2021–2022 San Joaquin County Grand Jury

San Joaquin County and Its Seven Cities: Cybersecurity: Local Defense Against a Global Threat Case #0321

Summary

We hear reports on a daily basis of cyberattacks occurring around the world. These attacks are becoming increasingly sophisticated, disruptive and expensive. Attacks on government agencies can disrupt essential services, crippling communities. Agencies small and large are equally vulnerable. There is an ever-growing demand for stolen data in an underground market. Compromise of information has proven to be a serious threat on the cyber battleground, both domestically and internationally. Bad actors hack intelligence, media and essential service systems. Other disasters such as floods, fires, storms or prolonged power outages can interrupt essential services if providers' information systems are not adequately secure. According to one expert witness interviewed by the 2021-2022 Grand Jury, "World War III will be fought in cyberspace, not on the battlefield."

Grand Jury members are not technical experts but sought to understand the cybersecurity landscape and local governments' management of their cybersecurity risks and vulnerabilities. In this investigation of information security of San Joaquin County and its seven cities, the 2021-2022 Grand Jury made a "point in time" assessment of each entity's Information Systems Department (ISD), focusing primarily on cybersecurity. The Grand Jury considered nine elements of any ISD and, through research of relevant literature and input from industry experts, established an expected standard for each of those elements. The Grand Jury then evaluated each of the agencies with respect to those expectations.

The Grand Jury concluded that San Joaquin County (SJC) has mature and robust security policies and systems. The County's security architecture provided a model in evaluating each city's systems. The Grand Jury determined that Escalon, Lodi and Stockton met a lay person's expectations for cybersecurity but were lacking either a formal Business Continuity Plan (BCP) or Disaster

Preparedness Plan (DPP). Lathrop, Manteca and Tracy were found to have adequate security systems in place but lack documented plans for both Business Continuity and Disaster Preparedness. Ripon was found to-need improvement in meeting several of the Grand Jury's expectations, with lack of personnel being their greatest challenge.

The Grand Jury recommends that the County and affected cities:

- develop, adopt and implement a Business Continuity Plan;
- develop, adopt and implement an IT Disaster Preparedness Plan;
- remedy specific cybersecurity risks found in this investigation; and
- the City of Ripon undergo a data system security review by an expert third party to assess the City's IT systems and protocols.

The Grand Jury recognizes that cybersecurity is a dynamic process, a continually moving target which needs constant monitoring and updating.

Glossary

- **Access:** The ability and means to communicate with or otherwise interact with a system; to use system resources to manage information; to gain knowledge of the information the system contains; to control system components and functions.
- **Actor, bad actor, threat actor or attacker:** An individual, group, organization or government that attempts or executes an attack.
- **Attack:** An intentional attempt to gain unauthorized access to system services, resources or information; an attempt to compromise system integrity.
- **Authentication:** The process of verifying the identity or other attributes of an entity (user, process or device).
- **Authorization:** A process of determining, by evaluating applicable access control information, whether a subject is allowed to have the specified types of access to a particular resource.
- **BCP:** Business Continuity Plan**.** A document that sets forth procedures for the continued performance of core capabilities, critical operations and user services during any disruption or potential disruption.
- **CCISDA:** California County Information Services Directors Association. This is the official organization of the county IT directors and chief information officers throughout the state of California. CCISDA represents all 58 California counties in the area of information technology in county government.
- **CIO:** Chief Information Officer.
- **Computer Aided Dispatch Systems:** Used by dispatchers, call-takers, and 911 operators to prioritize and record incident calls, identify the status and locations of responders in the field and effectively dispatch responders.
- **Confidentiality:** A property of information that is not disclosed to users, processes or devices unless they have been authorized to access the information.
- **Cyber event or 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. An occurrence that constitutes a violation or imminent threat of violation of security policies, security procedures or acceptable use policies.

