SANTA CRUZ COUNTY
Civil Grand Jury

701 Ocean Street, Room 318-I
Santa Cruz, CA 95060
(831) 454-2099
grandjury@scgrandjury.org

Cyber Threat Preparedness

Phishing and Passwords and Ransomware, Oh My!

Summary

Cyber attacks targeting computer information systems, personal digital devices, or smartphones increase every year with the largest number of attacks typically hitting California. Cyber criminals target all types of businesses and all sizes of government agencies including small cities that often have limited resources to invest in cybersecurity. As Santa Cruz County continues its plans to expand broadband access and to provide efficient digital services to its residents, adherence to cybersecurity measures and best practices is critical.

Santa Cruz County and the cities of Santa Cruz, Watsonville, Scotts Valley, and Capitola understand the cyber threat environment and the potential consequences of a cyber attack. These government entities have implemented varying levels of security measures to mitigate such threats.

The Jury's overall recommendations encompass the following:

- The County and the four cities should write and implement Cybersecurity Plans and Incident Response Plans that detail frameworks for mitigating cyber attacks and details for responding to a cyber incident.
- Each of our cities should designate a city official as the lead for cybersecurity. Even when an information technology consulting firm supports the city, one government official should be responsible for cybersecurity.
- The County and cities would benefit from cyber threat information sharing across the county, enabling greater knowledge of potential threats and shared ideas for threat mitigation.

Table of Contents

Background

Cyber preparedness is the practice of ensuring that an entity has a strategy to mitigate, respond, and recover from a cyber incident on its networks or devices. With cyber attacks continuing to escalate year over year, and targets expanding to include small- and mid-sized cities, schools, and medical facilities, Santa Cruz County and its cities need to allocate sufficient attention to this threat. Cyber attacks can occur in many ways and can produce a wide range of effects including:

- Damaging financial security and theft of intellectual property;
- Theft of personally identifiable information (PII);
- Blocking digital access or deleting information and accounts;
- Complicating or blocking business and government services, and
- Interfering with transportation, power networks, and other critical infrastructure.

The United States remains the top target worldwide for all types of cyber attacks, with Californians constituting the most frequent victims, totalling over 67,000 people or businesses for a total loss of more than $1.2 billion in 2021.[1] [2] According to the California Cybersecurity Integration Center (Cal-CSIC), in 2022, ransomware was by far the most common type of cyber attack in the state, although other cyber crimes, including data breaches and investment crimes, are common as well. No industry sector has been spared from cyber attacks. In the last six months of 2022 alone, the Cal-CSIC recorded over 250 cyber incidents in California and a 22 percent increase in ransomware attacks over the first six months of the year.[2] [3] [4]

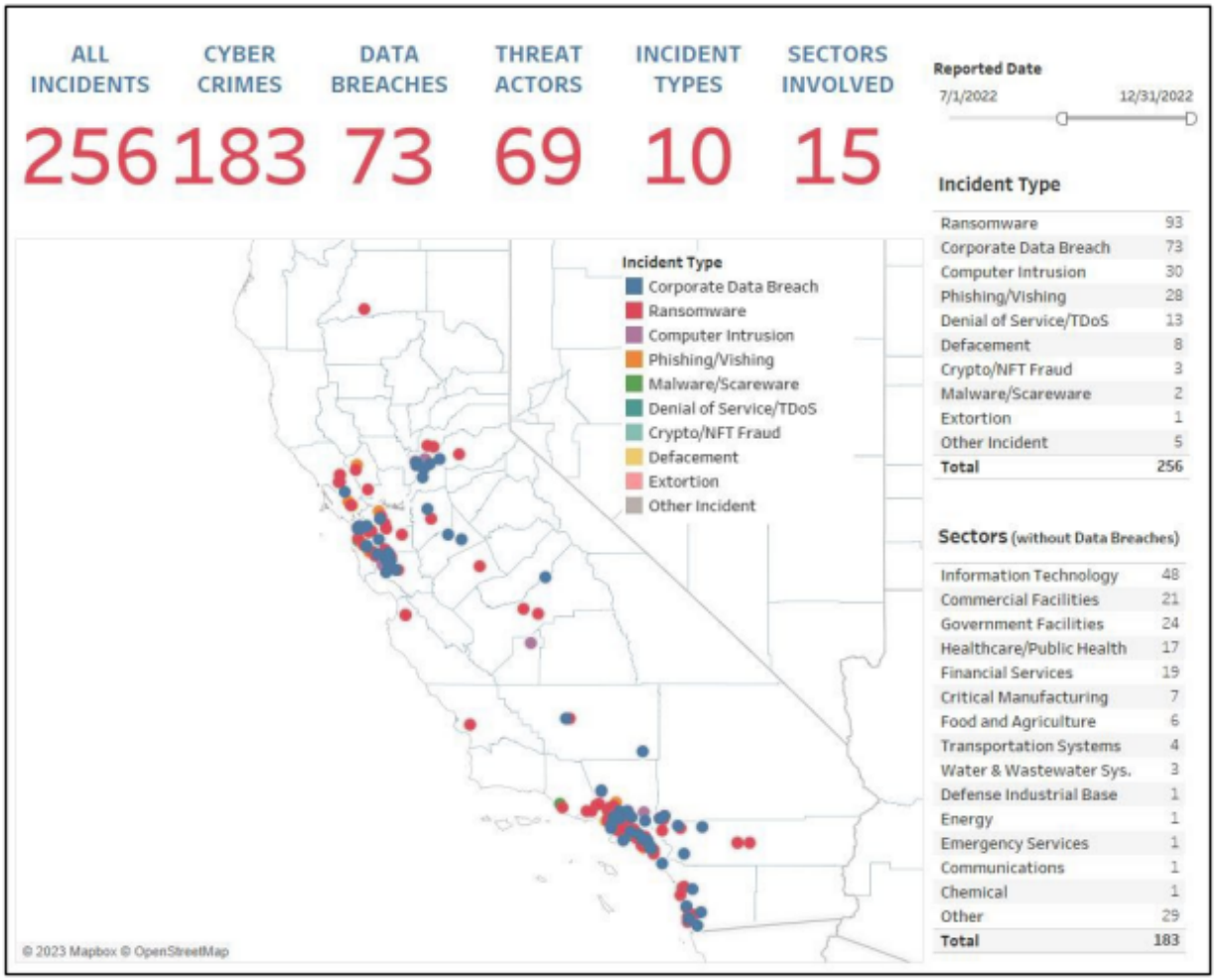

Figure 1. Cal-CSIC reporting on sectors targeted and types of cyber attacks in California in the second half of 2022.[3]

Over the past several years, cyber attacks have become much more sophisticated, often leveraging multiple attack surfaces, third-party software, or cloud-based infrastructure to reach a viable target. In the cyber industry, experts recognize that it is not a question of whether an attack will happen, but rather when an attack will happen and how prepared the target entity is to mitigate the impacts.[5] [6] [7] [8]

In mid-February 2023, the city of Oakland declared a local emergency and shut down some of its city services, including non-emergency calls, parking and business payments, and planning services, when it was hit by a ransomware attack.[9] As of early March, the hacker group had released over nine gigabytes of data including employees' social security numbers, driver license numbers, addresses, and bank statements of the city's operating accounts.[10] [11]

In March 2018, the city of Atlanta was the target of a ransomware attack that shut down many city services, including court services and utilities, for several weeks and at the cost of more than $10 million.[12] [13] [14]

Small cities are not immune to ransomware attacks, as evidenced by the November 2018 ransomware attack against Valdez, Alaska, a city of less than 4,000 residents. Contrary to FBI advice, the city admitted to paying the ransom to recover access to their network.[15] The cost of the attack probably totaled considerably more than the ransom itself as the city hired a well known cybersecurity firm to negotiate the ransom payment and ensure recovery of their data. While the cost of the Valdez ransomware attack was in the tens of thousands, in 2022, the cost of a data breach reached an average of $4.35 million, according to IBM's Cost of a Data Breach Report.[16]

Fortunately, Santa Cruz County has not experienced the breadth of cyber attacks that many other counties experience; however, an attack could occur at any time and could have significant impacts across the county.[17] [18] Given the daily barrage of news about cyber attacks, the Santa Cruz County Civil Grand Jury elected to shine a light on the level of cyber preparedness in our county and our cities.

Scope and Methodology

The Santa Cruz Civil Grand Grand Jury sought to evaluate the overall level of preparedness for a cyber incident against the county or city networks. It performed research across federal and state resources, top cyber security sites, and reputable media sources to build an understanding of the current cyber landscape and a foundation for cyber preparedness. Based on interviews with subject matter experts and resources available from the Cybersecurity and Infrastructure Security Agency (CISA) at the Department of Homeland Security (DHS) and the National Institute of Standards and Technology (NIST) in the U.S. Department of Commerce, the jury delineated key elements of strong cyber hygiene, the security and health of the information systems, and best practices for local governments.[6] [19] [20]

The Grand Jury conducted multiple interviews of employees in Santa Cruz County and its cities. The investigation examined the extent to which cyber precautions are implemented and maintained–including cyber awareness training, common network security measures, and planning for cyber incidents–across Santa Cruz County and the cities of Santa Cruz, Watsonville, Scotts Valley, and Capitola. The Grand Jury specifically looked at:

- Do Santa Cruz County and its cities stay informed on emerging technologies and current cyber threat trends?
- Is there an identified individual responsible for cyber security?
- Do the County and its cities routinely follow recommended cyber security practices?
- What is the extent of cyber awareness training for county and city staff, particularly given that most attacks begin with phishing emails?
- To what extent do the County and cities participate in regional or state-level information sharing or information sharing within the County itself with respect to cyber threats?
- Do the County and the cities have a plan in place for mitigating cyber attacks?

- Are there policies and procedures in place for how our local governments will respond to a cyber attack?
- Do the County and cities have cyber insurance?

In each interview the Civil Grand Jury conducted, it discussed best practices in cyber security and the state of each entity's cyber hygiene or the practices organizations and individuals perform regularly to maintain the security and functionality of users, devices, networks, and data.[21] The discussions highlighted the preparations to mitigate, detect, and manage cyber incidents and the level of attention to training and education, all of which constitute an entity's level of cyber maturity.

The Civil Grand Jury investigation focused solely on the county and city governments. It did not assess cyber preparedness at the County Office of Education or the schools, law enforcement and fire entities, or critical infrastructure such as water systems and public health facilities.

Investigation

The Civil Grand Jury's research underscored the fact that, to date, our county has not been a target of a major cyber attack. This favorable status is not likely to continue given the increasing volume of cyber incidents and the very broad nature of targets, many of which are simply targets of opportunity rather than entities of specific interest to cyber criminals.

