprehensive cyber incident response, recovery and business continuity plans. (FA-28, FA-29)

C-08. The Grand Jury concluded some Cities are not following the recommended best practices for teleworking published by California Cyber Security Integration Center (FA-03, FA-04)

Recommendations

R-01. The Grand Jury recommends Cities establish secure web addresses through the use of HTTPS or other such protocols. (C-02)

R-02. The Grand Jury recommends Cities establish trustworthy web addresses by following the California Department of Technology domain name taxonomy guidance. (C-02)

R-03. The Grand Jury recommends Cities utilize free federal and federally aligned cybersecurity services as set forth in Appendix 02 to supplement internal staff and/or replace vendor services whenever possible. (C-03)

R-04. The Grand Jury recommends Cities' IT staff subscribe to CISA updates online. (C-03)

R-05. The Grand Jury recommends Cities take advantage of discounted services and cooperative purchasing programs whenever possible. (C-03)

R-06. The Grand Jury recommends Cities develop personnel cost-saving opportunities and create a cybersecurity talent pool by recruiting interns or graduating students using: (C-04)

- The Scholarships for Service program described in Appendix 02
- Local education institutions (high school, community college, private college and state university)

R-07. The Grand Jury recommends Cities maintain good vendor management by: (C-03, C-05)

- Obtaining CISA assistance to conduct risk management assessments on all third-party vendors that have access to any confidential data or that interact with City networks and systems
- Requiring all vendors provide cybersecurity documentation. As part of their ongoing third-party due diligence, Cities should evaluate vendors for compliance and risk on an annual basis
- Requiring IT vendors obtain cybersecurity insurance.

R-08. The Grand Jury recommends Cities clearly identify expenses for their Information Services (Technology) Departments in their approved budgets. (C-06)

R-09. The Grand Jury recommends Cities develop and test cyber incident response, recovery and business continuity plans. (C-07)

R-10. The Grand Jury recommends Cities implement the best practices for teleworking as published by the California Cyber Security Integration Center. (C-08)

R-11. The Grand Jury recommends Cities develop a written plan for implementation of R-01 through R-10 prior to December 31, 2020.

Responses

Responses Required From:

City Council, City of Camarillo (C-01, C-02, C-03, C-04, C-05, C-06, C-07, C-08) (R-01, R-02, R-03, R-04, R-05, R-06, R-07, R-08, R-09, R-10, R-11)

City Council, City of Fillmore (C-01, C-02, C-03, C-04, C-05, C-06, C-07, C-08) (R-01, R-02, R-03, R-04, R-05, R-06, R-07, R-08, R-09, R-10, R-11)

City Council, City of Moorpark (C-01, C-02, C-03, C-04, C-05, C-06, C-07, C-08) (R-01, R-02, R-03, R-04, R-05, R-06, R-07, R-08, R-09, R-10, R-11)

City Council, City of Ojai (C-01, C-02, C-03, C-04, C-05, C-06, C-07, C-08) (R-01, R-02, R-03, R-04, R-05, R-06, R-07, R-08, R-09, R-10, R-11)

City Council, City of Oxnard (C-01, C-02, C-03, C-04, C-05, C-06, C-07, C-08) (R-01, R-02, R-03, R-04, R-05, R-06, R-07, R-08, R-09, R-10, R-11)

City Council, City of Port Hueneme (C-01, C-02, C-03, C-04, C-05, C-06, C-07, C-08) (R-01, R-02, R-03, R-04, R-05, R-06, R-07, R-08, R-09, R-10, R-11)

City Council, City of Santa Paula (C-01, C-02, C-03, C-04, C-05, C-06, C-07, C-08) (R-01, R-02, R-03, R-04, R-05, R-06, R-07, R-08, R-09, R-10, R-11)

City Council, City of Simi Valley (C-01, C-02, C-03, C-04, C-05, C-06, C-07, C-08) (R-01, R-02, R-03, R-04, R-05, R-06, R-07, R-08, R-09, R-10, R-11)

City Council, City of Thousand Oaks (C-01, C-02, C-03, C-04, C-05, C-06, C-07, C-08) (R-01, R-02, R-03, R-04, R-05, R-06, R-07, R-08, R-09, R-10, R-11)