- **Cybersecurity**: The activity, process, ability, capability or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use, modification or exploitation.
- **DPP:** Disaster Preparedness Plan. A document that sets forth policies and procedures for restoration of information systems after a critical incident or event from any source. The plan addresses interim restoration of information operations in the short and medium term and full restoration of all capabilities in the longer term.
- **Data integrity:** The property that data is complete, intact and trusted and has not been modified or destroyed in an unauthorized or accidental manner.
- **Data security policy:** A rule or set of rules that governs 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.
- **Encryption:** The process of converting data into a form that cannot be easily understood by unauthorized people or agents.
- **Firewall:** A capability to limit network traffic between networks and/or information systems. A hardware/software device, or a software program, that limits network traffic according to a set of rules of what access is and is not allowed or authorized.
- **Hacker:** An unauthorized user who attempts to or gains access to an information system.
- **ISD:** Information Systems Department.
- **IT:** Information Technology.
- **KnowB4:** A proprietary security awareness training platform. KnowB4 is used by agencies for simulated phishing activities and other email compromise tests, as well as for other IT security training needs.
- **Malware:** Software that compromises the operation of a system by performing an unauthorized function or process.
- **Mobile device management tool**: A security software tool designed to help organizations secure, manage and monitor mobile devices such as smartphones and tablets.
- **Multi-factor authentication:** An electronic authentication mechanism in which a user is granted access to an application only after presenting two or more pieces of evidence (factors or keys only the authentic user knows or possesses).
- **Multi-layer security access:** Multi-layer security refers to a system that uses numerous components to shield the IT infrastructure. It is a defense mechanism that mitigates, delays or prevents threats.
- **Network or cyber infrastructure:** The information and communication systems and services composed of all hardware and software that process, store and communicate information; any combination of all these elements.
- **Next-generation systems:** Security systems consisting of both firewall and intrusion prevention systems built in, rather than as add-ons, along with the features of basic firewalls.
- **Phishing:** A digital form of social engineering to deceive individuals into providing sensitive information.
- **Phishing test:** A security training exercise designed to test users' vulnerability and reinforce vigilance.
- **Presidential Executive Order 14028: "**Improving the Nation's Cybersecurity" (issued May 12, 2021) requires agencies to enhance their cybersecurity system integrity.

- **Ransomware:** A type of malicious software designed to block access to a computer system until a sum of money is paid.
- **Ransomware attack response plan:** A set of predetermined and documented procedures to detect and respond to a cyber incident involving demand for ransom for recovery and restoration of data or systems.
- **Records Management System:** The management of records for an organization throughout the records' life cycle.
- **Redundancy:** Additional or alternative systems, sub-systems, assets or processes that maintain a degree of overall functionality in case of loss or failure of another system, sub-system, asset or process. Typically applied to power supplies and data backup systems.
- **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.

  Wi-Fi network: A family of wireless network protocols used for local area networking of devices and internet access, allowing nearby digital devices to exchange data by radio waves.

Background

The 2008-2009 San Joaquin County Grand Jury reported on information technology security, finding that several County departments and two of the seven cities in the county met expectations for Information Technology (IT) security, while some County departments and five cities did not. Recommendations were made and generally accepted in agency responses. In terms of technology, 2008-2009 was at least a generation ago. Government agencies use and store vast amounts of sensitive data on their residents and their employees, including personal identification data, financial data, health data and legal data. Additionally, these agencies provide services essential to our day-to-day lives, including public safety (police and fire), public works, health services, water services and community development. The Grand Jury recognizes that we are lay people, hardly experts, in the field of IT. It was the intent of the 2021-2022 Grand Jury to examine how the county and city governments within San Joaquin County are exercising due diligence to protect information, defend against future cyberattacks, maintain current disaster plans and provide on-going training to employees in these matters.

Reason for Investigation

As stated in Presidential Executive Order 14028, "…the prevention, detection, assessment and remediation of cyber incidents is a top priority and essential to national economic security."

