SANTA CRUZ
COUNTY
GRAND JURY

Grand Jury <grandjury@scgrandjury.org>

ATTN: Civil Grand Jury Response (Cyber Threat Preparedness)

Emeline Nguyen <enguyen@santacruzca.gov> Tue, Aug 15, 2023 at 5:08 PM
To: "syda.cogliati@santacruzcourt.org" <syda.cogliati@santacruzcourt.org>, "grandjury@scgrandjury.org" <grandjury@scgrandjury.org>
Cc: Dean Kashino <dean.kashino@scgrandjury.org>, Fred Keeley <fkeeley@santacruzca.gov>, Matt Huffaker <mhuffaker@santacruzca.gov>, Laura Schmidt <LSchmidt@santacruzca.gov>, Ken Morgan <kmorgan@santacruzca.gov>

Good afternoon Honorable Judge Cogliati and Santa Cruz County Grand Jury,

On behalf of the City, I've attached the Civil Grand Jury Response relating to Cyber Threat Preparedness from the August 8th Council meeting for your review. Please let me know if you have any questions.

Thank you,

CITY OF
SANTA CRUZ

Emeline Nguyen

Principal Management Analyst

City of Santa Cruz | City Manager's Office

809 Center Street, Santa Cruz, CA 95060

Phone: 831-420-5017

Email: enguyen@santacruzca.gov
Web: www.cityofsantacruz.com

20230816_Civil Grand Jury_Cyber Threat Preparendess.pdf
226K

The 2022–2023 Santa Cruz County Civil Grand Jury

Requires the

Santa Cruz City Council

to Respond by August 16, 2023

to the Findings and Recommendations listed below which were assigned to them in the report titled

Cyber Threat Preparedness

Phishing and Passwords and Ransomware, Oh My!

Responses are **required** from elected officials, elected agency or department heads, and elected boards, councils, and committees which are investigated by the Grand Jury. You are required to respond and to make your response available to the public by the California Penal Code (PC) §933(c).

Your response will be considered **compliant** under PC §933.05 if it contains an appropriate comment on **all** findings and recommendations **which were assigned to you** in this report.

Please follow the instructions below when preparing your response.

Instructions for Respondents

Your assigned Findings and Recommendations are listed on the following pages with check boxes and an expandable space for summaries, timeframes, and explanations. Please follow these instructions, which paraphrase PC §933.05:

1. ***For the Findings, mark one of the following responses with an "X" and provide the required additional information:***
   a. **AGREE with the Finding**, or
   b. **PARTIALLY DISAGREE with the Finding** – specify the portion of the Finding that is disputed and include an explanation of the reasons why, or
   c. **DISAGREE with the Finding** – provide an explanation of the reasons why.

2. ***For the Recommendations, mark one of the following actions with an "X" and provide the required additional information:***
   a. **HAS BEEN IMPLEMENTED** – provide a summary of the action taken, or
   b. **HAS NOT YET BEEN IMPLEMENTED BUT WILL BE IN THE FUTURE** – provide a timeframe or expected date for completion, or
   c. **REQUIRES FURTHER ANALYSIS** – provide an explanation, scope, and parameters of an analysis to be completed within six months, or
   d. **WILL NOT BE IMPLEMENTED** – provide an explanation of why it is not warranted or not reasonable.

3. ***Please confirm the date on which you approved the assigned responses:***

   We approved these responses in a regular public meeting as shown in our minutes dated August 8, 2023**.**

4. ***When your responses are complete, please email your completed Response Packet as a PDF file attachment to both***

   The Honorable Judge Syda Cogliati Syda.Cogliati@santacruzcourt.org **and**

   The Santa Cruz County Grand Jury grandjury@scgrandjury.org.

If you have questions about this response form, please contact the Grand Jury by calling 831-454-2099 or by sending an email to grandjury@scgrandjury.org.

Findings

F4. The City of Santa Cruz seems to have an adequate IT Department structure; however, in late 2022, 40 percent of its positions remained vacant, leaving them inadequately staffed to mitigate and respond to cyber attacks.