City Council, City of Ventura (C-01, C-02, C-03, C-04, C-05, C-06, C-07, C-08) (R-01, R-02, R-03, R-04, R-05, R-06, R-07, R-08, R-09, R-10, R-11)

References

Ref-01. Shi, Flemming. Threat Spotlight: Government Ransomware Attacks. Barracuda blog, August 28, 2019
https://blog.barracuda.com/2019/08/28/threat-spotlight-government-ransomware-attacks/
Accessed April 7, 2020

Ref-02. McGalliard, Tad. How Local Governments Can Prevent Cyberattacks. New York Times, March 30, 2018
https://www.nytimes.com/2018/03/30/opinion/local-government-cyberattack.html
Accessed April 7, 2020

Ref-03. Nelson, Sarah. Report: Local Gov Cyberattacks Reach Critical Level. Government Technology, December 18, 2019
https://www.govtech.com/security/Report-Local-Gov-Cyberattacks-Reach-Critical-Level.html
Accessed April 7, 2020

Ref-04. Kim, Allen. In the last 10 months, 140 local governments, police stations and hospitals have been held hostage by ransomware attacks. CNN, October 8, 2019
https://www.cnn.com/2019/10/08/business/ransomware-attacks-trnd/index.html
Accessed April 7, 2020

Ref-05. Patterson, Dan. Four U.S. cities attacked by ransomware this month. CBS News, December 17, 2019
https://www.cbsnews.com/news/ransomware-attack-pensacola-florida-4-u-s-cities-attacked-by-ransomware-this-month-2019-12-17/
Accessed April 15, 2020

Ref-06. Ng, Alfred. Ransomware froze more cities in 2019. Next year is a toss-up. CNET, December 5, 2019
https://www.cnet.com/news/ransomware-devastated-cities-in-2019-officials-hope-to-stop-a-repeat-in-2020/
Accessed April 15, 2020

Ref-07. Freed, Benjamin. Ransomware Attacks Map chronicles a growing threat. Statescoop, October 22, 2019
https://statescoop.com/ransomware-attacks-map-state-local-government/
Accessed April 15, 2020

Ref-08. Whitnall, Becca. City's online payment system falls victim to hackers. Thousand Oaks Acorn, November 8, 2018
https://www.toacorn.com/articles/citys-online-payment-system-falls-victim-to-hackers/
Accessed April 15, 2020

Ref-09. CISA. Security Tip (ST08-001) Using Caution with USB Drives. November 15, 2019
https://www.us-cert.gov/ncas/tips/ST08-001
Accessed April 15, 2020

Ref-10. Lohrmann, Dan. 2019: The Year Ransomware Targeted State & Local Governments. Government Technology, December 23, 2019
https://www.govtech.com/blogs/lohrmann-on-cybersecurity/2019-the-year-ransomware-targeted-state--local-governments.html
Accessed April 15, 2020

Ref-11. Ropek, Lucas. Pensacola Hires Deloitte to Investigate Extent of Cyberattack. Government Technology, December 19, 2019
https://www.govtech.com/security/Pensacola-Hires-Deloitte-to-Investigate-Extent-of-Cyberattack.html
Accessed April 15, 2020

Ref-12. Ikeda, Scott. Ransomware Attacks Are Causing Cyber Insurance Rates to Go Through the Roof; Premiums up as Much as 25 Percent. CPO Magazine, February 10, 2020
https://www.cpomagazine.com/cyber-security/ransomware-attacks-are-causing-cyber-insurance-rates-to-go-through-the-roof-premiums-up-as-much-as-25-percent/
Accessed April 15, 2020

Ref-13. IBM. IBM Security Study: Taxpayers Oppose Local Governments Paying Hackers in Ransomware Attacks. September 5, 2019
https://newsroom.ibm.com/2019-09-05-IBM-Security-Study-Taxpayers-Oppose-Local-Governments-Paying-Hackers-in-Ransomware-Attacks
Accessed April 15, 2020