The most notable cyber attack raised during the jury's research was the December 2010 Distributed Denial of Service (DDOS) attack against the Santa Cruz County website that temporarily shut down the site and county digital services. A DDOS attack is a malicious attempt to disrupt a website by overwhelming the site with communication requests, thus denying access to legitimate users. According to the 2011 Department of Justice indictment, the People's LIberation Front (PLF), a group associated with the Anonymous hacktivist group, planned and executed the attack. The cyber actor, known by the moniker "Commander X," conducted the DDOS attack as part of "Operation Peace Camp 2010," a protest against the county's camping policies.[22] [23]

The Commander X cyber incident was a wake-up call for Santa Cruz County, highlighting the vulnerabilities and potential damage of a cyber attack that could quickly shut off county services. Since that time, the sophistication, frequency, and nature of cyber attacks has evolved dramatically with ransomware attacks becoming the most common and costly type of cyber incident. Ransomware is a form of malware that encrypts files on a device or network rendering the files and/or services unusable. Malicious actors then demand ransom in exchange for releasing the files. Examples in 2022 include the September 3rd ransomware attack against the Los Angeles Unified School District, the October 2nd ransomware attack against Hartnell College in Salinas, and the October 5th ransomware attack against CommonSpirit, the parent company of Dominican Hospital, that exposed the personal data of 623,700 patients and recently prompted a lawsuit. Fortunately, the CommonSpirit attack did not impact patients at Dominican Hospital in Santa Cruz.[15] [24] [25] [26] [27] [28]

A CISA cybersecurity advisory published in 2022 noted that recent trends, tactics, and protocols (TTP) among ransomware actors encompass:

- Gaining access to networks via phishing emails, stolen Remote Desktop Protocols (RDP) credentials or brute force, and exploiting network vulnerabilities. The pandemic-caused increase in remote work significantly expanded the landscape for cyber actors.
- Using cybercriminal services-for-hire. Ransomware attacks can now be conducted through ransomware-as-a-service (RaaS) that sells malware as well as services to negotiate and facilitate payments.
- Sharing victim information across cyber criminal groups.
- Targeting a greater number of medium and smaller organizations, including local governments and public services.
- Diversifying avenues for extorting money to include the threat of releasing stolen data, further network disruptions, and informing shareholders and partners.[6]

The same CISA Advisory, along with additional CISA cybersecurity resources for state and local governments, recommends several measures for minimizing the chance of and mitigating the impact of cyber attacks:

- Maintain data back-up versions, preferably to multiple locations, requiring multi-factor authentication (MFA) for access, and encrypting data in the cloud.
- Require MFA for as many services as possible, particularly for webmail, accounts that access critical systems, privileged accounts that manage backups, and virtual private networks (VPN).
- Keep all operating systems and software up to date.
- Implement a user training program and phishing exercises to raise awareness among users about the risks of visiting suspicious websites, clicking on suspicious links, and opening suspicious attachments.
- Evaluate and monitor third-party software for security concerns.
- Ensure devices are properly configured and that security features are enabled.
- Maintain a current Cybersecurity Policy and Incident Response Policy that is accessible when networks are inoperable.[6] [19]

Cyber Best Practices across Santa Cruz County

The Civil Grand Jury applied this list of best practices cited above, with the addition of a Cyber Insurance Policy, in its assessment of cyber preparedness in the county and cities. With respect to cyber insurance, insurance companies such as Beazley, Ironshore, and other markets offered through the Monterey Bay Area Self Insurance Authority (MBASIA) and Alliant, which provide insurance coverage for our cities, are now requiring government entities to meet basic cyber best practices to be eligible for all insurance coverages. If these requirements are not met, the government entities may still have cyber insurance for some causes of loss, but payments may be restricted if the

cyber measures are not implemented before an incident occurs. In order to obtain competitive insurance terms, access all coverage terms available, and control claims exposures, cyber hygiene measures should be prioritized for implementation.[23]

The Jury concluded that Santa Cruz County and its cities are well educated on the potential cyber threats–probably more so than most U.S. cities of similar size–and are making efforts to improve their cyber posture. The jury identified several areas for improvement and a critical need for more attention to cybersecurity among county and city leaders. Information Technology (IT) and cyber professionals understand that cybersecurity constitutes a business problem, not an IT problem, and therefore, is everyone's responsibility.

Table 1 summarizes the cyber best practices and levels of adoption by Santa Cruz County and city government entities.

Table 1. Summary of best practices

Cyber Security Practice	Santa Cruz County	Santa Cruz City	Watsonville	Scotts Valley	Capitola
Routinely Back-up Data	M	M	M	M	M
Multi-factor Authentication	M	M	IP	A	IP
Timely Patching and Updates	M	IP	M	M	M
Restrict Admin Accounts	M	M	M	M	M
Security Awareness Training	M	M	M	M	IP
Cybersecurity Policy	A	A	A	A	A
Incident Response Plan	A	A	A	A	A
Cyber Insurance	IPA	IPA	IPA	IPA	IPA

Key:		
	M	Currently meet standards
	IP	Improvement in process
	A	Needs attention
	IPA	Needs more attention before an incident

Source: Grand Jury interviews and document requests[29] [30] [31] [32] [33] [34] [35] [36] [37] [38] [39] [40] [41] [42] [43] [44] [45] [46] [47] [48] [49] [50] [51] [52] [53] [54] [55] [56] [57] [58] [59] [60] [61] [62] [63] [64] [65] [66] [67] [68] [69] [70] [71] [72]

Steps in the Right Direction

Santa Cruz County and the city governments of Santa Cruz, Watsonville, Scotts Valley, and Capitola demonstrate a strong awareness of potential cyber threats and the risks of a ransomware attack against county or city networks. Across these public entities, there is a wide variation in resources assigned to cybersecurity and efforts to mitigate the growing threats.

With a well structured Information Services Department (ISD) and a plan to hire a dedicated Chief Information Security Officer (CISO) in 2023, Santa Cruz County has built a solid foundation for cybersecurity.[73] [74] The County is aware of possible areas for improvement and is working towards filling any cybersecurity gaps. With its strong foundation and IT resources, the County is positioned to take a leading role in cybersecurity across the county.

Santa Cruz City appears well educated on the potential cyber threats to cities, although it lacks sufficient resources to fully implement appropriate security measures. The City's primary challenge is hiring and retaining qualified personnel. The City IT department is implementing measures to raise its level of cyber hygiene, including participation in CISA services and augmenting cyber best practices.[35]

Watsonville recently revamped and enlarged its IT Department to meet its IT requirements and match the changing threat environment. While its new IT structure and system upgrades are critical for improving the functionality and security of city networks, they are not yet sufficient to mitigate the range of potential cyber threats. Watsonville is working towards raising awareness of cyber threats across city departments and expanding its capabilities.[62]

Scotts Valley manages its IT needs, including cybersecurity, through a local contracting company that is responsible for all aspects of information technology from user support and staff training to network monitoring and cybersecurity. The consulting company maintains a current and strong understanding of cyber threats and the status of city networks. The company is positioned to respond rapidly to any network threats.[9] [52]

With one person responsible for all of the IT needs of Capitola, the City is inadequately resourced to meet the threat of cyber attacks. Capitola did not replace its IT Director when he departed in mid-2022. Although Capitola recently contracted with an IT consulting company for technology services, the contract support is limited. There is no city official responsible for cybersecurity, and awareness of the potential threats–especially in the wake of increased national attention following the 2023 storms–is limited.[43] [46]

Conclusion

Overall, the Grand Jury investigation found that the IT staff in the county and city governments are well aware of current and growing cyber threats to local governments and the potential consequences of a cyber attack. The level of preparedness for mitigating and responding to an attack varies from the County's excellent cyber security

foundation to minimal security measures in some of the cities. Nationwide, under-resourced public sectors are insufficiently prepared for cyber attacks and continue to be heavily targeted by cyber criminals. Lack of adequate budgets and skills shortages make these localities potentially vulnerable. In several cases in our county, IT staff appeared swamped with the daily press of the business of managing hardware, software, and access issues, leaving cybersecurity to fall to a lower priority.[75] [76]

The potentially high cost of a ransomware attack underscores that in addition to the IT staff, executive-level attention to the risks and a greater investment in cybersecurity is a sound business practice for local governments.[77] All of our government entities would benefit from greater countywide collaboration and information sharing.[78] Multiple regional and state resources offer opportunities for cyber threat information sharing. As one official noted, monthly coffees with the IT leads in each local government would offer a very useful opportunity to share cyber TTPs and best practices specific to Santa Cruz County.

The Grand Jury recognizes the limited resources available to small counties and cities, a situation that often leads to a lack of funding and insufficient attention to cybersecurity. The Jury would argue that the potential cost of a ransomware attack more than justifies a much greater investment in cybersecurity.[79] There are several avenues small cities should consider to enhance their cybersecurity including:

1. **Secure long-term funding for cybersecurity in the core budget.** A proactive approach that prioritizes network defense, situational awareness, and education is a critical element of cybersecurity and well worth the commitment. Cybersecurity should be a budget item on a business level, not solely an IT budget allocation.
2. **Hire and retain cyber talent.** Small and medium-sized cities need to identify innovative methods for hiring and retaining the appropriate expertise to ensure secure networks and a vigilant security program. If funding limits the ability to hire a sufficient number of competent IT professionals, cities may want to consider a part-time CISO position, shared resources, or hiring an outside contractor.
3. **Set up strong relationships with the private sector**. Santa Cruz is well positioned to leverage private sector partnerships in the region that may offer additional resources and superb cyber expertise with minimal investments.
4. **Build an exhaustive Incident Response Policy.** Every entity should maintain a current Incident Response Policy that delineates established relationships, detailed scenario planning, step-by-step instructions for incident responses, defined public relations measures, and plans for business continuity. Such a plan is critical to delineate the processes that will allow cities to continue serving the public in the event of an attack. The plan should define how systems will be restored without disrupting the business continuity, steps for a thorough investigation of the nature of the breach, and an immediate investment in addressing the vulnerabilities.

5. **Improve training and culture.** A company culture that encourages security and provides a broad range of cybersecurity training is the best approach to mitigating cyber threats, in both government and private entities.[73] [74]
6. **Rely on cybersecurity best practices.** At a minimum, entities should ensure the use of reputable automation and cybersecurity tools across all networks. The cybersecurity foundation should encompass firewalls, antivirus software, and strong endpoint and network security products that allow visibility into the network.[18]

With proper cybersecurity measures in place, our county and cities could take advantage of the cybersecurity grant opportunities available from federal agencies such as DHS/CISA and the Federal Emergency Management Agency (FEMA). In the event of limited resources to prepare and apply for grants, the County and cities would be well served by hiring a consultant to write grant proposals. In the long run–or possibly in the short run–such expenditures would pay for themselves and much more.[43] [73] [79]

Findings—Santa Cruz County

F1. Santa Cruz County does not have a Cybersecurity Plan, and the absence of a current plan that defines security policies, procedures, and controls required to protect its networks and devices increases the risk of vulnerabilities.