San Joaquin County has experienced ransomware and cybersecurity attacks firsthand. School districts, municipalities and county agencies have been victimized in recent years. Given the rise in complexity of IT, the current sophistication of cybercrime, and the essential nature of government services provided, the 2021-2022 Grand Jury undertook an investigation into the current state of security and disaster preparedness of the IT systems of San Joaquin County and the seven incorporated cities within the county.

Method of Investigation

The 2021-2022 Grand Jury surveyed six San Joaquin County IT department heads and the City Manager or City Administrator of each of the seven cities in the county; each responded to the survey. Subsequently, an agency IT department head or staff member, an IT consultant or a city administrator was interviewed to clarify responses and to provide additional material when applicable. The Grand Jury also interviewed independent cybersecurity experts. The expert witnesses have collectively more than 50 years' experience at diverse levels of government ranging from county to state to national information systems and cybersecurity. IT executives from one school district were also interviewed. For this investigation, the Grand Jury interviewed 16 individuals and attended cybersecurity presentations.

The Grand Jury also reviewed numerous websites and newspaper and magazine articles relevant to this investigation. Additionally, the Grand Jury reviewed documents provided, including network diagrams, ransomware insurance policies and other items.

Materials Reviewed

- 2021-2022 San Joaquin County Grand Jury surveys
- Biden, Joseph. *Executive Order on Improving the Nation's Cybersecurity*. 12 May 2021. Executive Order#14028
- *California Joint Cyber Incident Response Guide*. California Office of Emergency Services Cyber Security Integration Center, 2 Aug. 2021
- *Cyber Atack Preparedness in Contra Costa County*. Contra Costa County Civil Grand Jury, 2021. Report 2104
- *Digital Services and Innovation Strategy*. San Joaquin County, 19 Nov. 2020
- *How to Develop a Ransomware Remediation Plan*. Rubrik, 2021
- *Information Technology Security*. 2018-2019 Santa Barbara County Grand Jury, 2019
- *Information Technology Security: Cities and San Joaquin County*. 2008/2009 San Joaquin County Grand Jury, 2009. Report No.03-08
- *Ransomware Defense for Dummies--2nd Edition*. 2nd ed., Cisco Umbrella, 2021

Websites Visited

- Cybersecurity & Infrastructure Security Agency. "CYBERSECURITY | CISA." *Cisa.gov*, Cybersecurity and Infrastructure Security Agency, 2019, www.cisa.gov/cybersecurity. Accessed 6 May 2022.
- Federal Trade Commission, and Alvaro Puig. "Cybersecurity Advice to Protect Your Connected Devices and Accounts." *Sjgov.org*, 24 Mar. 2022, www.sjgov.org/department/da/consumer-alerts/consumer-alerts/2022/03/24/cybersecurity-advice-to-protect-your-connected-devices-and-accounts. Accessed 6 May 2022.
- Kuykendall, By Kristal. "Cybersecurity Experts Call for More Transparency and Immediate Resources for Schools -." *The Journal*, 17 Mar. 2022, thejournal.com/Articles/2022/03/17/Cybersecurity-Experts-Call-For-More-Transparency-and-Immediate-Resources-for-Schools.aspx?Page=1. Accessed 6 May 2022.

- Marcum Accounts Advisors. “What Is a SOC 2?” *The SSAE 18 Reporting Standard - SOC 1 - SOC 2 - SOC 3 (Formerly SSAE 16)*, 8 Jan. 2022, www.ssae-16.com/faq/what-is-a-soc-2/. Accessed 30 Apr. 2022.
- National Institute for Cybersecurity Careers and Studies. “Cybersecurity Glossary | National Initiative for Cybersecurity Careers and Studies.” *Niccs.cisa.gov*, niccs.cisa.gov/about-niccs/cybersecurity-glossary. Accessed 6 May 2022.
- Unisys. “Cyber Attacks--What You Need to Know.” *Unisys*, 2022, www.unisys.com. Accessed 6 May 2022.