Ref-14. U.S. Department of Commerce, National Institute of Standards and Technology. Cybersecurity Framework, The Five Functions
https://www.nist.gov/cyberframework/online-learning/five-functions
Accessed April 17, 2020

Ref-15. California Public Records Act Government Code Section 6254.19
http://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=6254.19&lawCode=GOV
Accessed April 17, 2020

Ref-16. California Cyber Security Integration Center. CYBERSECURITY ADVISORY Teleworking Quick Reference Guide. March 13, 2020
https://www.caloes.ca.gov/LawEnforcementSite/Documents/Cal-CSIC_Advisory_Teleworking%20Guidance.pdf
Accessed April 17, 2020

Ref-17. Registration List. 2019 MISAC Annual Conference
https://www.misac.org/events/RSVPlist.aspx?id=1243109
Accessed April 17, 2020

Ref-18. Vendors. 2019 MISAC Annual Conference
https://www.misac.org/page/VendorConfInfo2019
Accessed April 17, 2020

Ref-19. CIS. MS-ISAC Local Governments
https://www.cisecurity.org/partners-local-government/
Accessed April 17, 2020

Ref-20. California Lutheran University. Cal Lutheran starts cybersecurity program. September 20,2019
https://www.callutheran.edu/news/story.html?id=13865#story
Accessed April 17, 2020

Ref-21. California State University Channel Islands. Computer Science Program - BS Information Technology
https://compsci.csuci.edu/degrees/bsit.htm
Accessed April 17, 2020

Ref-22. California State University Channel Islands. Computer Science Program - Internships
https://compsci.csuci.edu/resources/internships.htm
Accessed April 17, 2020

Ref-23. Moorpark College. Computer Science Curriculum
https://www.moorparkcollege.edu/faculty-and-staff/curriculum-committee/course-outlines-of-record/computer-science-curriculum
Accessed April 17, 2020

Ref-24. MISAC. MISAC's New Security Committee Up and Running. July 6, 2018
https://www.misac.org/news/407088/MISACs-New-Security-Committee-Up-and-Running.htm
Accessed April 17, 2020

Ref-25. Newcome, Tod. Cyber Insurance Evolves to Meet the Ransomware Threat. Government Technology, October/November 2019
https://www.govtech.com/security/Cyberinsurance-Evolves-to-Meet-the-Ransomware-Threat.html
Accessed April 17, 2020

Ref-26. Thompson, Lisa. Cybersecurity Best Practices for Municipalities. New Hampshire Municipal Association, August 2019
https://www.nhmunicipal.org/town-city-article/cybersecurity-best-practices-municipalities
Accessed April 7, 2020

Glossary

TERM	DEFINITION
Attacker	Any individual or organization who attempts to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset.
Big Data	A field that treats ways to analyze, systematically extract information from or otherwise deal with data sets that are too large or complex to be dealt with by traditional data-processing application software.
Bitcoin(s)	A decentralized digital currency without a central bank or single administrator that can be sent from user to user on the peer-to-peer bitcoin network without the need for intermediaries.
CIS	Center for Internet Security
CISA	Cybersecurity and Infrastructure Security Agency
Cities	The 10 incorporated cities in the County
County	Ventura County
Cyberattack	Any type of offensive maneuver that targets computer information systems, infrastructures, computer networks, or personal computer devices.
Cybersecurity	The protection of computer systems and networks from the theft of or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide.
DHS	Department of Homeland Security
Encrypt	The process of encoding a message or information in such a way that only authorized parties can access it and those who are not authorized cannot.
FedRAMP	The Federal Risk and Authorization Management Program. A U.S. government-wide program that provides a standardized approach to security assessment, authorization and continuous monitoring for cloud products and services.
FedRAMP Moderate	The California administered FedRAMP