F2. Santa Cruz County does not have a sufficiently detailed Incident Response Plan, indicating they would not be prepared to respond rapidly and effectively in the event of a cyber incident.

F3. Santa Cruz County participates in multiple information sharing groups at regional and state levels, although it has only minimal interaction with the cities across Santa Cruz County, degrading their ability to fully understand regional vulnerabilities.

Recommendations—Santa Cruz County

R1. Santa Cruz County should prepare and implement a Cybersecurity Plan by the end of 2023, ensuring that city officials and all staff are well aware of the plan details, their responsibilities, and associated policies. (F1)

R2. By the end of 2023, the county should revise and expand its Incident Response Plan to clearly delineate the steps it will take in response to a cyber attack, the responsibilities of identified officials, and the coordination required with state and federal officials for each type and level of cyber attack. A detailed plan is a requirement for continuity of county operations in a cyber incident. (F2)

R3. The County's information sharing efforts should be expanded to ensure fulsome information sharing across all government entities in the county, specifically Santa Cruz, Watsonville, Scotts Valley, and Capitola, by the end of 2023. A simple schedule of monthly meetings would permit regular sharing of possible threats, TTPs seen across the county, and information learned from outside organizations such as the Cal-CSIC. (F3)

Findings—City of Santa Cruz

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.

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

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.

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.

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.

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.

Recommendations—City of Santa Cruz

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)

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)

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)

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)

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)

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)

Findings—City of Watsonville

F10. After recently expanding its IT Department, the City of Watsonville has improved its IT functions although it does not yet allocate sufficient resources to cybersecurity.

F11. The City does not have an individual whose primary responsibility is cybersecurity for the city networks, leaving cybersecurity oversight to the IT Director–along with a multitude of other IT responsibilities–and lowering the priority for cybersecurity measures.

F12. Watsonville does not have a Cybersecurity Plan that defines security policies, procedures, and controls required to protect its networks and devices, a situation that increases the risks of vulnerabilities.

F13. Watsonville does not have an Incident Response Plan that provides detailed information on how to respond to an attack, suggesting the City would not be able to respond rapidly and effectively to a cyber attack.

F14. Watsonville participates in some regional information sharing forums, but it does not have the resources to expand its participation or tap into state-level information sharing, thus forfeiting valuable best practices and cyber threat information.

Recommendations—City of Watsonville

R10. Watsonville should conduct an evaluation of its recently expanded IT Department, critical IT upgrades, and the status of cybersecurity measures by the end of 2023. Based on this assessment, the City should allocate existing or newly identified resources to ensure cybersecurity is adequately addressed going forward. (F10)

R11. Given the size of Watsonville, the City should have a dedicated position for cybersecurity by the end of 2023, to ensure adherence to best practices, mitigation of potential threats, and education of city staff and leadership. (F11)

R12. By early 2024 or sooner, Watsonville should prepare and implement a Cybersecurity Plan that addresses all of the best practices for strong cyber hygiene. (F12)

R13. By early 2024 or sooner, Watsonville should prepare and implement an Incident Response Plan with sufficient detail to serve as a guide in the event of a cyber attack. (F13)

R14. Upon completion of IT structural upgrades and a higher level of cyber maturity, and by the end of 2023, Watsonville should participate in local, regional, and state information sharing initiatives. (F14)

Findings—City of Scotts Valley

F15. Although Scotts Valley's managed service provider is very knowledgeable and capable of providing cybersecurity services, there is no single city official with cybersecurity oversight, potentially leading to a poor understanding of the threats and an inadequate response to a cyber attack.

F16. Scotts Valley does not have a current Cybersecurity Plan that defines security policies, procedures, and controls required to protect its networks and devices, potentially increasing the risks of vulnerabilities.

F17. Scotts Valley does not have a current Incident Response Plan, which could exacerbate the effects of a cyber incident such as increase the time a network is unavailable or raise the potential financial costs of a resolution.

F18. Scotts Valley does not participate in any cybersecurity information sharing groups to enhance best practices, rather they depend on their contractor to stay informed, which makes the City last to know of critical cyber threats.

Recommendations—City of Scotts Valley

R15. By mid-2023, Scotts Valley should assign a city official as the lead for cybersecurity for the city. This individual should oversee the contractor's performance in cybersecurity and ensure city leaders are well informed on emerging threats, cybersecurity challenges, and information provided from regional and state entities. (F15)

R16. Working with its IT contractor, by Fall 2023, Scotts Valley should write and implement a Cybersecurity Plan that is shared with all city officials to demonstrate comprehensive security measures and executive-level cyber threat awareness. (F16)

R17. By Fall 2023, Scotts Valley should write an Incident Response Plan that clearly delineates the steps it will take in response to a cyber attack, the responsibilities of identified officials, and the coordination required with state and federal officials for each type and level of cyber attack. (F17)

R18. Scotts Valley should participate in local, regional, and state cybersecurity organizations for information sharing by the end of 2023. (F18)

Findings—City of Capitola

F19. With one individual responsible for IT services, Capitola does not allocate sufficient resources to cybersecurity, a status that could lead to poor cyber knowledge and unnecessary vulnerabilities.

F20. The City of Capitola does not have a robust cybersecurity training program, nor does it conduct phishing tests or routinely remind employees to adhere to cybersecurity measures during potential periods of increased threats.

F21. The City of Capitola does not have a Cybersecurity Plan to address cybersecurity measures city wide, suggesting the city is not adequately mitigating the potential impact of cyber incidents.

F22. The City of Capitola does not have an Incident Response Plan, which could exacerbate the effects of a cyber incident such as increase the time a network is unavailable or raise the potential financial costs of a resolution.

F23. Capitola does not participate in any cyber-focused information sharing groups, nor does it take advantage of state and federal resources designed to assist small cities with mitigating cyber attacks, thereby forfeiting opportunities to learn best practices and raise their cyber awareness.

Recommendations—City of Capitola

R19. By Fall 2023, Capitola should hire a full-time IT Director to replace the IT Director who departed in mid-2022. The IT Director should oversee and expand IT services, including those of the consulting company, and lead cybersecurity initiatives. (F19)

R20. The City should develop a more robust cybersecurity training and phishing testing program for all employees by Fall 2023 or earlier. (F20)

R21. Capitola should establish and implement a Cybersecurity Plan by the end of 2023. Several resources exist to provide a foundation or templates for these plans including NIST Guidelines, CISA resources, and Cal-CSIC guidance. (F21)

R22. By Fall 2023 Capitola should prepare an Incident Response Plan that provides detailed guidance for a city response to a cyber attack. (F22)

R23. When appropriately resourced to monitor cyber threats, and by the end of 2023, Capitola should participate in regional cybersecurity information sharing groups, to gain valuable information to best protect the City. (F23)

R24. By mid-2023, Capitola city management should raise the priority it assigns to cybersecurity and demonstrate a recognition of their role in ensuring the security of the City's information networks.(F19–F23)

Commendations

C1. Santa Cruz County has built an excellent foundation for preparing for the possibility of cyber incidents. Its Information Services Department (ISD) has a very knowledgeable Director, is very well informed, and has taken steps to prioritize cybersecurity. The integration of ISD in all IT purchasing processes provides a sound check on the security of third-party software, and its cyber training appears well integrated for all county staff.

C2. The City of Santa Cruz has instituted a cyber awareness program that is strongly enforced. Its IT Advisory Team and standard security questions provide a security perspective for all third-party software purchases, thus minimizing supply chain threats.

C3. Watsonville has instituted commercial cyber security training for all employees and has recently begun to raise cyber risk awareness among city executives, highlighting that cyber security is a business problem for all departments and that promoting cyber education among government leaders is a critical element of effective cyber hygiene.

Required Responses

Respondent	*Findings*	*Recommendations*	*Respond Within/ Respond By*
Santa Cruz County Board of Supervisors	F1–F3	R1–R3	90 Days August 16, 2023
Santa Cruz City Council	F4–F9	R4–R9	90 Days August 16, 2023
Watsonville City Council	F10–F14	R10–R14	90 Days August 16, 2023
Scotts Valley City Council	F15–F18	R15–R18	90 Days August 16, 2023
Capitola City Council	F19–F23	R19–R24	90 Days August 16, 2023

Definitions

Access:The ability and means to communicate with or otherwise interact with a system, to use system resources to handle information, to gain knowledge of the information the system contains, or to control system components and functions.

Adversary: An individual, group, organization, or government that conducts or has the intent to conduct detrimental activities.

Antivirus software: A program that monitors a computer or network to detect or identify major types of malicious code and to prevent or contain malware incidents. Sometimes by removing or neutralizing the malicious code.

Attack: An attempt to gain unauthorized access to system services, resources, or information, or an attempt to compromise system integrity.

Attack surface: The set of ways in which an adversary can enter a system and potentially cause damage.

Continuity of operations plan: A document that sets forth procedures for the continued performance of core capabilities and critical operations during any disruption or potential disruption. Continuity of operations may be included in an Incident Response Plan.

Critical infrastructure: The systems and assets, whether physical or virtual, that are so vital to society that the incapacity or destruction of such may have a debilitating impact on the security, economy, public health or safety, environment, or any combination of these matters.

Cyber hygiene: The practices organizations and individuals perform regularly to maintain the health and security of users, devices, networks, and to ensure the safe handling of data.

Cybersecurity: The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation.

Cybersecurity maturity: Cybersecurity maturity refers to an organization's capabilities and degree of readiness to mitigate vulnerabilities and threats from cyber criminals. The more 'mature' a company's cybersecurity protocols and practices are, the better equipped it is at preventing threats before they become breaches.

Data breach: The unauthorized movement or disclosure of sensitive information to a party, usually outside the organization, that is not authorized to have or see the information.

Denial of service: An attack that prevents or impairs the authorized use of information system resources or services.

Disruption: An event which causes unplanned interruption in operations or functions for an unacceptable length of time.

Distributed denial of service (DDOS): A denial of service technique that uses numerous systems to perform the attack simultaneously.

Event: An observable occurrence in an information system or network; also known as an incident.

Exploit: A technique to breach the security of a network or information system in violation of security policy.

Hacker: An unauthorized user who attempts to or gains access to an information system.

Incident: An occurrence that actually or potentially results in adverse consequences to an information system or the information that the system processes, stores, or transmits and that may require a response action to mitigate the consequences.

Incident response: The activities that address the short-term, direct effects of an incident and may also support short-term recovery.