Discussions, Findings and Recommendations

General Discussion

The Grand Jury recognizes cybersecurity is an extremely complicated topic. Specialized knowledge, experience and expertise are required for a deep understanding of what is necessary for adequate policies, systems and architecture. Lacking such specialized knowledge, the Grand Jury researched numerous sources, including recognized experts in this field to determine the following elements of any ISD and to define the following expectations for adequate cybersecurity in today’s environment.

Expectations

- **Organization:** Each organization should have a detailed Organization Chart demonstrating the structure of its independent IT department. Cities lacking an independent IT department should have a chart showing where IT resides in their overall structure.
- **Network Diagram:** Each organization should have a detailed network diagram indicating the relationships between all IT architectural elements. Best-practice guidelines suggest that this diagram be confidential.
- **Data Confidentiality:** Each organization should have an organization-wide policy determining data confidentiality and access control. Policy for data access should be clearly defined and desk-specific or station-specific.
- **Data Security:** Each organization should have next-generation systems and controls to ensure both physical and cyber security for all IT assets. Next-generation firewalls and endpoint management systems provide protection against ever-evolving means of cyberattack. Data should be protected with daily or continuous backup and archival systems. Backups should be protected against corruption, external encryption and/or destruction. Agencies should require multi-factor authentication for access to network systems.
- **Business Continuity Plan (BCP):** Each organization should have a detailed, current, comprehensive plan for restoring services in the event of disruption from any source.
- **Disaster Preparedness Plan (DPP):** Each organization should have a formal, detailed plan to prepare for various possible IT disruptions. This plan should be tested frequently and updated regularly.
- **Ransomware Policy:** Each organization should have an internal (confidential) documented policy for agency response to a ransomware attack.

- **Cyber Event Insurance:** Each organization should have insurance coverage to help offset economic losses from cyber events.
- **Ongoing Employee Training:** Each organization should provide rigorous, frequent training and ongoing testing of all employees as an integral part of its cybersecurity profile.

Survey Results:

The table below indicates whether an agency met (**M**), did not meet (**NM**) or was in the process of meeting (**IP**) the nine defined expectations.

	Org Chart	Network Diagram	Data Confidentiality	Data Security	BCP	DPP	Ransomware Policy	Cyber Insurance	Training
SJC	M	M	M	M	M	M	NM	M	M
Escalon	M	M	M	M	NM	M	M	M	M
Lathrop	M	M	M	M	NM	M	NM	NM	M
Lodi	M	M	M	M	IP	M	M	M	M
Manteca	M	M	M	M	M	M	IP	IP	M
Ripon	M	M	M	M	NM	NM	NM	M	M
Stockton	M	M	M	M	M	M	NM	M	M
Tracy	M	M	M	M	IP	IP	NM	M	M

1.0 San Joaquin County–Discussion

In November 2020, San Joaquin County released a three-year (2020-2023) strategic plan for ensuring continuing security, efficacy, cost-effectiveness and best-service outcomes to all end-users of County services and systems. The plan document "San Joaquin County Digital Services and Innovation Strategy" established goals for County digital service systems. These goals—Modernizing and Leveraging Our Technology Environment—address objectives for a security posture:

1. Acquire and implement cybersecurity technology to enable SJC to develop industry-leading capabilities to help mitigate and address cybersecurity risk.
2. Develop and mature security governance and processes to meet or exceed industry standards, enhance security enforcement partnerships, and strengthen County practices.
3. Develop a robust security training program for the County workforce, including enhanced training and development for the security workforce.

Excerpt from "San Joaquin County Digital Services and Innovation Strategy," November 19, 2020 (page 6)

San Joaquin County has met these objectives and continues to update and enhance these processes as the cybersecurity landscape continues to evolve.

