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.

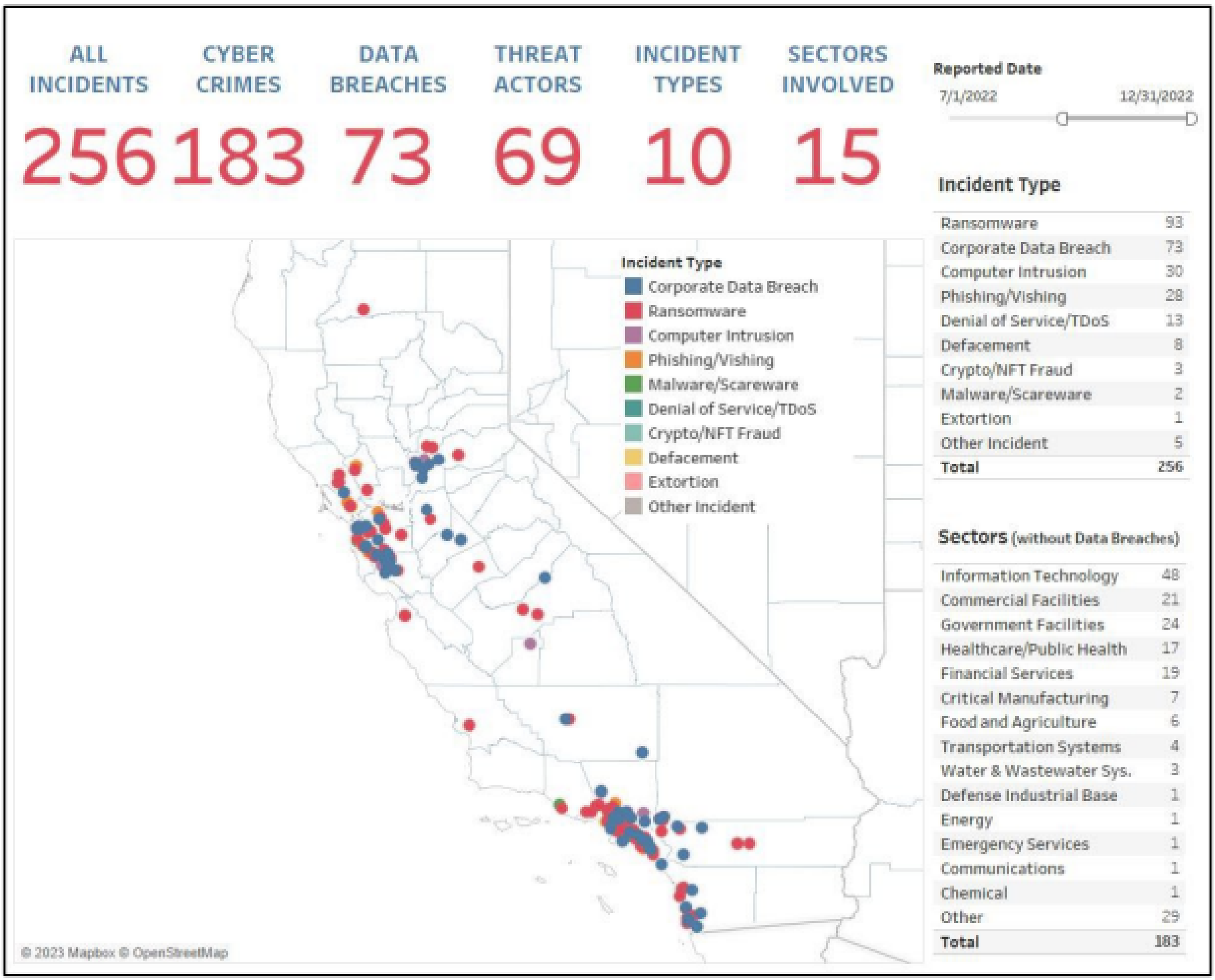
Table of Contents

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]



ALL INCIDENTS	CYBER CRIMES	DATA BREACHES	THREAT ACTORS	INCIDENT TYPES	SECTORS INVOLVED
256	183	73	69	10	15

Reported Date

7/1/2022 12/31/2022

Incident Type

Ransomware	93
Corporate Data Breach	73
Computer Intrusion	30
Phishing/Vishing	28
Denial of Service/TDoS	13
Defacement	8
Crypto/NFT Fraud	3
Malware/Scareware	2
Extortion	1
Other Incident	5
Total	256

Sectors (without Data Breaches)

Information Technology	48
Commercial Facilities	21
Government Facilities	24
Healthcare/Public Health	17
Financial Services	19
Critical Manufacturing	7
Food and Agriculture	6
Transportation Systems	4
Water & Wastewater Sys.	3
Defense Industrial Base	1
Energy	1
Emergency Services	1
Communications	1
Chemical	1
Other	29
Total	183

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_AIVNxXUAR2n8AI7EAAYASAAEgJH9PD_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