

San Joaquin County Grand Jury



INFORMATION TECHNOLOGY SECURITY Cities and San Joaquin County 2008/2009 San Joaquin County Grand Jury Case No. 03-08

SUMMARY

Members of the 2008/2009 San Joaquin County Grand Jury expressed interest in determining if the local municipalities and county offices of San Joaquin County have planned or installed sufficient safeguards to protect the information systems against virus, accidental/deliberate disclosures, and/or equipment failure.

REASON FOR INVESTIGATION

This report was based on concerns by the Grand Jury about the current status of the information systems used by city and county governments in San Joaquin County. This review is a point in time snapshot of what was seen by the Grand Jury at the time the information was made available.

It is the intent of the Grand Jury that this investigation would demonstrate that San Joaquin County and its seven incorporated cities were exercising due diligence in protecting information resources and making appropriate plans for disaster recovery and business continuity.

BACKGROUND

As defined in the United States Code, Information Security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction.¹ Today, even the smallest governmental entity, including small and large cities and the numerous county departments, accumulates a large quantity of sensitive information about its business and citizens. Much of this information is collected, stored in and/or transmitted across networks to other computers electronically. Each of these entities has dedicated staff that operates and maintains these systems. Computer security is an ever increasing component of its responsibilities.

¹ United States Code, Title 44, Chapter 35, Subchapter III, Section 3542

METHOD OF INVESTIGATION

This investigation was a “layman’s” inquiry into the current state of information technology (IT) security within San Joaquin County’s governmental bodies. Therefore it is important that this investigation should not be construed as a formal security audit.

Materials Reviewed

- City and County IT Security Policies
- City and County network diagrams
- City and County Organization Charts
- City and County websites online documentation
- Responses to questionnaires submitted to San Joaquin County departments

Interviews Conducted

Representatives of San Joaquin County and each of its seven incorporated cities were interviewed.

EXPECTATIONS

Grand Jury expectations were that each of the IT organizations investigated would have included the following as components of a comprehensive security plan.

- **Security policy:** Each organization should have a top-level statement endorsed by the senior management team on which all security processes and procedures are subsequently based. This policy should be published and understood by all users with access to information systems, and should be reviewed and updated as necessary.
- **Physical and environmental security:** Precautions should be taken to ensure the physical security for all IT assets including data centers, local computers and laptops.
- **Communications and operations management:** Adequate tools and services be provided to ensure that information in these systems is properly monitored, managed and protected. (i.e. anti-virus software, spam and internet filters, security patching, and supported operating systems on all servers and workstations).
- **Access control:** Each organization should have systems in place to closely monitor and control individuals authorized to read and to amend the organization’s information.
- **Disaster planning:** Each organization should have a documented plan for managing any incident and a documented process for restoring critical systems.
- **Business continuity:** Each organization should have a plan to minimize the impact of major disasters on the business processes until essential services are restored.

- **Validation and testing:** Ensure that established controls and policies continue to work and deliver the required level of protection to the organization's assets.

FINDINGS

The extent to which each IT organization was able to meet the Grand Jury's expectations varied significantly. The largest organizations seemed to be the best prepared. However, the Grand Jury found that some of the smaller cities included sophisticated security measures and clear goals for measures yet to be implemented.

The Grand Jury found that all organizations investigated provided at least the bare minimum of security for IT assets:

- Routine backup of all servers
- Installed and managed Anti-Virus software
- Physical security for data center
- Access control using account login & passwords

San Joaquin County

San Joaquin County has a highly fractured Information Technology (IT) infrastructure with 16 separate organizations serving various county departments, in addition to the Information Systems Division (ISD). A number of the departments made compelling arguments for maintaining departmental development and support services.

The Grand Jury understands some departments are bound by state and federal mandates and regulations to maintain isolated IT systems. However, significant savings would be realized by consolidating network infrastructure and common software.