San Joaquin County ISD oversees all County departments, making it one of the largest county ISDs in California. San Joaquin County ISD is an active participant in the California County Information Systems Department Association (CCISDA). This association provides opportunities for counties to share information and experiences and offers guidance, such as standards for best-practice policies. Several large and specialized departments within the County have their own IT departments and department chiefs who report to the County's Chief Information Officer. Additionally, SJC has a dedicated Information Security Officer. All these IT executives form a cybersecurity governance committee which meets monthly, with subgroups meeting more frequently as needed.

County ISD and Human Resource Departments conduct frequent and on-going employee training and testing using proprietary software. In addition to these County departments, several Independent Special Districts in SJC use County IT services through various memoranda of understanding.

The only element of the defined expectations not met by SJC is having an internal documented policy for response to a ransomware attack.

San Joaquin County is a model agency in the realm of information technology and maintenance of cybersecurity.

Findings

F1.1 San Joaquin County does not have a formal internal policy concerning payments or procedures in ransomware attacks. This absence of policy could cause confusion, delay and greater loss of security in the event of such an attack.

F1.2 San Joaquin County has an exemplary profile regarding cybersecurity and should serve as a model for other government agencies within San Joaquin County.

Recommendations

R1.1 By November 1, 2022, the San Joaquin County Board of Supervisors, in conjunction with San Joaquin County ISD, develop, adopt and implement a formal internal policy and procedure for response to a ransomware attack.

2.0 City of Escalon−Discussion

The City of Escalon does not have an independent IT department but has a contract agreement with Mid Valley IT to provide all IT services. In the City organization, IT functions report to the Finance and HR Directors. Each employee is given a level of access according to assigned responsibilities within their department. All employees receive information security training specific to their responsibilities as well as general security awareness training. The IT consultant employs an aggressive multi-layered approach to mitigate security threats through software and hardware protection measures. Critical or confidential data is stored in multiple cloud-based locations and systems employing numerous safeguards, including use of multi-factor authentication for access.

IT functions are protected with a standby generator and redundant backups in case of a system failure. The generator is tested periodically for functionality.

The City of Escalon met all but one of the expectations for adequate cybersecurity. Escalon is by far the smallest city in San Joaquin County, but by using a contracted IT service provider, Escalon is meeting its cybersecurity needs. The City of Escalon does not have a documented Business Continuity Plan.

Findings

F2.1 The City of Escalon does not have a documented Business Continuity Plan, leaving the City relatively unprepared to restore essential services in a disruptive event.

Recommendations

R2.1 By January 1, 2023, the Escalon City Council, in conjunction with Mid Valley IT, develop, adopt and implement a Business Continuity Plan.

3.0 City of Lathrop−Discussion

The City of Lathrop met six of the expectations for the nine elements considered in this investigation. Lathrop's IT organization includes a Director of Information Technology at the cabinet leadership level, a policy strongly recommended by an IT expert for maximum IT security. Including the Director of IT in frequent, regular meetings with other department heads allows effective communication of IT security needs to all City departments.

Expectations for data confidentiality and data security were met. However, use of multi-factor authentication for system access was not universal at the time of this investigation, leaving Lathrop at higher risk of attack. Lathrop provides an unsecured public Wi-Fi network, separate from the City's secure business network and accessible to any user. Hackers or other bad actors could take advantage of the unsecured network, possibly resulting in compromise of log-in credentials from that network and possibly exposing the City to costly liability suits. Lathrop was in the process of developing and approving a BCP and DPP plan at the time of this investigation. Similarly, the City was updating an internal policy for response to a ransomware attack. At the time of this investigation, Lathrop lacked insurance against losses incurred in a cybersecurity incident.

Findings

F3.1 The City of Lathrop does not employ multi-factor authentication universally, leaving City systems more vulnerable to the activities of bad actors.

F3.2 The City of Lathrop provides an unsecured public Wi-Fi network. Misuse of this unsecured network could expose the City to liability risks.

F3.3 The City of Lathrop does not have an approved Business Continuity Plan, rendering the City relatively unprepared to restore essential services in a disruptive event.