Grand Jury	2019-2020 Ventura County Grand Jury
HTTPS	Hypertext Transfer Protocol Secure
IT (Information Technology)	The use of computers to store, retrieve, transmit and manipulate data information. Typically used within the context of business operations as opposed to personal or entertainment technologies. All hardware, software and peripheral equipment operated by a limited group of users, as in "IT Department."
Malware	Any software intentionally designed to cause damage to a computer, server, client, or computer network. By contrast, software that causes unintentional harm due to some deficiency is typically described as a software bug. A wide variety of malware exists, including computer viruses, worms, Trojan horses, ransomware, spyware, adware, and scareware.
MISAC	The Municipal Information Systems Association of California
MS-ISAC	Multi State Information Sharing and Analysis Center
NIST	National Institute for Standards and Technology (U.S. Department of Commerce)
NSF	National Science Foundation (administers SFS)
Server	A computer that provides data to other computers.
SFS	CyberCorps Scholarships for Service
SLTT	State, Local, Tribal and Territorial Governments; includes special districts (e.g. Libraries, airports, water districts, harbors, etc.)
USB Drive	A data storage device that includes flash memory with an integrated USB interface. It is typically removable and rewritable.
URL	Colloquially termed a "web address," is a reference to a web resource that specifies its location on a computer network and a mechanism for retrieving it. A URL (Uniform Resource Locator) is a specific type of Uniform Resource Identifier (URI), although many people use the two terms interchangeably.

Appendices

App-01. A Compilation of Best Practices from Authoritative Sources

App-02. Cybersecurity Resources

App-03. City Budgets

App-04. Federal Government Cybersecurity Recommendations for SLTTs

App-05. State of the Art Platforms and Tools

Appendix 01

A Compilation of Best Practices from Authoritative Sources

A Compilation of Best Practices from Authoritative Sources	
Source	**Recommendation**
California Department of Technology Internet Domain Name Taxonomy Preparation instructions in the Statewide Information Management Manual – Section 40A https://cdt.ca.gov/wp-content/uploads/2017/05/SIMM-40A-Internet-Domain-Instructions.pdf	Each city government domain name should be "cityof" followed by the name of the city OR the name of the city followed by "city.ca.gov" OR in the case that there is no county with the same name, just the name of the city followed by ".ca.gov".
	Each county government domain name should be "countyof" followed by the name of the county OR the name of the county followed by "county.ca.gov" OR in the case that there is no city with the same name, the name of the county followed by ".ca.gov"
National League of Cities Protecting Our Data: WHAT CITIES SHOULD KNOW ABOUT CYBERSECURITY https://www.nlc.org/sites/default/files/2019-10/CS%20Cybersecurity%20Report%20Final.pdf	Convert to .gov domains in order to prevent impersonators of municipal services from targeting residents.
United States Senate DOTGOV Online Trust in Government Act of 2019 (S.2749) https://www.hsgac.senate.gov/media/minority-media/peters-johnson-klobuchar-and-lankford-introduce-bipartisan-bill-to-strengthen-cybersecurity-for-local-governments	The bill sponsors note that it can be difficult to identify a legitimate website when a government uses a .com, .org, or .us domain name. The sponsors note that when local governments don't use the .gov domain, it allows cybercriminals to more easily impersonate government officials in order to defraud the public and get people to share sensitive information.
	The bill helps the transition to a .gov domain name to be more affordable for local governments by making the change an allowable expense under DHS's Homeland Security Grant Program.
DHS – CISA https://www.cisa.gov/insights https://www.us-cert.gov/ncas/tips/ST18-006	Phishing emails and the use of unencrypted Hypertext Transfer Protocol (HTTP) remain persistent channels through which malicious actors can exploit vulnerabilities in an organization's cybersecurity posture. Attackers may spoof a domain to send a phishing email that looks like a legitimate email. At the same time, users transmitting data via unencrypted HTTP protocol, which does not protect data from interception or alteration, are vulnerable to eavesdropping, tracking and the modification of the data itself.
CISA – Cyber Essentials Infographic https://www.cisa.gov/sites/default/files/publications/19_1105_cisa_CISA-Cyber-Essentials.pdf	Cyber Essentials Infographic Guide for Leaders and IT Professionals.