X AGREE
__ **PARTIALLY DISAGREE**
__ **DISAGREE**

Response explanation (required for a response other than **Agree**):

F5. Inadequate staffing and high attrition has led to overworked staff and raises the risk of cyber vulnerabilities across its networks.

X AGREE
__ **PARTIALLY DISAGREE**
__ **DISAGREE**

Response explanation (required for a response other than **Agree**):

F6. The City does not have an individual dedicated as the lead for cyber security, which could lead to inadequate preparation for and response to a cyber attack.

X AGREE
__ **PARTIALLY DISAGREE**
__ **DISAGREE**

Response explanation (required for a response other than **Agree**):

F7. The City of Santa Cruz does not have a Cybersecurity Policy, suggesting that preparations to mitigate a cyber attack are inadequate and not widely shared.

X **AGREE**

__ **PARTIALLY DISAGREE**

__ **DISAGREE**

Response explanation (required for a response other than **Agree**):

F8. The City of Santa Cruz does not have an Incident Response Plan, and this absence indicates that the City will be challenged in responding to a cyber attack, especially a ransomware attack.

X **AGREE**

__ **PARTIALLY DISAGREE**

__ **DISAGREE**

Response explanation (required for a response other than **Agree**):

F9. Santa Cruz participates in some information sharing organizations such as the California Municipal Information Services Association (MISAC), yet it has minimal collaboration within the county and the other cities, forfeiting opportunities to share best practices and understand threats.

X **AGREE**

__ **PARTIALLY DISAGREE**

__ **DISAGREE**

Response explanation (required for a response other than **Agree**):

Recommendations

R4. The City of Santa Cruz should prioritize filling its vacant IT department positions by Fall 2023. The IT Department and the Human Resources (HR) Department should revise its position requirements, compensation packages, and recruiting priorities to enable the City to attract qualified personnel to these positions. (F4)

X **HAS BEEN IMPLEMENTED –** summarize what has been done

__ **HAS NOT YET BEEN IMPLEMENTED BUT WILL BE IN THE FUTURE –** summarize what will be done and the timeframe

__ **REQUIRES FURTHER ANALYSIS –** explain the scope and timeframe (not to exceed six months)

__ **WILL NOT BE IMPLEMENTED –** explain why

Required response explanation, summary, and timeframe:

At the time of the interview with the Civil Grand Jury, the City of Santa Cruz (City) Information Technology (IT) Department was experiencing significant staffing shortages. Since the interview, the IT Department staffing shortages have improved. Currently, 22 of the 23 Full Time Equivalent (FTE) IT positions have been filled. This includes filling positions critical to helping manage, and proactively improving the City's overall cybersecurity posture.

R5. By Fall 2023, Santa Cruz should identify and implement creative approaches to hiring and retention so they can maintain a fully staffed IT Department despite the competition with surrounding counties. The City should investigate potential partnerships with one or more of the 18 California colleges and universities with National Centers of Academic Excellence in Cybersecurity. (F5)

__ **HAS BEEN IMPLEMENTED –** summarize what has been done

X **HAS NOT YET BEEN IMPLEMENTED BUT WILL BE IN THE FUTURE –** summarize what will be done and the timeframe

__ **REQUIRES FURTHER ANALYSIS –** explain the scope and timeframe (not to exceed six months)

__ **WILL NOT BE IMPLEMENTED –** explain why

Required response explanation, summary, and timeframe:

The City's Human Resources (HR) department is continually exploring avenues to adopt dynamic and innovative recruitment strategies, such as direct networking, compensation analysis, engaging with educational institutions, and fostering workforce development. By fall of 2023, IT recruitments will involve actively seeking collaborations with state and local universities renowned for their academic excellence in cybersecurity.

R6. By Fall 2023, the City of Santa Cruz should assign one individual responsible for cybersecurity. Adoption of a managed service provider arrangement will boost its security posture, although it does not eliminate the need for a dedicated security lead within the City's IT Department. (F6)

X **HAS BEEN IMPLEMENTED –** summarize what has been done

__ **HAS NOT YET BEEN IMPLEMENTED BUT WILL BE IN THE FUTURE –** summarize what will be done and the timeframe

__ **REQUIRES FURTHER ANALYSIS –** explain the scope and timeframe (not to exceed six months)

__ **WILL NOT BE IMPLEMENTED –** explain why

Required response explanation, summary, and timeframe:

Reduced staffing has likely increased the risk of cyber vulnerabilities across City IT networks. In 2022, the City partnered with a Managed Security Service Provider (MSSP) to augment the City's staffing challenges. The City's MSSP provides a comprehensive outsourced security solution for the City, including 24-hour-a-day security monitoring of networks and endpoints and incident response assistance.