Incident response plan: A set of predetermined and documented procedures to detect and respond to a cyber incident.

Information or cyber security policy: An aggregate of directives, regulations, rules, and practices that prescribe how an organization manages, protects, and distributes information.

Information sharing: An exchange of data, information, and/or knowledge to manage risks or respond to incidents.

Information technology: Any equipment or interconnected system or subsystem of equipment that processes, transmits, receives, or interchanges data or information.

Malicious code: Program code intended to perform an unauthorized function or process that will have adverse impact on the confidentiality, integrity, or availability of an information system.

Malware: Software that compromises the operation of a system by performing an unauthorized function or process.

Mitigation: The application of one or more measures to reduce the likelihood of an unwanted occurrence and/or lessen its consequences.

Multi Factor Authentication (MFA): A form of authentication that requires a user to provide two or more verification factors to access a resource such as an online account.

Personally identifiable information (PII): The information that permits the identity of an individual to be directly or indirectly inferred.

Phishing: A digital form of social engineering to deceive individuals into providing sensitive information.

Preparedness: The activities to build, sustain, and improve readiness capabilities to prevent, protect against, respond to, and recover from natural or manmade incidents.

Ransomware as a Service (RaaS): A business model where cyber criminals pay to launch ransomware attacks using malware developed by other individuals.

Recovery: The activities after an incident or event to restore essential services and operations in the short and medium term and fully restore all capabilities in the longer term.

Remote Desktop Protocol (RDP): RDP is a technical standard for using a desktop computer remotely.

Resilience: The ability to adapt to changing conditions and prepare for, withstand, and rapidly recover from disruption.

Response: The activities that address the short-term, direct effects of an incident and may also support short-term recovery.

Risk: The potential for an unwanted or adverse outcome resulting from an incident, event, or occurrence, as determined by the likelihood that a particular threat will exploit a particular vulnerability, with the associated consequences.

Risk assessment: The product or process that collects information and assigns values to risks for the purpose of informing priorities, developing or comparing courses of action, and informing decision making.

Risk mitigation: A structured approach to managing risks to data and information by which an organization selects and applies appropriate security controls in compliance with policy and commensurate with the sensitivity and value of the data.

Security policy: A rule or set of rules that govern the acceptable use of an organization's information and services to a level of acceptable risk and the means for protecting the organization's information assets.

Supply chain: A system of organizations, people, activities, information and resources, for creating and moving products including product components and/or services from suppliers through to their customers.

Supply chain risk management: The process of identifying, analyzing, and assessing supply chain risk and accepting, avoiding, transferring or controlling it to an acceptable level considering associated costs and benefits of any actions taken.

Tactics, techniques, and procedures (TTP): The behavior of an actor. A tactic is the highest-level description of this behavior, while techniques give a more detailed description of behavior in the context of a tactic, and procedures an even lower-level, highly detailed description in the context of a technique.

Targets: The potential and selected subjects of cyber incidents.

Threat: A circumstance or event that has or indicates the potential to exploit vulnerabilities and to adversely impact organizational operations, organizational assets, individuals, other organizations, or society.

Threat analysis: The detailed evaluation of the characteristics of individual threats. Identification and analysis of the capabilities and activities of cyber criminals or foreign intelligence entities.

Threat assessment: The product or process of identifying or evaluating entities, actions, or occurrences, whether natural or man-made, that have or indicate the potential to harm life, information, operations, and/or property.

Unauthorized access: Any access that violates the stated security policy.

Virtual Private Network (VPN): A virtual network built on top of existing networks that can provide a secure communications mechanism for data and IP information transmitted between networks.

Virus: A computer program that can replicate itself, infect a computer without permission or knowledge of the user, and then spread or propagate to another computer.

Vulnerability: A characteristic or specific weakness that renders an organization or asset (such as information or an information system) open to exploitation by a given threat or susceptible to a given hazard.

Sources

References

1. Cowley, Conor. Dec. 13, 2022. “Top US States for Cyber Attacks.” Accessed 11/7/2022. https://tech.co/news/top-us-states-cybersattacks#:~:text=According%20to%20the%20report%20from,of%20%241.2%20billion%20in%202021.

2. Cawley, Conor. Dec. 13, 2022. “Top 10 US States for Cyber-Attacks in 2021, California is the most cyberattacked state largely due to its high population of tech-savvy citizens..” Accessed 2/23/2023. https://tech.co/news/top-us-states-cybersattacks

3. Confidential Grand Jury document.

4. McGee, Vaneesha. Oct. 4, 2022. “Most Common Cyberattacks.” Accessed 2/23/2023. https://www.cyberdegrees.org/resources/most-common-cyber-attacks/

5. Mee, Paul and Chaitra Chandrasekhar. May 3, 2021. “Cybersecurity is too big a job for governments or businesses to handle alone.” *www.weforum.org*. Accessed Nov. 2, 2022. https://www.weforum.org/agenda/2021/05/cybersecurity-governments-business/

6. DHS/CISA. Feb. 10, 2022. “2021 Trends Show Increased Globalized Threat of Ransomware.” *cisa/gov.uscert*. Accessed Nov. 2, 2022. https://www.cisa.gov/uscert/ncas/alerts/aa22-040a

7. Kurtz, George. no date. “2022 Global Threat Report.” *go.crowdstrike.com*. Accessed Nov. 1, 2022. https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2022GTR.pdf

8. Recorded Futures. Mar. 15, 2022. “2021 Malware and TTP Threat Landscape.” *go.recordedfuture.com*. Accessed Nov. 1, 2022. https://go.recordedfuture.com/hubfs/reports/cta-2022-0315.pdf

9. Gatlan, Sergiu. Feb. 10, 2023. “City of Oakland systems offline after ransomware attack.” Accessed 2/13/2023. https://www.bleepingcomputer.com/news/security/city-of-oakland-systems-offline-after-ransomware-attack/

10. Neilson, Susie and Sarah Ravani. March 6, 2023. “Hackers release data of thousands of Oakland city workers--including senior officials.” *News Media*. Accessed 3/7/2023. https://www.sfchronicle.com/eastbay/article/oakland-ransomware-attack-employees-17822693.php

11. no author. Feb. 10, 2023 and updated Feb. 23, 2023. “City of Oakland Targeted by Ransomware Attack, Work Continues to Secure and Restore Services Safely.” Accessed 2/23/2023. https://www.oaklandca.gov/news/2023/city-of-oakland-targeted-by-ransomware-attack-core-services-not-affected

12. Ivayuk, Alexander. Jul. 20, 2018. “The ransomware attack that cost Atlanta over $10 million would have been stopped by Acronis Active Protection.” *acronis.com/blog*. Accessed 10/7/2022. https://www.acronis.com/en-us/blog/posts/ransomware-attack-cost-atlanta-over-10m-would-have-been-stopped-acronis-active-protection/

13. no author. 2022. “Federal Bureau of Investigation 2021 Internet Crime Report.” Accessed 2/23/2023. https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

14. no author. mid-2022. “Microsoft Digital Defense Report 2022.” Accessed 2/23/2023. https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report-2022-state-of-cybercrime

15. Cimpanu, Catalin. Nov. 21, 2018. “City of Valdez, Alaska, admits to paying off ransomware attackers.” *zdnet.com*. Accessed 10/1/2022. https://www.zdnet.com/article/city-of-valdez-alaska-admits-to-paying-off-ransomware-infection/

16. No author. 2022. “Cost of a Data Breach Report 2022.” *ibm.com*. Accessed 1/4/2023. https://www.ibm.com/reports/data-breach?utm_content=SRCWW&p1=Search&p4=43700072379268628&p5=p&gclid=EAIaIQobChMIo4SVqevF_AIVNxXUAR2n8Al7EAAYASAAEgJH9PD_BwE&gclsrc=aw.ds

17. Cimpanu, Catalin. Nov. 21, 2018. “City of Valdez, Alaska, admits to paying off ransomware infection.” *zdnet.com*. Accessed Oct. 30, 2022. https://www.zdnet.com/article/city-of-valdez-alaska-admits-to-paying-off-ransomware-infection/

18. Leader, Megan. Sep. 28, 2022. “How to Apply for Cybersecurity Funding through State and Local Cybersecurity Grant Funding.” *virtru.com*. Accessed 1/30/2023. https://www.virtru.com/blog/how-to-apply-for-cybersecurity-funding-through-the-state-local-cybersecurity-grant-program-slcgp?utm_campaign=&utm_medium=ppc&utm_source=adwords&utm_term=cyber%20security%20grant&hsa_mt=p&hsa_net=adwords&hsa_ver=3&hsa_kw=cyber%20security%20grant&hsa_acc=2362271830&hsa_grp=144213986604&hsa_tgt=kwd-345978984170&hsa_src=g&hsa_ad=628944996457&hsa_cam=18630922509&gclid=EAIaIQobChMIhJyYs9ny_AIVWR-tBh2WiAWQEAAYASAAEgLZ_vD_BwE

19. no author. no date. “Resources for State, Local, Tribal, and Territorial Governments.” *cisa/gov.uscert*. Accessed Oct. 21, 2022. https://www.cisa.gov/uscert/resources/sltt

20. No author. No date. “NIST Cybersecurity Framework.” *nist.gov*. Accessed 10/7/2022. https://www.nist.gov/cyberframework

21. Center for Internet Security. March 15, 2021. “The Solarwinds Cyber-attack: What You Need to Know.” *cisecurity.org*. Accessed Sep. 9, 2022. https://www.cisecurity.org/solarwinds

22. no author. June 15, 2021. “Former Mountain View Resident Christopher Doyen Apprehended in Mexico and Returned to the United States.” *www.justice.gov*. Accessed Oct. 14, 2022. https://www.justice.gov/usao-ndca/pr/former-mountain-view-resident-christopher-doyon-apprehended-mexico-and-returned-united

23. Picon, Andres. Mar. 10, 2022. “Christopher Doyon, Anonymous hacktivist known as "Commander X" to Plead Guilty to 2010 Santa Cruz Cyber Attack.” *San Francisco Chronicle*. Accessed April 24, 2023. https://www.sfchronicle.com/bayarea/article/Anonymous-hacktivist-to-plead-guilty-to-16993702.php

24. Page, Carly. Dec. 9, 2022. “CommonSpirit Health Says Patient Data Stolen During Ransomware Attack.” *techcrunch.com*. Accessed 1/6/2023. https://techcrunch.com/2022/12/09/commonspirit-health-ransomware-attack-exposed-patient-data/

25. GIbbs, Molly. Oct. 12,2022. “Hartnell College Confirms Ransomware Attack.” *Monterey Daily Herald*. Accessed 10/16/2022. https://www.hartnell.edu/news/2022-news-releases/hc_press_release_111222.html