CISA – Recommendations for Incident Response Plans, Recovery Plans and Business Continuity Plans https://www.cisa.gov/sites/default/files/publications/19_1106_cisa_CISA_Cyber_Essentials_S508C_0.pdf	• Develop an incident response and disaster recovery plan outlining roles and responsibilities. • Test the plan often. • Leverage business impact assessments to prioritize resources and identify which systems must be recovered first. • Learn who to call for help (outside partners, vendors, government/industry responders, technical advisors and law enforcement). • Develop an internal reporting structure to detect, communicate and contain attacks. Leverage in-house containment measures to limit the impact of cyber incidents when they occur.
California Cyber Security Integration Center Guidance for Teleworkers (3/13/20) https://www.caloes.ca.gov/LawEnforcementSite/Documents/Cal-CSIC_Advisory_Teleworking%20Guidance.pdf	Teleworking Quick Reference Guide. Teleworking requires additional network security and user considerations. This document highlights some of the security concerns and best practices end-users and network administrators should consider when implementing a teleworking program.
"Cybersecurity Best Practices for Municipalities", New Hampshire Municipal Association, by Lisa M. Thompson, August 2019 https://www.nhmunicipal.org/town-city-article/cybersecurity-best-practices-municipalities	City vendors should provide cybersecurity documentation to the cities. As part of their ongoing third-party due diligence, cities should evaluate vendors for compliance and risk on an annual basis.

This page intentionally left blank

Appendix 02

Cybersecurity Resources

Cybersecurity Resources	
Source	**Service**
CISA https://www.cisa.gov/sites/default/files/publications/2019-CSSS-CISA-Regional-Services-508.pdf, slides 10 and 15. CISA was established within Homeland Security in 2018 by the Cybersecurity and Infrastructure Security Agency Act of 2018 to coordinate efforts to address cybersecurity threats to critical infrastructure by working with private companies as well as state and local governments. https://www.cisa.gov/about-cisa	Provides SLTTs with a "one-stop shop" of free services for cyber risk assessments, cybersecurity evaluations, incident assistance coordination, cyber exercises/training, and best practices.
CISA – Assessments https://www.cisa.gov/about-cisa	CISA offers a range of free cybersecurity assessments that evaluate operational resilience, cybersecurity practices, organizational management of external dependencies, and other key elements of a robust cybersecurity framework. CISA's cybersecurity assessment services are offered solely on a voluntary basis and are available to SLTTs upon request.
CISA – Infrastructure Security Division Protective Security Advisor (PSA) Program https://www.dhs.gov/cisa/protective-security-advisors	PSAs are trained critical infrastructure protection and vulnerability mitigation subject matter experts who facilitate local field activities in coordination with other Department of Homeland Security offices. They advise and assist state, local and private sector officials and critical infrastructure facility owners and operators.
Local CISA Protective Security Advisor https://www.cisa.gov/sites/default/files/publications/PSA-Program-Fact-Sheet-05-15-508.pdf	The DHS has a free Protective Security Advisor in the Camarillo, California, Office of Homeland Security.

Cybersecurity Resources	
Source	**Service**
CISA – "Cyber Essentials" https://www.cisa.gov/sites/default/files/publications/19_1105_cisa_CISA-Cyber-Essentials.pdf	On November 6, 2019, CISA launched "Cyber Essentials" in an effort to equip small organizations with basic steps and resources to improve their cybersecurity.
CISA's Cyber Essentials https://www.cisa.gov/blog/2019/12/12/get-your-city-cyber-ready-cisas-cyber-essentials https://www.cisa.gov/sites/default/files/publications/19_1106_cisa_CISA_Cyber_Essentials_S508C_0.pdf	In a December 12, 2019 blog on the CISA website Bradford Willke wrote "CISA intends for this to be the first of many '*Cyber Essentials'* product releases. In the coming months, we will be developing a toolkit that provides users with additional detail on each Essential and links them to helpful resources for implementation. We will also continue to engage with partner organizations to get the word out about the 'Cyber Essentials' and collaborate with us in developing the toolkit."
The National League of Cities "What Cities Should Know About Cybersecurity" https://41g41s33vxdd2vc05w415s1e-wpengine.netdna-ssl.com/wp-content/uploads/2019/10/NLC_CybersecurityReport.pdf	The report is intended to be a guide to help local governments understand their cybersecurity vulnerabilities and how they can improve security practices.
CIS https://www.cisecurity.org/about-us/ https://www.cisa.gov/partnership-engagement-branch	A nonprofit, member driven organization formed in 2000. Its mission is to identify, develop, validate, promote, and sustain best practice solutions for cyber defense. CIS operates the MS-ISAC program which is designated by DHS as the cybersecurity Information Sharing and Analysis Center (ISAC) for SLTT governments to share information between government and industry.