F3.4 The City of Lathrop does not have a formal internal policy or procedure to address ransomware attacks. This absence of policy could cause confusion, delay and greater loss of security in the event of such an attack.

F3.5 The City of Lathrop does not have an insurance policy covering financial losses from a cyberattack, possibly exposing City financial resources.

Recommendations

R3.1 By November 1, 2022, the Lathrop City Council, in conjunction with the City's IT department, develop, adopt and implement a procedure for universal multi-factor authentication for access to City data.

R3.2 By November 1, 2022, the Lathrop City Council, in conjunction with the City's IT department, provide a secure public Wi-Fi network.

R3.3 By January 1, 2023, the Lathrop City Council, in conjunction with the City's IT department, develop, adopt and implement a Business Continuity Plan.

R3.4 By November 1, 2022, the Lathrop City Council, in conjunction with the City's IT department, develop, adopt and implement a formal internal policy and procedure for a ransomware attack.

R3.5 By January 1, 2023, the Lathrop City Council, in conjunction with the City's IT department, obtain an insurance policy to mitigate fiscal impact resulting from cyberattack or other critical information system loss.

4.0 City of Lodi−Discussion

The City of Lodi has a large IT division, responsible for all IT functions of the City. The division is responsible for the integrity of the City's cyber infrastructure, maintenance and support of all hardware and software, and assuring secure access to all network resources. Lodi fell victim to a ransom attack in April 2019. That unfortunate event caused the City to change its management of cybersecurity, significantly elevating the importance of vigilance by all City staff. Lodi has implemented a robust cyber awareness training program for all City employees, incorporating education in tactics used by bad actors both inside and outside the City's network. Monthly training is followed by testing in topics covered. Citywide campaigns occur quarterly to test employee response to phishing and other email-based attacks. The IT division head reports directly to the Deputy City Manager and meets regularly with all City department heads. The City of Lodi met all expectations for cybersecurity except for having a completed, up-to-date Business Continuity Plan. The City has contracted a business consulting firm to create a BCP, projected to be completed and implemented by the end of June 2022.

Findings

F4.1 The City of Lodi does not have an approved Business Continuity Plan, rendering the City relatively unprepared to restore essential services in a disruptive event.

F4.2 The City of Lodi has implemented an excellent cyber awareness training program for all employees minimizing risk to damage from cyberattack.

Recommendations

R4.1 By January 1, 2023, the Lodi City Council, in conjunction with the City's IT division, develop, adopt and implement a Business Continuity Plan.

5.0 City of Manteca−Discussion

The City of Manteca met seven of the nine expectations considered in this investigation. Manteca's Information Technology department is independent in the City's organization. The department director reports directly to the City Manager and meets weekly with other City department heads. User level of access is determined by position, background and other departmental factors. Employees are trained on a regular basis. The training is mandatory for all employees. Hard drives are encrypted, and a Mobile Device Management tool is used for tablets, laptops and phones.

Manteca's ISD is currently updating its Information Technology Security Policy. This comprehensive policy has not been updated since 2010. Manteca's Department of Information Technology and Innovation is collaborating with City administration and the City Attorney to update all policies relating to information technology security. Similarly, the City is in the process of bringing both hardware and software systems up to next-generation standards with new firewall, malware, user access, backup systems and applications in place. Employee training is executed through KnowB4, an industry-standard cybersecurity training program which includes phishing and other email compromise testing.

Regarding firewalls and switches, roughly 60% still operate off single rather than dual or redundant power supplies. Over the next five years, the City is phasing out older devices as they reach end-of-life.

Findings

F5.1 The City of Manteca has an Information Technology Security Policy which has not been updated since 2010, leaving the City relatively unprepared for a cyber event.

F5.2 The City of Manteca lacks a policy and procedure for ransomware attacks. This absence of policy could cause confusion, delay, and greater loss of security in the event of such an attack.

F5.3 The City of Manteca has a significant number of security devices with single power supplies. This lack of redundant power presents vulnerability in major or prolonged power outages.