26. Gooden, Dan. Oct. 3, 2022. “Big data trove dumped after La Unified School District says no to ransomware crooks.” *arstechnica.com*. Accessed 10/16/2022. https://arstechnica.com/information-technology/2022/10/ransomware-crooks-dump-big-data-trove-stolen-from-la-school-district/

27. Liss, Samantha. Jan. 5, 2023. “Patient Sues CommonSpirit Over Ransomware Attack.” *healthcaredive.com*. Accessed 1/6/2023. https://www.healthcaredive.com/news/patient-sues-commonspirit-ransomware-attack-class-action/639710/

28. Blume, Howard. Sep. 21, 2022. “Los Angeles Unified School District Hackers Demand Ransom.” *LA Times*. Accessed 1/6/2023. https://www.govtech.com/security/los-angeles-unified-school-district-hackers-demand-ransom

29. Confidential Grand Jury interview.

30. Confidential Grand Jury document.

31. Confidential Grand Jury interview.

32. Confidential Grand Jury interview.

33. Confidential Grand Jury interview.

34. Confidential Grand Jury interview.

35. Hughes, Owen. Oct. 25, 2022. “Cybersecurity Teams are Reaching Their Breaking Point. We Should All Be Worried.” *https://www.zdnet.com*. Accessed Oct. 25, 2022. https://www.zdnet.com/article/cybersecurity-teams-are-reaching-their-breaking-point-we-should-all-be-worried/
36. Confidential Grand Jury interview.
37. Confidential Grand Jury interview.
38. Confidential Grand Jury interview.
39. Confidential Grand Jury interview.
40. Confidential Grand Jury interview.
41. Confidential Grand Jury interview.
42. Confidential Grand Jury interview.
43. Avast Business Team. Feb. 7, 2020. “How do you manage cybersecurity as a one-person IT team?.” *Avast Blog*. Accessed 1/6/2023. https://blog.avast.com/how-do-you-manage-cybersecurity-as-a-one-person-it-team#
44. Confidential Grand Jury interview.
45. Confidential Grand Jury interview.
46. Confidential Grand Jury interview.
47. Confidential Grand Jury interview.
48. Confidential Grand Jury interview.
49. Confidential Grand Jury interview.
50. Confidential Grand Jury interview.
51. Confidential Grand Jury interview.
52. Confidential Grand Jury interview.
53. Confidential Grand Jury interview.
54. Confidential Grand Jury interview.
55. Confidential Grand Jury document.
56. Confidential Grand Jury interview.
57. Confidential Grand Jury interview.
58. Confidential Grand Jury interview.
59. Confidential Grand Jury interview.
60. Confidential Grand Jury interview.
61. Confidential Grand Jury interview.

62. Confidential Grand Jury interview.
63. Confidential Grand Jury interview.
64. Confidential Grand Jury interview.
65. Confidential Grand Jury interview.
66. Confidential Grand Jury interview.
67. Confidential Grand Jury interview.
68. Confidential Grand Jury interview.
69. Confidential Grand Jury interview.
70. Confidential Grand Jury interview.
71. Confidential Grand Jury interview.
72. Confidential Grand Jury interview.
73. Rufus Coleman. June 23, 2021. “What local governments can do to build better cybersecurity.” *americancityandcounty.com*. Accessed Jan. 5, 2023. https://www.americancityandcounty.com/2021/06/23/what-local-governments-can-do-to-build-better-cybersecurity/
74. no author. no date. “How to Structure your Cybersecurity Program.” *csbs.org*. Accessed Jan. 4, 2023. https://www.csbs.org/cyber-structure
75. Krehel, Ondrej. Apr. 6. 2021. “How Small Towns and Municipalities Can Shore Up Cybersecurity Protocols.” *cpomgazine.com*. Accessed 1/12/2023. https://www.cpomagazine.com/cyber-security/how-small-towns-and-municipalities-can-shore-up-cybersecurity-protocols/
76. Newcombe, Tod. Oct/Nov 2017. “Small Towns Confront Big Cyber Risks.” *govtech.com*. Accessed 1/12/2023. https://www.govtech.com/security/gt-octobernovember-2017-small-towns-confront-big-cyber-risks.html
77. Rose, Ashley. Jan. 11, 2022. “Why Security Awareness Should Begin in the C-Suite.” *DarkReading*. Accessed Jan. 5, 2023. https://www.darkreading.com/careers-and-people/why-security-awareness-training-should-begin-in-the-c-suite
78. no author. no date. “Information Sharing and Analysis.” *cisa.gov*. Accessed Jan. 5, 2023. https://www.cisa.gov/information-sharing-and-awareness
79. Ladin-Sienne, Sari. Oct. 19, 2016. “Six Ways Cities Can Make Cybersecurity a Top Priority.” *Data Smart City Solutions, Harvard.edu*. Accessed 1/12/2023. https://datasmart.ash.harvard.edu/news/article/5-ways-cities-can-make-cybersecurity-a-top-priority-best-practices-from-lea

SANTA CRUZ COUNTY GRAND JURY

Grand Jury <grandjury@scgrandjury.org>

Revised Board of Supervisors Response to 2022-2023 Grand Jury Report

Caitlin Smith <Caitlin.Smith@santacruzcountyca.gov> Tue, Oct 3, 2023 at 2:12 PM

Good Afternoon,

Please see attached for the revised Board of Supervisors response to the 2022-2023 Grand Jury Report "Cyber Threat Preparedness". As you may recall, the original response was approved by the Board on August 8th and this revised response was approved on September 19th.

Best,

Caitlin C. Smith

County Supervisors' Analyst

Santa Cruz County Board of Supervisors

701 Ocean Street, Room 500

Santa Cruz, CA 95060

831-454-2200 main

831-454-3516 direct

caitlin.smith@santacruzcountyca.gov

To email all five members of the Board of Supervisors at once,

please use: boardofsupervisors@santacruzcountyca.gov

Revised Board of Supervisors Response to Grand Jury Report Cyber Threat Preparedness.pdf
249K

County of Santa Cruz

BOARD OF SUPERVISORS

701 OCEAN STREET, SUITE 500, SANTA CRUZ, CA 95060-4069
(831) 454-2200 • FAX: (831) 454-3262 TDD/TTY - Call 711

MANU KOENIG	ZACH FRIEND	JUSTIN CUMMINGS	FELIPE HERNANDEZ	BRUCE MCPHERSON
FIRST DISTRICT	SECOND DISTRICT	THIRD DISTRICT	FOURTH DISTRICT	FIFTH DISTRICT

September 29, 2023

The Honorable Syda Cogliati
Santa Cruz Courthouse
701 Ocean Street
Santa Cruz, CA 95060

RE: Revised Response to the 2022-2023 Grand Jury Report "Cyber Threat Preparedness"

Dear Judge Cogliati:

The purpose of this letter is to formally transmit the revised response of the Santa Cruz County Board of Supervisors to the 2022-2023 Grand Jury Report "Cyber Threat Preparedness".

Sincerely,

ZACH FRIEND, Chair
Board of Supervisors

ZF: cs
Attachment

CC: Clerk of the Board
Santa Cruz County Grand Jury

The 2022–2023 Santa Cruz County Civil Grand Jury

Requires the

Santa Cruz County Board of Supervisors

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 September 19, 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

F1. Santa Cruz County does not have a Cybersecurity Plan, and the absence of a current plan that defines security policies, procedures, and controls required to protect its networks and devices increases the risk of vulnerabilities.

_x_ AGREE

__ PARTIALLY DISAGREE

__ DISAGREE

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

In 2019, the County developed an Incident Response Plan for Cyber events and is working on establishing a more formal Cybersecurity Plan that addresses emerging threats and responses. The County has reached out to the four cities and Santa Cruz Regional 911 (SCR911) to convene a regional Cybersecurity Consortium to take a regional approach to developing Cybersecurity and incident response plans that can be leveraged for the individual needs and requirements of each participating agency. The plans will be completed before or by December 31, 2023

F2. Santa Cruz County does not have a sufficiently detailed Incident Response Plan, indicating they would not be prepared to respond rapidly and effectively in the event of a cyber incident.

_x_ AGREE

__ PARTIALLY DISAGREE

__ DISAGREE

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

In 2019, the County developed an Incident Response Plan for Cyber events and is working on establishing a more formal Cybersecurity Plan that addresses emerging threats and responses. The County is coordinating with the four cities and SCR911 to develop a regional plan that can be modified for the individual needs and requirements of each entity. The plans will be completed before or by December 31, 2023

F3. Santa Cruz County participates in multiple information sharing groups at regional and state levels, although it has only minimal interaction with the cities across Santa Cruz County, degrading their ability to fully understand regional vulnerabilities.

__ AGREE

_x_ PARTIALLY DISAGREE

__ DISAGREE

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

The County has reached out in the past to inform cities of Cybersecurity resources, such as the Northern California Regional Intelligence Center and Urban Areas Security Initiative Program. A more formal information sharing has been established through a regional Cybersecurity Consortium to promote and encourage communication and resources. The Consortium began meeting on June 12, 2023.

Recommendations

R1. Santa Cruz County should prepare and implement a Cybersecurity Plan by the end of 2023, ensuring that city officials and all staff are well aware of the plan details, their responsibilities, and associated policies. (F1)

__	**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 County has reached out to the four cities and SCR911 to convene a regional Cybersecurity Consortium to take a regional approach to developing Cybersecurity and incident response plans that can be leveraged for the individual needs and requirements of each participating agency. The plans will be completed before or by December 31, 2023

R2. By the end of 2023, the county should revise and expand its Incident Response Plan to clearly delineate the steps it will take in response to a cyber-attack, the responsibilities of identified officials, and the coordination required with state and federal officials for each type and level of cyber-attack. A detailed plan is a requirement for continuity of county operations in a cyber incident. (F2)

__	**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 County is coordinating with the four cities and SCR911 to develop a regional plan that can be modified for the individual needs and requirements of each entity. The plan will provide clear delineated steps for the County to respond to a cyber-attack. The FY 2023-24 budget funds a position to establish a dedicated security analyst that will take on this work on behalf of the County. This will be completed by December 31, 2023

R3. The County's information sharing efforts should be expanded to ensure fulsome information sharing across all government entities in the county, specifically Santa Cruz, Watsonville, Scotts Valley, and Capitola, by the end of 2023. A simple schedule of monthly meetings would permit regular sharing of possible threats, TTPs seen across the county, and information learned from outside organizations such as the Cal-CSIC. (F3)

_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:

On June 12, 2023, a regional Cybersecurity group was formally convened. The focus of the group will be to develop the Cybersecurity policy and plans, along with an incident response plan as noted above. The Santa Cruz Cybersecurity Consortium will meet regularly on at least a monthly basis going forward to look at iterative changes needed for policy and discuss regional approaches to mitigating emerging Cybersecurity threats.