1. *Information Systems Division* – Meets expectations for IT Security
 - a. Written Security Policy was clear and comprehensive and all employees were made aware of its content
 - b. The division has developed an online security training program required to be completed by all employees
 - c. Founded intra-governmental IT Security group inviting all county departments and cities to discuss common security issues
2. *Human Services Agency, Behavioral Health Services, Public Health Services, and San Joaquin County General Hospital* – Meets expectations for IT Security
 - a. Each of these health related departments are subject to federal and state oversight and numerous security related regulations; as a result, each exhibited a very sophisticated level of IT security
3. *Assessor-Recorder-County Clerk Division* – Meets expectations for IT Security
 - a. Documented and thorough “Emergency Contingency and Disaster Recovery Plans for Information Systems”

4. *Agricultural Commissioner's Office* – Does not meet expectations for IT Security
 - a. Out-dated and unsupported Sever Operating System (Windows NT 4.0) still in service, though not in a critical role
 - b. Disaster preparedness and recovery plan is currently under review
 - c. Personnel IT Security training has not yet begun
5. *Department of Child Support Services* – Meets expectations for IT Security
 - a. Provides a good model for the distribution of IT services allowing ISD to maintain and configure the network infrastructure while utilizing departmental IT staff for local support and unique development requirements
6. *Community Development Department* – Meets expectations for IT Security
 - a. The departments' implementation of 'thin client terminals' provides a high level of IT security
 - b. Server recovery from backup is tested annually
 - c. Reciprocal catastrophic disaster recovery plan with neighboring county
7. *District Attorney's Office* – Does not meet expectations for IT Security
 - a. Evidence of a documented disaster preparedness and recovery plan was not provided
8. *Employment & Economic Development Department* – Meets expectations for IT Security
 - a. EEDD has created a detailed Disaster Recovery Plan and ensured that IT staff had it on hand at all times
 - b. Encryption software for laptops is currently being deployed
9. *Environmental Health Department* – Meets expectations for IT Security
 - a. EHD is transitioning to server virtualization that will significantly enhance disaster recovery efforts
 - b. Ambitious plans for high availability, redundant data systems are in development but budget constraints make near term deployment unlikely
10. *Public Defenders Office* – Does not meet expectations for IT Security
 - a. Primary and backup servers are out-dated. The server operating system (Windows NT 4.0) is nearly 4 years past the manufacturer's end-of-life date.
 - b. 90% of department employees have so far failed to complete the county's IT security training
 - c. Critical or confidential "case information" is allowed to be stored on local workstations
 - d. Portable and mobile devices, presumably also with confidential case information, are unencrypted, though password protected

11. *Public Works Department* – Meets expectations for IT Security
 - a. Installing encryption software on all new laptops
 - b. Disaster recovery plan is dependent upon the ability to fall back to paper hard copies for daily operations. This may be appropriate for this department

12. *Sheriff-Coroners Office* – Does not meet expectations for IT Security
 - a. Very clear and well defined standards for a user's access to confidential data and the determination of the sensitivity of that data exists.
 - b. At least one server is running dated operating system (Windows NT 4.0)
 - c. The department's IT systems have been designed for high availability and redundant components
 - d. Disaster recovery plan was thorough and comprehensive

13. *Treasurer and Tax Collector* – Meets expectations for IT Security
 - a. Treasury and Tax records are unique in that they are 'public record'

City of Stockton – Does not meet expectations for IT Security

1. Chronic understaffing and the recent layoff of the Director of Information Technology
2. Lacks a documented disaster recovery or business continuity plan
3. Written Security Policy was clear and comprehensive and all employees were made aware of its content

City of Lodi – Does not meet expectations for IT Security

1. Well documented security policy with plans for continuing staff refresher classes
2. Well documented disaster and recovery plan
3. Policy and devices do restrict unauthorized connections to the city network
4. The current location of city data center and backup generator are below ground level
5. Web filtering is in place, but access to private email accounts has been allowed
6. Independent IT support of Finance Department should be answerable to central IT policies and lacks internal controls
7. Web email accounts and independent IT support for Finance violates sound security policy

City of Lathrop – Meets or is addressing expectations for IT security

1. IT Manager has only been on the job for a short time, yet he has a clear vision of security goals and is working to meet them
2. Written Security Policy was clear and all employees were made aware of its content
3. Recently upgraded Email filtering has dramatically reduced spam
4. Hardware redundancy on critical systems with plans to expand as budget allows
5. Plans for disaster recovery and business continuity are currently in development

City of Tracy – Does not meet expectations for IT Security

1. Enforces a strong password policy that includes routine changing
2. Lacks a written security policy
3. Employees are allowed unrestricted access to web email accounts and the internet

City of Manteca – Does not meet expectations for IT Security

1. Limited security polices in place address only email and software use
2. The few city owned laptops do not have hard drive encryption
3. Lacks a documented disaster recovery plan
4. Emergency backup power not available for the entire data center