Recommendations

R5.1 By January 1, 2023, the Manteca City Council, in conjunction with the City's ISD, develop, approve and implement an updated Information Technology Security Policy.

R5.2 By January 1, 2023, the Manteca City Council, in conjunction with the City's ISD, develop, approve and implement a confidential policy and procedure for response to a ransomware attack**.**

R5.3 By March 1, 2023, the Manteca City Council, in conjunction with the City's ISD, develop, approve and adopt an updated timeline to replace single-powered units with dual-powered or redundant-powered units in their network architecture.

6.0 City of Ripon−Discussion

The City of Ripon has experienced turnover and vacancies in the IT Department in the past year. The Director of IT resigned in early 2021. Subsequently, another IT Director was hired but resigned within three months. The City has contracted with a former IT employee as a temporary IT Director and is currently updating the job description for a permanent director of the IT functions.

The City's organization chart does not include an IT department or department head. The only IT position shown is within the Police Department.

Data confidentiality is maintained through a three-tiered access structure. Management supervisors for each City department determine who has access to appropriate information. Sensitive data is held within a Computer Aided Dispatch Program or a Records Management System within the IT division of the Ripon Police Department. The sensitivity of data with all other City departments is determined by supervisors.

Findings

F6.1 It is unclear in the City of Ripon's Organization Chart where responsibilities for IT and IT security lie, creating confusion over who is responsible to act in a disruptive event.

F6.2 The City of Ripon has a rudimentary network diagram outlining the City's router and firewall relationship with networks used, but the diagram lacks detail, leaving uncertainty about data security.

F6.3 Although the City of Ripon met expectations in the areas of data confidentiality and security, lack of IT staff and leadership leaves these areas vulnerable to cyberattack.

F6.4 The City of Ripon lacks a Business Continuity Plan, rendering the City relatively unprepared to restore essential services in a disruptive event.

F6.5 The City of Ripon does not have a Disaster Preparedness Plan, leaving the City at risk for significant delay and cost to restore IT systems in the event of a disaster.

F6.6 The City of Ripon does not have a formal policy or procedure to address ransomware attacks. This absence of policy could cause confusion, delay and greater loss of security in the event of an attack.

Recommendations

R6.1 By January 1, 2023, the Ripon City Council develop and make public an updated City Organization chart showing details of the City's IT functions, including all IT positions.

R6.2 By January 1, 2023, the Ripon City Council develop and adopt a detailed Network Diagram to decrease security vulnerabilities.

R6.3 By January 1, 2023, the Ripon City Council obtain a third-party security review of the City's IT department assets, positions, and policies and an evaluation of data confidentiality, security systems and protocols.

R6.4 By January 1, 2023, the Ripon City Council develop, adopt and implement a formal Business Continuity Plan.

R6.5 By January 1, 2023, the Ripon City Council develop, adopt and implement a formal Disaster Preparedness Plan for IT functions.

R6.6 By January 1, 2023, the Ripon City Council develop, adopt and implement a formal internal policy and procedure for response to a ransomware attack.

7.0 City of Stockton−Discussion

The City of Stockton has a large IT department that oversees IT functions for all the City's other departments. Data confidentiality and user access are determined departmentally, following uniform standards. Information is protected by many safeguards aiming not only to minimize risk of penetration but also to detect any breach that might occur. Stockton has both a BCP and a DPP. Stockton is one of very few cities having license to use a cybersecurity tool integrating the City with the State of California's Office of Emergency Services. Stockton's IT Director meets weekly with other department heads, updating them on all matters related to cybersecurity.

Stockton met each of the cybersecurity expectations except for the presence of a documented internal policy and procedure for response to a ransomware attack. However, the City does have a Cybersecurity Response Book detailing response procedures for other cyber events. Employee security awareness training is required every six months.