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,

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.

SANTA CRUZ COUNTY GRAND JURY

grandjury <grandjury@scgrandjury.org>

City of Watsonville Response to Grand Jury Report

'Irwin Ortiz' via Santa Cruz Grand Jury <grandjury@scgrandjury.org> Thu, Sep 7, 2023 at 12:16 PM
Reply-To: Irwin Ortiz <irwin.ortiz@watsonville.gov>
To: "grandjury@scgrandjury.org" <grandjury@scgrandjury.org>, "syda.cogliati@santacruzcourt.org" <syda.cogliati@santacruzcourt.org>

Dear Grand Jury and Honorable Judge Cogliati,

I hope this email finds you in good health. At our August 29, 2023, City Council Meeting, the City Council unanimously approved the response packet to the Grand Jury Report received by the City. We thank you for your patience and your good work. Please see the response packet as approved by our City Council attached to this email.

If you have any questions, please fee free to contact me.

Irwin I. Ortiz, CMC
City Clerk

Office: (831) 768-3040
Direct: (831) 768-3048
Fax: (831) 761-0736

275 Main St, Suite 400, Watsonville, CA 95076

Irwin I. Ortiz, City Clerk
City Clerk's Office (831) 768-3048
275 Main Street, Suite 400, Watsonville, CA 95076
FAX: 831-761-0736
E-mail: irwin.ortiz@watsonville.gov
Open Monday - Friday 8:00 AM to 5:00 PM

**Public Records Requests (PRR) submitted via email, fax, USPS, or dropoff after 5:00 p.m. on a business day, Saturday, Sunday, holidays, will be processed as received on the next open business day. The 10-day response period begins when the PRR is received.
Please note: Our website domain and emails have changed on 4/17/23 to watsonville.gov

Item 9.b. Civil Grand Jury Housing & Cyber Response.pdf
1178K

Agenda Report

MEETING DATE: **Tuesday, August 29, 2023**

TO: **City Council**

FROM: **COMMUNITY DEVELOPMENT DIRECTOR MERRIAM**
INNOVATION & TECHNOLOGY DIRECTOR GILL

THROUGH: **CITY MANAGER MENDEZ**

SUBJECT: **CITY RESPONSE TO THE SANTA CRUZ COUNTY CIVIL GRAND JURY'S INVESTIGATION OF HOUSING OUR WORKERS AND CYBER THREAT PREPAREDNESS**

RECOMMENDED ACTION:

It is recommended that the City Council by Motion approve the response packets prepared for the 2022-2023 Santa Cruz County Grand Jury's Investigation on two specific topics: 1) Cyber Threat Preparedness: Phishing and Passwords and Ransomware, Oh My! and 2) Housing Our Workers: Essential Workers Need Affordable Housing!

BACKGROUND:
Each year the Santa Cruz Civil Grand Jury (Grand Jury) issues reports and requires certain agencies and departments to respond. In many cases, the respondents are department heads and administrators. In other cases, the respondent is an agency itself. This year the Grand Jury is requiring a response to the reports on Cyber Threat Preparedness and Housing Our Workers from the Watsonville City Council.

DISCUSSION:
The Santa Cruz County Civil Grand Jury prepared two reports addressing issues in the Watsonville community and requested that the Council prepare responses to several findings and recommendations in each report. The County and all four cities within the County received these reports and were compelled to respond.

The Grand Jury looks for contact information, budget data, policies, and procedures, etc. to conduct their investigation. The reports contain findings by the 2022-2023 Grand Jury and offer recommendations for consideration and ongoing improvement of operations.

Both Grand Jury reports are included as Attachments 1 through 4; below is a summary of the areas of interest for each issue reviewed and some highlights of the recommendations made by the Grand Jury:

Cyber Threat Preparedness: Phishing and Passwords and Ransomware, Oh My!:
This report sought to evaluate the overall level of preparedness for a cyber incident against the county or city networks. It performed research across federal and state resources, top cyber security sites, and reputable media sources to build an understanding of the current cyber landscape and a foundation for cyber preparedness. Based on interviews with subject matter experts and resources available from the Cybersecurity and Infrastructure Security Agency (CISA) at the Department of Homeland Security (DHS) and the National Institute of Standards and Technology (NIST) in the U.S. Department of Commerce, the jury delineated key elements of strong cyber hygiene, the security and health of the information systems, and best practices for local governments. They recommend that the cities and county hire staff that focus specifically on cybersecurity, develop a cybersecurity plan, and develop an incident response plan. With the resourcing of the IT department that began a couple of years ago, staff have been proactively working to make improvements system wide. One of the areas has been an increased focus on security to protect against cyber threats. For example, the City recently implemented a double authentication process and as is articulated in the report while some of the recommendations are not yet fully implemented, they are underway and many will be implemented over this current 2-year budget cycle.

Housing Our Workers: Essential Workers Need Affordable Housing!
This report investigated the reasons that housing scarcity and cost has increased over the last 5 years, and its impact on Santa Cruz County works that earn between $35,000-$99,999 per year. Specifically, the Grand Jury considered:

- What affordable housing options are available in Santa Cruz County to support middle class workers?
- Are employers offering housing support to their employees?
- What can local city and county planning departments do to provide more housing for these workers?
- What changes are needed in the planning and permit process to make it easier to build more workforce housing in our cities and unincorporated areas?
- How can local jurisdictions leverage recent state bills and initiatives to encourage more housing here?
- How can local agencies work together to help support housing for local workers?
- What changes are needed to plan for the future housing needs of our workforce?
- What is UCSC doing to help house its students, faculty, and staff?

The Grand Jury found that Watsonville should have been more proactive in implementing state regulatory changes, however Watsonville was also commended for being the jurisdiction that continued to build housing in years that other jurisdictions were not.

The Grand Jury found that local jurisdictions should implement local preference policies for both housing projects and construction. The City of Watsonville does have a local preference policy in for-sale ownership projects by way of a lottery system in which local residents or workers get additional entries into the lottery to purchase affordable units. We do not currently have a local preference policy for rental projects. Further, the City adopted

a local hiring procedure (WMC 7-15) in 2002 that requires contractors who enter into contracts for Public Works projects over $600,000.

The Grand Jury recommended that the City of Watsonville reestablish regular meetings with planners from all agencies in the county to regularly meet to share ideas on housing development and develop joint projects. In addition, it was recommended that Watsonville give local preference to those contractors developing affordable housing.

The answers to these Findings and Recommendations are listed in Attachment 4.

STRATEGIC PLAN:
The response to the Grand Jury 2023 report aligns with Goal 7 of the 2023-2025 Strategic Plan: Efficient and High Performing Government.

FINANCIAL IMPACT:
There is no financial impact associated with filing responses to the Grand Jury report.

ALTERNATIVE ACTION:
The Council may choose not to approve the Response Packet, or to modify the responses, however the responses are due to the Grand Jury no later than August 31, 2023.

ATTACHMENTS AND/OR REFERENCES (If any):
1. Report: “Cyber Threat Preparedness: Phishing and Passwords and Ransomware, Oh My!”
2. Watsonville response to “Cyber Threat Preparedness: Phishing and Passwords and Ransomware, Oh My!”
3. Report: “Housing Our Workers: Essential Workers Need Affordable Housing!”
4. Watsonville response to “Housing Our Workers: Essential Workers Need Affordable Housing!”

The 2022–2023 Santa Cruz County Civil Grand Jury

Requires the

Watsonville 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 29, 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

F10. After recently expanding its IT Department, the City of Watsonville has improved its IT functions although it does not yet allocate sufficient resources to cybersecurity.

_X_ AGREE

__ PARTIALLY DISAGREE

__ DISAGREE

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

F11. The City does not have an individual whose primary responsibility is cybersecurity for the city networks, leaving cybersecurity oversight to the IT Director–along with a multitude of other IT responsibilities–and lowering the priority for cybersecurity measures.

_X_ AGREE

__ PARTIALLY DISAGREE

__ DISAGREE

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

F12. Watsonville does not have a Cybersecurity Plan that defines security policies, procedures, and controls required to protect its networks and devices, a situation that increases the risks of vulnerabilities.

_X_ AGREE

__ PARTIALLY DISAGREE

__ DISAGREE

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

F13. Watsonville does not have an Incident Response Plan that provides detailed information on how to respond to an attack, suggesting the City would not be able to respond rapidly and effectively to a cyber attack.

_X_ AGREE

__ PARTIALLY DISAGREE

__ DISAGREE

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

F14. Watsonville participates in some regional information sharing forums, but it does not have the resources to expand its participation or tap into state-level information sharing, thus forfeiting valuable best practices and cyber threat information.

_X_ AGREE

__ PARTIALLY DISAGREE

__ DISAGREE

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

Recommendations

R10. Watsonville should conduct an evaluation of its recently expanded IT Department, critical IT upgrades, and the status of cybersecurity measures by the end of 2023. Based on this assessment, the City should allocate existing or newly identified resources to ensure cybersecurity is adequately addressed going forward. (F10)

__	**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:

A cybersecurity remediation team has been formed and is currently identifying all cybersecurity elements that require remediation. The team is creating a remediation plan as items are identified. If approved in the fy24/25 budget, a position will be reclassified to focus on cybersecurity as a major job function.

R11. Given the size of Watsonville, the City should have a dedicated position for cybersecurity by the end of 2023, to ensure adherence to best practices, mitigation of potential threats, and education of city staff and leadership. (F11)

__ **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:

If approved in the fy24/25 budget, a position will be reclassified to focus on cybersecurity as a major job function.

R12. By early 2024 or sooner, Watsonville should prepare and implement a Cybersecurity Plan that addresses all of the best practices for strong cyber hygiene. (F12)

__ **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:

Funds for professional services are identified in the FY24/25 budget to assist with plan creation. In addition, the County of Santa Cruz is leading an effort with the City of Watsonville, the City of Capitola, the City of Scotts Valley, and the City of Santa Cruz to create a cybersecurity plan that will support both cities and the county. The Cybersecurity Plan will be substantially completed by Spring 2024.

R13 By early 2024 or sooner, Watsonville should prepare and implement an Incident Response Plan with sufficient detail to serve as a guide in the event of a cyber attack. (F13)

__ **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:

Funds for professional services are identified in the FY24/25 budget to assist with plan creation. In addition, the County of Santa Cruz is leading an effort with the City of Watsonville, the City of Capitola, the City of Scotts Valley, and the City of Santa Cruz to create an incident response plan that will support both cities and the county. The incident response plan will be substantially completed by early 2024.