The IT infrastructure team has jointly managed the City's cybersecurity initiatives in collaboration with the City's MSSP. Beginning June 1st, 2023, the IT Manager overseeing the infrastructure team will be the single point of contact within the City responsible for performing the duties as the dedicated cybersecurity lead.

Additionally, the City is evaluating the feasibility of adding a dedicated FTE to lead cybersecurity initiatives across the City.

R7. By the end of 2023 or sooner, the City of Santa Cruz should develop and implement a Cybersecurity Plan that encompasses all aspects of information security. (F7)

__ **HAS BEEN IMPLEMENTED –** summarize what has been done

X **HAS NOT YET BEEN IMPLEMENTED BUT WILL BE IN THE FUTURE –** summarize what will be done and the timeframe

__ **REQUIRES FURTHER ANALYSIS –** explain the scope and timeframe (not to exceed six months)

__ **WILL NOT BE IMPLEMENTED –** explain why

Required response explanation, summary, and timeframe:

The IT Department has completed a draft Cybersecurity Policy Plan, which is currently undergoing an approval process to be formalized as an internal Administrative Procedure Order (APO). The Cybersecurity Policy will be integrated into the City's existing Technology Use APO upon completion. The policy formalization process is expected to conclude by the end of 2023 or potentially earlier.

In addition, the City has initiated discussions with neighboring organizations, such as the County of Santa Cruz, the City of Watsonville, the City of Scotts Valley, and the Santa Cruz Public Libraries, to develop a comprehensive Cybersecurity plan that covers the entire county. The County of Santa Cruz is leading this effort, organizing regular meetings to foster collaboration among the involved parties.

R8. By the end of 2023 or sooner, the City should complete an Incident Response Plan with sufficient detail for city officials to use as a step-by-step guide in the event of a cyber incident. (F8)

__	**HAS BEEN IMPLEMENTED –** summarize what has been done
X	**HAS NOT YET BEEN IMPLEMENTED BUT WILL BE IN THE FUTURE –** summarize what will be done and the timeframe
__	**REQUIRES FURTHER ANALYSIS –** explain the scope and timeframe (not to exceed six months)
__	**WILL NOT BE IMPLEMENTED –** explain why

Required response explanation, summary, and timeframe:

The City's IT Department has completed a draft Cybersecurity Incident Response plan. This plan will become an integral part of IT's internal policies upon final approval. The formalization of this plan is expected to be completed by the end of calendar year 2023 or potentially earlier.

R9. Once the IT Department has adequate staffing and by the end of 2023, it should expand its participation in local and state information sharing groups to maintain current knowledge of the threat environment and emerging technologies. (F9)

X **HAS BEEN IMPLEMENTED –** summarize what has been done

__ **HAS NOT YET BEEN IMPLEMENTED BUT WILL BE IN THE FUTURE –** summarize what will be done and the timeframe

__ **REQUIRES FURTHER ANALYSIS –** explain the scope and timeframe (not to exceed six months)

__ **WILL NOT BE IMPLEMENTED –** explain why

Required response explanation, summary, and timeframe:

The City’s IT Department is actively engaged in multiple local, state, and federal groups that emphasize sharing cybersecurity-related information among local and state organizations. The City regularly participates in the Northern California Regional Information Center (NCRIC) and the Municipal Information Systems Association of California (MISAC). Additionally, the City has partnered with Cybersecurity and Infrastructure Security Agency (CISA) for regular vulnerability and hygiene scans. Moreover, several local government agencies have initiated a collaborative effort, namely the City of Watsonville, the City of Capitola, the County of Santa Cruz, and the Santa Cruz Public Library. This newly formed regional group focuses specifically on cybersecurity and conducts regular meetings to exchange knowledge and security insights.