Response to Grand Jury Report Form

Report Title: Cybersecurity Strategies for Cities in Ventura County

Report Date: October 19, 2020

Response By: Aaron Wedemeyer

Title: Information Systems and Technology Manager

FINDINGS

- I (we) agree with the findings / conclusions numbered: C 01-08 and FA 01-31
- I (we) disagree wholly or partially with the facts numbered:_____
  (Attach a statement specifying any portions of the Findings/Conclusions that are disputed; include an explanation of the reasons.)

RECOMMENDATIONS

- Recommendations numbered R-01, 03, 04, 05, 10 have been implemented.
  (Attach a summary describing the implemented actions and date completed.)

- Recommendations numbered R-09, 11 have not yet been implemented, but will be implemented in the future.
  (Attach a timeframe for the implementation.)

- Recommendations numbered R-02, 06, 07, 08 require further analysis.

- Recommendations numbered_____ will not be implemented because they are not warranted or are not reasonable.

Date: Oct. 25, 2020

Signed: Laura D. Hernandez

Laura D. Hernandez, Mayor
City of Port Hueneme

Number of pages attached: 3

Responses

Recommendation R-01. The Grand Jury recommends Cities establish secure web addresses through the use of HTTPS or other such protocols. (C-02)
Response to R-01: By default, the City of Port Hueneme uses HTTPS (Hypertext Transfer Protocol Secure) for all internal and external web sites. If an end user browses to an HTTP address, the communication is automatically switched to HTTPS, or terminated. This practice began in December, 2018.

Recommendation R-02. The Grand Jury recommends Cities establish trustworthy web addresses by following the California Department of Technology domain name taxonomy guidance. (C-02)
Response to R-02: During the establishment of the City's web presence in approximately 2002, the City followed what were the current naming conventions for government entities, and maintain that naming convention today. The use of California Department of Technology domain name taxonomy guidance seems to provide limited additional security for the public, and results in a significant amount of work to effect the change. Such a change would also negatively impact the existing public communication established over the years using the current naming convention. City will investigate costs and impacts associated with such a change and consider the establishment of a new internet presence if the City undergoes a rebranding/renaming effort during the 75th Anniversary celebration of the City's charter in 2022.

Recommendation 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)
Response to R-03: Port Hueneme has taken advantage of the external penetration testing services provided by CISA since December, 2019. The City has requested additional services to include targeted phishing exploits/training, but has not yet been provided that service. Staff recently joined MS_IASC, applying for IP and Domain-name filtering services. MS_IASC's offer of targeted phishing is being reviewed for implementation.

Recommendation R-04. The Grand Jury recommends Cities' IT staff subscribe to CISA updates online. (C-03)
Response to R-04: Port Hueneme IT have received weekly vulnerability updates from US-CERT since approximately 2015. In December, 2019 the City began utilizing services from CISA. The addition of IP and Domain filtering from MS_IASC in July, 2020 further increases the layers of protection utilized.

Recommendation R-05. The Grand Jury recommends Cities take advantage of discounted services and cooperative purchasing programs whenever possible. (C-03)
Response to R-05: The City of Port Hueneme leverages cooperative purchase agreements whenever possible. The City of Port Hueneme will review cooperative service offerings the next time services are needed to replace, upgrade, or supplement existing cybersecurity measures. The current major provider of network services has an established relationship and understanding of the network architecture, which is a valuable asset that must be considered in determining if change for the sole sake of saving initial purchase price is valid.

Recommendation 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)

Response to R-06: Utilizing temporary interns as the basis for a cybersecurity talent pool introduces a high level of potential risk on a critical system. This provides an unknown level of risk each time an intern leaves, as critical information and passwords leave the control of City staff. The level of work to ensure no unauthorized access can be attained needs to be carefully weighed against the value of personnel cost-saving opportunities from intern assistance. Staff currently administering changes to the City's network security have established career dedication to the City, and have extended experience with the current systems. The City must carefully review the following: Do cyber related non-critical tasks exist that could be assigned to an intern without jeopardizing city security; proper onboarding process (background investigation) and security measures that would need to be in place; level of access to be granted for such a position.

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

a. 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
b. 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
c. Requiring IT vendors obtain cybersecurity insurance.

Response to R-07:

a. Further analysis is required. The City has a concern that Cybersecurity and Infrastructure Agency (CISA) risk management assessments on all third-party vendors may adversely impact the timing of the award and project execution. A better understanding of the CISA risk management assessment process and response is required.
b. The City agrees we should require all vendors provide cybersecurity documentation and evaluate vendors for compliance on an annual basis. Financial audits typically include a requirement to provide such documentation on major systems that store Personally Identifiable Information (PII)
c. The City agrees we should require all IT vendors obtain cybersecurity insurance.

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

Response to R-08: Budget appropriations for the City's Information Technology function currently serve as the predominate portion of the City's *General Government* cost center. The City will undertake a project to restructure the City budget in a way that isolates IT costs from other city expenses. The City seeks to implement this change as part of the development of the next municipal budget, which is expected to be adopted prior to July 1, 2021. If it is determined that such a change impacts that City's existing Cost Allocation Plan (CAP), the project will be delayed until such time as the next CAP is performed. The City typically develops CAPs every two years, the most recent one having been completed in April 2020. As such it is anticipated that the next CAP will be conducted in the first half of calendar year 2022.

Recommendation R-09. The Grand Jury recommends Cities develop and test cyber incident response, recovery and business continuity plans. (C-07)
Response to R-09: The City is in the midst of selecting a candidate to perform an IT Master Plan. The City anticipates that direction and funding for Business Continuity planning will be a recommendation of the IT Master Plan. Timeline: The IT Master Plan completion is anticipated for May, 2021.

Recommendation R-10. The Grand Jury recommends Cities implement the best practices for teleworking as published by the California Cyber Security Integration Center. (C-08)
Response to R-10: City staff who need to telework are issued laptop resources. All laptops have been configured by IT department to assure anti-virus and operating system updates. Connection to internal network resources are accomplished with VPN software to encrypt traffic between endpoints. Personal devices are not approved for use in telework except in unique cases. These cases require the use of secure desktop sharing applications.
Security of City-provided cell phones has not been addressed. Cell phone are used for email connectivity only.

Recommendation R-11. The Grand Jury recommends Cities develop a written plan for implementation of R-01 through R-10 prior to December 31, 2020
Response to R-11: The City will develop formal written plans for each recommendation that requires further action. Timeline: prior to December 31, 2020.