R14. Upon completion of IT structural upgrades and a higher level of cyber maturity, and by the end of 2023, Watsonville should participate in local, regional, and state information sharing initiatives. (F14)

__ **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:

Along with participation in the NCRIC (regional) and MS-ISAC (national), the city will subscribe to CAL-CSIC (state) information sharing. Watsonville will also participate in a quarterly cybersecurity focused discussion led by the County of Santa Cruz, with the City of Santa Cruz, the City of Capitola, and the City of Scotts Valley (local) as additional participants.

SANTA CRUZ COUNTY GRAND JURY

grandjury <grandjury@scgrandjury.org>

Scotts Valley Response - Cyber Threat Preparedness

'Cathie Simonovich' via Santa Cruz Grand Jury <grandjury@scgrandjury.org> Thu, Aug 3, 2023 at 9:14 AM

Reply-To: Cathie Simonovich <csimonovich@scottsvalley.gov>
To: "Syda.Cogliati@santacruzcourt.org" <Syda.Cogliati@santacruzcourt.org>, "grandjury@scgrandjury.org" <grandjury@scgrandjury.org>
Cc: Mali LaGoe <mlagoe@scottsvalley.gov>, Stephanie Hill <shill@scottsvalley.gov>

Dear Honorable Judge Cogliati and Members of the Santa Cruz County Grand Jury,

We have attached the completed response packet for the report titled *Cyber Threat Preparedness - Phishing and Passwords and Ransomware, Oh My!* This report was approved by the Scotts Valley City Council at the regular public meeting held on August 2, 2023.

Please confirm receipt of the report.

Best regards,

Cathie Simonovich
City Clerk

City of Scotts Valley
1 Civic Center Drive
Scotts Valley, CA 95066
csimonovich@scottsvalley.gov
Phone: 831-440-5608

NOTE: ***My regular work schedule is Tuesday through Friday from 7:00 AM to 5:30 PM.***

2023-3dR_Cyber_ScottsValleyCC_Packet.pdf
252K

The 2022–2023 Santa Cruz County Civil Grand Jury

Requires the

Scotts Valley 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 2, 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

F15. Although Scotts Valley's managed service provider is very knowledgeable and capable of providing cybersecurity services, there is no single city official with cybersecurity oversight, potentially leading to a poor understanding of the threats and an inadequate response to a cyber attack.

__ AGREE

__ PARTIALLY DISAGREE

_X_ DISAGREE

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

We agree that the Scotts Valley managed service provider is very knowledgeable and capable of providing cybersecurity services. In addition, the Administrative Services Director overseas the City's managed services provider contract including cybersecurity services. The Administrative Services Director and City Manager meet at least monthly with the managed service provider where reports of phishing, cyber incidents and training statistics are reviewed and discussed. In the event of an immediate threat or incident, there is immediate communication between the managed service provider, City Manager, and Administrative Services Director. The City Manager and Administrative Services Director have an appropriate understanding of the potential cybersecurity threats and the managed service provider ensures the City has the tools in place to respond to a cyber attack. Therefore we disagree that our organizational structure as the potential to lead to a poor understanding or inadequate response to a cyber attack.

F16. Scotts Valley does not have a current Cybersecurity Plan that defines security policies, procedures, and controls required to protect its networks and devices, potentially increasing the risks of vulnerabilities.

_X_ AGREE

__ PARTIALLY DISAGREE

__ DISAGREE

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

F17. Scotts Valley does not have a current Incident Response Plan, which could exacerbate the effects of a cyber incident such as increase the time a network is unavailable or raise the potential financial costs of a resolution.

__ **AGREE**

_X_ **PARTIALLY DISAGREE**

__ **DISAGREE**

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

Although the City does not have a written Incident Response Plan, we have reporting channels in place in the event of a cyber incident and access to a cybersecurity response consultant via our risk management insurance pool who is under contract to provide cybersecurity incident response and maintains plans accordingly.

F18. Scotts Valley does not participate in any cybersecurity information sharing groups to enhance best practices, rather they depend on their contractor to stay informed, which makes the City last to know of critical cyber threats.

__ **AGREE**

_X_ **PARTIALLY DISAGREE**

__ **DISAGREE**

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

Via the City's insurance pool, MBASIA, cybersecurity information is shared among the 10 city members and our contracted risk management consultants. In addition, our managed service provider stays informed of the cybersecurity environment and alerts the City of potential threats. The City's relationship with a contracted managed service provider does not make the City any less informed or more vulnerable. In fact the team we are served by is more informed and provides a broader skillset, knowledge base and faster response times than we could expect if the contract was replaced by 1-2 City staff. That being said, there are always more opportunities for information sharing and collaboration which the City, via it's managed service provider, will pursue.

Recommendations

R15. By mid-2023, Scotts Valley should assign a city official as the lead for cybersecurity for the city. This individual should oversee the contractor's performance in cybersecurity and ensure city leaders are well informed on emerging threats, cybersecurity challenges, and information provided from regional and state entities. (F15)

__ **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)

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

Required response explanation, summary, and timeframe:

The City already oversees the managed service provider's performance via the Administrative Services Director and City Manager.

R16. Working with its IT contractor, by Fall 2023, Scotts Valley should write and implement a Cybersecurity Plan that is shared with all city officials to demonstrate comprehensive security measures and executive-level cyber threat awareness. (F16)

__ **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 will work with the managed service provider in developing a written Cybersecurity Plan by 11/30/2023. The plan will be shared with those who need to know and have a role in implementing security measures. The plan will not be publicly shared or available due to its sensitive nature.

R17. By Fall 2023, Scotts Valley should write an Incident Response Plan that clearly delineates the steps it will take in response to a cyber attack, the responsibilities of identified officials, and the coordination required with state and federal officials for each type and level of cyber attack. (F17)

__ **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 will work with our managed service provider and cyber insurance consultant to develop a written Incident Response Plan by 11/30/2023.

R18. Scotts Valley should participate in local, regional, and state cybersecurity organizations for information sharing by the end of 2023. (F18)

__	**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 will work with the managed service provider in identifying and selecting appropriate organizations to share cybersecurity information with by 11/30/2023.

SANTA CRUZ COUNTY GRAND JURY

Grand Jury <grandjury@scgrandjury.org>

Non-compliant response received

Moss, Julia <jmoss@ci.capitola.ca.us> Fri, Sep 15, 2023 at 1:18 PM
To: "grandjury@scgrandjury.org" <grandjury@scgrandjury.org>, Syda Cogliati <Syda.Cogliati@santacruzcourt.org>

Good Afternoon,

Please see attached updated response from the City of Capitola City Council. Please confirm receipt of this email.

Julia Moss

City Clerk - City of Capitola

831.475.7300 x228

2 attachments

Cyber - Minutes from July 27th.pdf
609K

2023-3eR_Cyber_CapitolaCC_Packet_edits.pdf
219K

City of Capitola
City Council Meeting Minutes
Thursday, July 27, 2023 – 6:00 PM

City Council Chambers
420 Capitola Avenue, Capitola, CA 95010

Mayor: Margaux Keiser
Vice Mayor: Kristen Brown
Council Members: Yvette Brooks, Joe Clarke, Alexander Pedersen

Closed Session – 5 PM

i. CONFERENCE WITH LABOR NEGOTIATORS (Gov. Code § 54957.6)
Negotiator: Chloé Woodmansee, Assistant to the City of Manager
Employee Organizations: Association of Capitola Employees, Police Officers Association, Mid-Management Employees, Confidential Employees, Police Captains, and Management

ii. CONFERENCE WITH LEGAL COUNSEL—LIABILITY CLAIMS (Gov. Code § 54956.95)
1) Graciela Cardiel
Claim against the City of Capitola

iii. CONFERENCE WITH LEGAL COUNSEL - ANTICIPATED LITIGATION (Gov. Code § 54956.9)
Initiation of litigation pursuant to paragraph (4) of subdivision (d) of Section 54956.9: one case

Regular Meeting of the Capitola City Council – 6 PM

1. Roll Call and Pledge of Allegiance

The meeting was called to order at 6:00 PM. In attendance: Council Members Brooks, Clarke, Pedersen, and Mayor Keiser. Absent: Vice Mayor Brown

2. Additions and Deletions to the Agenda - *None*

3. Report on Closed Session – *The City Council met and discussed three items on the Closed Session Agenda. No reportable action was taken.*

4. Additional Materials

A. Updated Attachments for Item 7F

B. Correspondence Received - Item 8C (*2 emails*)

C. Correspondence Received - Item 8E (*3 emails*)

D. Correspondence Received - Item 8F (*3 emails*)

5. Oral Communications by Members of the Public - *None*

6. Staff / City Council Comments

- *Police Chief Dally reminded the public of National Night Out on August 1st from 5-7 PM.*
- *Council Member Clarke commended the Random Acts of Capitola Kindness group for their efforts on the Depot Hill fence repair.*

7. Consent Items

A. City Council Meeting Minutes

Recommended Action: Approve the June 22, 2023, City Council meeting minutes.

B. City Check Registers
Recommended Action: Approve check registers dated June 23, 2023, and July 7, 2023.

C. Liability Claim of Graciela Cardiel
Recommended Action: Reject liability claim.

D. Grand Jury Response – Cyber Security
Recommended Action: Approve the responses to the Grand Jury Report and direct the City Clerk to submit the completed response packet pursuant to California Penal Code Section 933.05.

E. Grand Jury Response – Housing our Workers
Recommended Action: Approve the responses to the Grand Jury Report and direct the City Clerk to submit the completed response packet pursuant to California Penal Code Section 933.05.

F. Jade Street Park Universally Accessible Playground Fundraising Partnership
Recommended Action: 1) Authorize the City Manager to execute a Memorandum of Understanding with the Friends of Santa Cruz County Parks for a fundraising campaign and administration of donations for the Jade Street Park Universally Accessible Playground Project; and 2) approve an administrative policy regarding the Universally Accessible Playground at Jade Street Park Donor Recognition.

G. Plein Air Public Art Prize Amount
Recommended Action: Approve the Art & Cultural Commission recommendation to increase the Plein Air Public Art Festival Competition prize amount from $1,500 to $1,800 for first place and from $800 to $1,000 for second place.

Motion to adopt the Consent Calendar: Council Member Clarke
Seconded: Council Member Brooks
Voting Yea: Council Members Brooks, Clarke, Pedersen and Mayor Keiser
Absent: Vice Mayor Brown

8. General Government / Public Hearings

A. State Budget Update from Senator John Laird

Senator John Laird provided a presentation on the State of California Budget.

B. Children and Youth Bill of Rights
Recommended Action: Adopt a resolution adopting the City of Capitola Children and Youth Bill of Rights.

Deputy City Clerk Westly presented the staff report.

Council Member discussion included an overview of the partnership between the City and the Children's Network and Youth Action Network.