Cybersecurity Resources	
Source	**Service**
MS-ISAC https://www.cisecurity.org/blog/cis-securesuite-membership-free-for-u-s-sltts-what-you-need-to-know/	In 2018 MS-ISAC's CIS SecureSuite membership became free to SLTT governments in the United States.
MISAC https://www.misac.org/	Founded in 1980, MISAC is comprised of public agency information technology professionals working throughout California. On its website MISAC states it promotes the understanding and strategic use of information technology within local government agencies through sharing of best practices. MISAC is a member based organization that serves as an advisor to the League of California Cities. It does not have a relationship with DHS.
MISAC – Security Committee https://www.misac.org/news/407088/MISACs-New-Security-Committee-Up-and-Running.htm	Promotes three best practices that municipalities can implement to stay on top of their organization's cybersecurity: 1. Cyber liability insurance 2. Cyber for Internet Security (CIS) Controls 3. Multi-State Information Sharing & Analysis Center (MS-ISAC) membership. Joining MS-ISAC is free to municipal government IT operations.
GovLaunch https://govlaunch.com/	A national free, private platform for any verified employees of local government to share details of their projects or initiatives. It is a website where local governments can find out what technology their peers are turning to and how they're using it.

Cybersecurity Resources	
Source	**Service**
FedVTE niccs.us-cert.gov/training/federal-virtual-training-environment-fedvte	FedVTE is a free, online, on-demand cybersecurity training system managed by DHS that is available to SLTT government personnel. It contains more than 800 hours of training on topics such as ethical hacking, surveillance, risk management and malware analysis. Resource benefits include: • Diverse courses – The program offers more than 300 demonstrations and 3,000 related materials, including online lectures and hands-on virtual labs. • Certification offerings – Offerings include Network +, Security +, Certified Information Systems Security Professional (CISSP), Windows Operating System Security and Certified Ethical Hacker. • Experienced instructors – All courses are taught by experienced cybersecurity subject matter experts.
CIS CyberMarket https://www.cisecurity.org/services/cis-cybermarket/	CIS's collaborative purchasing program that serves SLTT organizations, not-for-profit entities, and public health and education institutions to improve cybersecurity through cost-effective group procurement. The objective of the CIS CyberMarket is to combine the purchasing power of governmental and nonprofit sectors to help participants improve their cybersecurity environment at a lower cost than they would have been able to attain on their own.

Cybersecurity Resources	
Source	**Service**
General Services Administration Cooperative Purchasing Program https://www.gsa.gov/technology/technology-products-services/it-security https://www.gsa.gov/buying-selling/purchasing-programs/gsa-schedules/schedule-buyers/state-and-local-governments/cooperative-purchasing	Allows SLTTs to purchase IT and security products and services offered through GSA's negotiated contracts. The advantage for eligible users of the GSA Cooperative Purchasing Program is that vendor services and products can be procured at the lowest possible price with the assurance that contractors are qualified to sell to the federal government.
FedRAMP Moderate https://www.fedramp.gov/ https://cdt.ca.gov/wp-content/uploads/2019/01/2018-Annual-Report_FINAL_accessible.pdf, p. 12 https://cdt.ca.gov/wp-content/uploads/2019/09/TA_18-05.pdf	A U.S. government program that establishes a standardized approach for validating that cloud services are secure**.** FedRAMP offers independent, third-party validation of a cloud provider's security posture and a standardized approach to security assessments, authorization and continuous monitoring for cloud products and services. It is administered by the states. Available to all California cities and counties. This single state contract provides cloud services to government customers at discounted prices of up to 9.5%, with additional volume discounts available for select providers. Service providers include Amazon, Microsoft and IBM.
California's Cybersecurity Task Force https://www.caloes.ca.gov/cal-oes-divisions/cybersecurity-task-force/task-force-subcommittees	While not currently providing direct cybersecurity support to California's cities, this task force may be a future resource.