Findings

F7.1 The City of Stockton does not have a formal internal policy concerning payments or procedures in ransomware attacks. This absence of policy could cause confusion, delay and greater loss of security in the event of an attack.

F7.2 The City of Stockton has a large IT Department which places cybersecurity and disaster preparedness at a high priority, minimizing risk to the City's information and service systems.

Recommendations

R7.1 By November 1, 2022, the Stockton City Council, in conjunction with the City's IT department, develop, adopt and implement a formal internal policy and procedure for response to a ransomware attack.

8.0 City of Tracy−Discussion

The City of Tracy met all expectations for cybersecurity or was in the process of meeting them when surveyed. The City has an Information Technology Division, which is part of the Finance Department. This division supports all departments and functions of the City except water treatment. Data confidentiality and security are guaranteed with industry-leading, next-generation firewalls and network access controls. Data storage, backup and cybersecurity are monitored continually. The IT Manager meets every two weeks with all other City department heads to address IT issues, including cybersecurity.

Tracy does not require encryption of thumb drives used on City devices, a requirement that is considered a "best practice" by an expert witness.

Tracy does not have either a formal Business Continuity Plan or Disaster Preparedness Plan in place but is in the process of developing both. The BCP was scheduled to be complete in April 2022. Completion date for the DPP was not specified by the City.

Findings

F8.1 Lacking a requirement for encryption of thumb drives used on City devices exposes the City of Tracy to potential data theft and contamination.

F8.2 The City of Tracy lacks a completed Business Continuity Plan, rendering Tracy relatively unprepared to restore essential services in a disruptive event.

F8.3 The City of Tracy lacks a completed Disaster Preparedness Plan, leaving Tracy at risk for delay and cost to restore IT systems in the event of a disaster.

Recommendations

R8.1 By November 1, 2022, the Tracy City Council, in conjunction with the IT division, develop, adopt and implement a policy requiring encryption of thumb drives used on City devices.

R8.2 By January 1, 2023, the Tracy City Council, in conjunction with the IT division, develop, adopt and implement a formal Business Continuity Plan.

R8.3 By January 1, 2023, the Tracy City Council provide the Grand Jury with an updated formal Disaster Preparedness Plan.

Conclusion

San Joaquin County is well protected regarding cybersecurity. The seven cities in the county vary with respect to Grand Jury expectations, most being well secured but lacking defined plans for Business Continuity and IT Disaster Preparedness. Cybersecurity is an evolving concern and requires ongoing efforts by government entities to remain current and vigilant against risks to their Information Systems.

In this investigation the Grand Jury learned from cybersecurity experts that three key elements lead to maximum agency cybersecurity:

- a dedicated information security position within each organization,
- a "seat at the table" with other agency department heads in regular meetings, and
- a rigorous employee education and training program in cybersecurity matters.

Disclaimers

Grand Jury reports are based on documentary evidence and the testimony of sworn or admonished witnesses, not on conjecture or opinion. However, the Grand Jury is precluded by law from disclosing such evidence except upon the specific approval of the Presiding Judge of the Superior Court, or another judge appointed by the Presiding Judge (Penal Code Section 911. 924.1 (a) and 929). Similarly, the Grand Jury is precluded by law from disclosing the identity of witnesses except upon an order of the court for narrowly defined purposes (Penal Code Sections 924.2 and 929).

Response Requirements

California Penal Code Sections 933 and 933.05 require that specific responses to all findings and recommendations contained in this report be submitted to the Presiding Judge of the San Joaquin County Superior Court within 90 days of receipt of the report.

The San Joaquin County Board of Supervisors and the City Councils of each city addressed shall respond to all findings and recommendations specific to their city.

Mail or hand deliver a hard copy of the response to:

Honorable Michael D. Coughlan, Presiding Judge
San Joaquin County Superior Court
180 E Weber Ave, Suite 1306J
Stockton, California 95202

Also, please email a copy of the response to Ms. Trisa Martinez, Staff Secretary to the Grand Jury, at grandjury@sjcourts.org