Motion to adopt the resolution adopting the Capitola Children and Youth Bill of Rights with direction to staff to research the addition of a $2,000 stipend for youth participation on City advisory boards: Council Member Brooks
Seconded: Council Member Clarke
Voting Yea: Council Members Brooks, Clarke, Pedersen and Mayor Keiser
Absent: Vice Mayor Brown

C. Jade Street Park UA Playground Project
Recommended Action: Approve the Final Conceptual Design for the Jade Street Park Universally Accessible (UA) Playground Project.

Public Works Director Kahn and Todd from Verde Design presented the staff report.

Public Comments:

- ***Brenda, community member, spoke in support of the UA Playground Project.***
- ***Dan Hastley, County Park Friends, spoke in support of the UA Playground Project.***
- ***Lisa Duran, Capitola Aptos Rotary Member, spoke in support of the UA Playground Project.***

Council Member discussion included thanks for the Santa Cruz County Park Friends for their fundraising efforts, and encouragement to the community to donate to the fundraiser.

Motion to approve the Final Conceptual Design: Council Member Brooks
Seconded: Council Member Pedersen
Voting Yea: Council Members Brooks, Clarke, Pedersen and Mayor Keiser
Absent: Vice Mayor Brown

D. Community Center Renovation Project – Budget Update
Recommended Action: 1) Receive update on external funding sources for the Community Center Renovation Project; and 2) authorize Amendment 1 to the Professional Services Agreement with Boone Low Ratliff Architects in the amount of $374,000 for final design documents, bidding support, and construction administration for the Community Center Renovation Project.

Public Works Director Kahn presented the staff report.

Council Member discussion included clarification on funding sources and timelines.

Motion to authorize Amendment 1 to the Agreement with Boone Low Ratliff Architects: Council Member Pedersen
Seconded: Council Member Clarke
Voting Yea: Council Members Brooks, Clarke, Pedersen and Mayor Keiser
Absent: Vice Mayor Brown

E. Capitola Wharf Enhancement Project Preliminary Conceptual Design
Recommended Action: Direct staff to prepare a final concept plan, for consideration by the City Council on August 24, 2023, for the Capitola Wharf Enhancement Project (CWEP).

Public Works Director Kahn presented the staff report.

Public Comments:

- ***Community member requested clarification on the conceptual design.***
- ***Gerry Jensen, CWET, thanked City staff and Wharf to Wharf staff for their collaboration efforts.***
- ***Skip Allen, community member, voiced concerns about enhanced lighting in the conceptual design.***

Council Members expressed thanks to CWET for their efforts, an interest in the addition of a kiosk element, and additional outreach for volunteer opportunities.

Direction provided to staff to prepare a Final Conceptual Design with the addition of a kiosk: Council Member Brooks
Seconded: Council Member Clarke
Voting Yea: Council Members Brooks, Clarke, Pedersen and Mayor Keiser
Absent: Vice Mayor Brown

F. Capitola Road Pavement Rehabilitation Project
Recommended Action: Approve the plans, specifications, and construction budget of $1,700,000 for the Capitola Road Pavement Rehabilitation Project; adopt a resolution amending the FY 2023-24 budget; and authorize the Department of Public Works to advertise for construction bids.

Public Works Director Kahn presented the staff report.

The City Council requested that staff provide an update on the ADA recommendations for this project and associated electrical improvements.

Public Comments:

- ***Marianne Mahern, resident, requested further consideration of ADA accommodations in the pavement plan.***

Motion to approve the plans, specifications, and budget for the Road Pavement Rehabilitation Project and adopt the resolution: Council Member Brooks
Seconded: Council Member Clarke
Voting Yea: Council Members Brooks, Clarke, Pedersen and Mayor Keiser
Absent: Vice Mayor Brown

G. City Council Appointments to City Advisory Bodies
Recommended Action: Appoint members of the public to the City of Capitola Arts and Cultural Commission and Historical Museum Board.

City Clerk Moss presented the staff report.

Motion to appoint Jennifer Major to the Arts and Cultural Commission to a term expiring 12/31/2024 and Brian Legakis to the Historical Museum Board to a term expiring 6/30/2024: Council Member Clarke
Seconded: Council Member Pedersen
Voting Yea: Council Members Brooks, Clarke, Pedersen and Mayor Keiser
Absent: Vice Mayor Brown

9. Adjournment – *The meeting was adjourned at 7:36 PM to the next regularly scheduled meeting on August 24, 2023, at 6:00 PM.*

ATTEST: Margaux Keiser, Mayor

Julia Moss, City Clerk

The 2022–2023 Santa Cruz County Civil Grand Jury

Requires the

Capitola 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 July 27, 2023, Updated on September 1, 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

F19. With one individual responsible for IT services, Capitola does not allocate sufficient resources to cybersecurity, a status that could lead to poor cyber knowledge and unnecessary vulnerabilities.

__ **AGREE**

__ **PARTIALLY DISAGREE**

_X_ **DISAGREE**

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

The City of Capitola allocates sufficient resources to cybersecurity. The City employs an Information Systems Specialist in the City Manager Department and holds a contract with Exceedio for 24-hour technical support, analysis, and security.

F20. The City of Capitola does not have a robust cybersecurity training program, nor does it conduct phishing tests or routinely remind employees to adhere to cybersecurity measures during potential periods of increased threats.

__ **AGREE**

X__ PARTIALLY DISAGREE

__ **DISAGREE**

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

The City is currently working to address the need for robust employee cybersecurity training. At present, the following is in place:
1. Capitola Police Department mandates twice-annual security awareness training for their IT, Captain & Chief, Officers, and Records Staff, as well as Public Works staff, the Volunteers in Policing (VIPs), and cleaning staff.
2. All City employees are required to complete “Email and Messaging Safety” training on an annual basis.

The City is developing new additions to the training plan, such as:
1. The City’s Information Systems Specialist is developing regular phishing tests to be sent to all employees on a rolling basis, with further help and training available to those employees who ‘fail’ phishing tests.
2. The City’s Information Systems Specialist is implementing mandatory cyber security training as a part of New Employee Onboarding that must be completed prior to new employees’ gaining access to the City’s network, shared files, internet, and email.

F21. The City of Capitola does not have a Cybersecurity Plan to address cybersecurity measures city wide, suggesting the city is not adequately mitigating the potential impact of cyber incidents.

__ **AGREE**

__ **PARTIALLY DISAGREE**

_X_ **DISAGREE**

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

Capitola Police Department has adopted Policy Section 806.11 regarding Information Technology and Cybersecurity.

The City has a functioning cybersecurity plan that addresses security concerns and outlines a response plan to a security breach. Staff is also working with the Santa Cruz County Cyber Security Consortium to draft a more comprehensive Cybersecurity Plan template that can be modified for each jurisdiction.

F22. The City of Capitola does not have an Incident Response Plan, which could exacerbate the effects of a cyber incident such as increase the time a network is unavailable or raise the potential financial costs of a resolution.

__ **AGREE**

__ **PARTIALLY DISAGREE**

_X_ **DISAGREE**

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

The City has a Cyber Attack Response plan in place. The plan is modified and updated annually by the Information Systems Specialist.

F23. Capitola does not participate in any cyber-focused information sharing groups, nor does it take advantage of state and federal resources designed to assist small cities with mitigating cyber attacks, thereby forfeiting opportunities to learn best practices and raise their cyber awareness.

__ **AGREE**

__ **PARTIALLY DISAGREE**

_X_ **DISAGREE**

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

The City's Information Systems Specialist participates in:

1. Cyber threat meetings sponsored by Alverez Technology Group
2. NCRIS.ca.gov Regional Information Center meetings regarding cyber threats
3. MISAC.org
4. Santa Cruz County Cyber Security Consortium

Recommendations

R19. By Fall 2023, Capitola should hire a full-time IT Director to replace the IT Director who departed in mid-2022. The IT Director should oversee and expand IT services, including those of the consulting company, and lead cybersecurity initiatives. (F19)

__ **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)

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

Required response explanation, summary, and timeframe:

The City has never employed an IT Director and does not intend to create/fill such a position.

R20. The City should develop a more robust cybersecurity training and phishing testing program for all employees by Fall 2023 or earlier. (F20)

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 is currently working to address the need for robust employee cybersecurity training:
1. Capitola Police Department mandates twice-annual security awareness training for their IT, Captain & Chief, Officers, Records Staff, as well as Public Works staff, the Volunteers in Policing (VIPs), and cleaning staff.
2. All employees are required to complete “Email and Messaging Safety” training on an annual basis.
3. The City’s Information Systems Specialist is developing regular phishing tests to be sent to all employees on a rolling basis, with further help and training available to those employees who ‘fail’ phishing tests.
4. The City’s Information Systems Specialist is considering including mandatory cyber security training to New Employee Onboarding that must be completed prior to new employees’ gaining access to the City’s network, shared files, internet, and email.

R21. Capitola should establish and implement a Cybersecurity Plan by the end of 2023. Several resources exist to provide a foundation or templates for these plans including NIST Guidelines, CISA resources, and Cal-CSIC guidance. (F21)

__	**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 of Capitola is working with regional entities as a member of the newly formed Santa Cruz County Cyber Security Consortium. One of the group's main goals is to develop a Cyber Security Plan that can be modified for each individual organization. Staff anticipates this will be completed by November 30, 2023.

R22. By Fall 2023 Capitola should prepare an Incident Response Plan that provides detailed guidance for a city response to a cyber attack. (F22)

__	**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 of Capitola is working with the regional entities as a member of the newly formed Santa Cruz County Cyber Security Consortium. One of the group's main goals is to develop a Cyber Security Plan, including an Incident Response Plan, that can be modified for each individual organization. Staff anticipates this will be completed by November 30, 2023.

R23. When appropriately resourced to monitor cyber threats, and by the end of 2023, Capitola should participate in regional cybersecurity information sharing groups, to gain valuable information to best protect the City. (F23)

_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 Information Systems Specialist currently participates in the regional cybersecurity information-sharing groups listed below and will continue to do so.

1. Santa Cruz County Cyber Security Consortium
2. Cyber threat meetings sponsored by Alverez Technology Group
3. NCRIS.ca.gov Regional Information Center
4. MISAC.org

R24. By mid-2023, Capitola city management should raise the priority it assigns to cybersecurity and demonstrate a recognition of their role in ensuring the security of the City's information networks.(F19–F23)

_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 Manager Department has increased prioritizing Information Technology and cybersecurity by:

1) Budgeting $250,000 towards information technology and cyber security
2) Joining the Santa Cruz County Cyber Security Consortium
3) Increasing employee training, for example with an annual Email and Messaging Safety training and more in-depth Anti-phishing training
4) Drafting a more comprehensive Cybersecurity Plan template with the assistance of the SCC Cyber Security Consortium