Cybersecurity Resources	
Source	**Service**
The National Science Foundation https://www.sfs.opm.gov/	Administers the Federal SFS program which is an effective recruiting tool for SLTTs. Upon graduation, scholarship recipients are required to work as cybersecurity professionals for a period equal to the length of their scholarship. The CyberCorps scholarship assists in funding the typical costs incurred by full-time students while attending a participating institution, including tuition and education and related fees. The scholarships are funded through grants awarded by the National Science Foundation in partnership with DHS and the Federal Office of Personnel Management (OPM). City hiring Managers and Human Resources Consultants interested in recruiting from the SFS program can gain access to this candidate pool by contacting the program office at sfs@opm.gov.

This page intentionally left blank

Appendix 03

City Budgets

City Budgets

City of Camarillo Adopted 2018-2020 [2 years] Budget
https://www.cityofcamarillo.org/Finance/Budget/City%20of%20Camarillo%202018%20-%202020%20Budget.pdf, p. 56

City of Fillmore, CA Adopted Operating Budget 2019-20
https://www.fillmoreca.com/home/showdocument?id=5431

City of Moorpark, CA Operating and Capital Improvement Projects Budget Fiscal Year 2019–2020
https://www.moorparkca.gov/DocumentCenter/View/9589/F-201920-Budget?bidId=, pp. 87-91

City of Ojai, CA Adopted Municipal Budget 2019–2020
https://ojaicity.org/the-adopted-municipal-budget-for-fiscal-year-2019-2020-now-online/, p. 35

City of Oxnard Adopted Budget Fiscal Year 2019-2020
https://www.oxnard.org/wp-content/uploads/2019/10/FINANCE_ADOPTED_Budget_Book_19_20.pdf, pp. 152–155

City of Port Hueneme FY 2019-21 Operating Budget
https://www.ci.port-hueneme.ca.us/DocumentCenter/View/2953/OperatingBudget-19-20-and-20-21?bidId=

City of Santa Paula 2019-2020 Fiscal Year Budget
https://spcity.org/209/Financial-Reports

City of Simi Valley FY2019-20 Adopted Budget
https://www.simivalley.org/home/showdocument?id=21214, pp. 97, 98

City of Thousand Oaks Adopted Operating Budget Fiscal Years 2019-2020 & 2020 – 2021
https://www.toaks.org/home/showdocument?id=22064

City of Ventura Adopted Budget
https://www.cityofventura.ca.gov/DocumentCenter/View/18416/FY-2019-20-Adopted-Budget?bidId=

Appendix 04

Federal Government
Cybersecurity Recommendations for SLTTs

Federal Government
Cybersecurity Recommendations for SLTTs

- Implement an awareness and training program emphasizing awareness of the threat of ransomware and how it is delivered. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and Domain Keys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions— with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.

Source: CISA, "Ransomware, What It Is and What To Do About It" https://www.us-cert.gov/sites/default/files/publications/Ransomware_Executive_One-Pager_and_Technical_Document-FINAL.pdf

Appendix 05

State of the Art Platforms and Tools

State of the Art Platforms and Tools		
Tool	**Risks**	**Rewards**
Mobile Devices	• Information breach from lost or stolen devices • Unclear data ownership due to both personal and private usage of devices • Additional endpoints to manage	• Increased accessibility to data anywhere and anytime • Consistent methodologies of data collection
Cloud Computing	• Compromised confidential data • An unauthorized user obtaining information • Insiders circumventing security and releasing private information	• Improved collaboration and continuity • Increased accessibility to information and resources • More opportunities for increased business agility
Big Data Initiatives	• Volumes of data expose organizations to more risks and threats • Challenging to stay ahead of attacks • Harder for agencies to be proactive in spotting big data vulnerabilities	• Identifies relationships, patterns and threats traditionally not seen • Real-time data can stop fraud and attacks faster than traditional data processing • Big data can increase secure operations and meet compliance requirements

Source: Government Technology
https://media2.govtech.com/images/symantecinfographicnewfinalsmall.jpg

This page intentionally left blank