City of Ripon – Does not meet expectations for IT Security

1. Lacks a written IT Security Policy and provides no means for insuring that employees are aware of and adhere to such policies
2. Lacks a documented disaster recovery plan
3. No systematic method exists to insure that critical software patches are applied as they become available
4. The secure storage of backup tapes was inadequate

City of Escalon – Meets or is addressing expectations for IT security

1. Escalon impressed the Grand Jury with the level of thought and steps already implemented toward its IT security
2. Written Security Policy was clear and comprehensive and all employees were made aware of its content
3. Disaster preparedness seemed appropriate for an organization of this size and included equipment redundancy and distributed locations

RECOMMENDATIONS

The 2008/2009 San Joaquin County Grand Jury recognizes the budget limitation due to current economic conditions. The Grand Jury therefore has limited recommendations to those that can be implemented with existing resources, except where minimal investment is required or the risks were deemed significant.

When economic conditions permit, the Grand Jury recommends all IT organizations contract for an independent security audit.

1) San Joaquin County

- a) *Agricultural Commissioner's Office*
 - i) Upgrade outdated server operating systems
 - ii) Ensure that IT Security training for all personnel begins immediately and full compliance is achieved in a timely manner
- b) *District Attorney's Office*
 - i) Prepare a comprehensive and documented disaster recovery and business continuity plans
- c) *Public Defenders Office*
 - i) Upgrade outdated server operating systems
 - ii) Ensure that IT Security training for all personnel begins immediately and full compliance is achieved in a timely manner
 - iii) Establish and enforce policy to prohibit local file storage of confidential information

- iv) Where portable devices such as laptops are required, insure that hard drives are encrypted
- d) *Sheriff-Coroner's Office*
 - i) Upgrade outdated server operating systems

2) City of Stockton

- a) Chronic understaffing and lack of leadership should be promptly addressed
- b) Prepare a comprehensive and documented disaster recovery and business continuity plans

3) City of Lodi

- a) Develop plans and preparations for the relocation of the data center to a more secure location
- b) Extend IT security policy to restrict access to external email accounts from the city network
- c) Ensure all IT support staff function under unified policies and management

4) City of Tracy

- a) Prepare a clear and comprehensive IT security policy approved and endorsed by city management
- b) Ensure and document that every employee is informed of the IT security policy and the consequences of violations
- c) Implement tighter internet access controls on the network

5) City of Manteca

- a) Expand current IT security policies to provide greater guidance and insure that all employees are informed of the policy updates
- b) Where portable devices such as laptops are required, insure that hard drives are encrypted
- c) Prepare a comprehensive and documented disaster recovery and business continuity plan
- d) Ensure that emergency backup power is provided to the entire data center

6) City of Ripon

- a) Prepare a clear and comprehensive IT security policy approved and endorsed by city management
- b) Ensure and document that every employee is informed of the contents of this policy and the consequences of its violation
- c) Prepare a comprehensive and documented disaster recovery and business continuity plan
- d) Adopt manual or automated process that insures every server and workstation is kept current with all security patches and anti-virus updates
- e) Ensure that the off-site storage of backup tapes is secure

RESPONSE REQUIRED

Pursuant to Section 933.05 of the California Penal Code:

The San Joaquin County Board of Supervisors and the various City Councils, where applicable, shall report to the Presiding Judge of the San Joaquin County Superior Court, in writing and within 90 days of publication of this report, with a response as follows:

The San Joaquin County District Attorney and the San Joaquin County Sheriff, where applicable, shall report to the Presiding Judge of the San Joaquin County Superior Court, in writing and within 60 days of publication of this report, with a response as follows:

As to each finding in the report a response indicating one of the following:

- a. The respondent agrees with the finding.
- b. The respondent disagrees with the finding, with an explanation of the reasons therefore.

As to each recommendation, a response indicating one of the following:

- a. The recommendation has been implemented, with a summary of the action taken.
- b. The recommendation has not yet been implemented, but will be with a time frame for implementation.
- c. The recommendation requires further analysis, with an explanation of the scope of analysis and a time frame not to exceed six (6) months.
- d. The recommendation will not be implemented, with an explanation therefore.

APPENDICES

Appendix A - Sample questionnaire submitted to San Joaquin County independent IT organizations:

- 1) Please describe your department's IT infrastructure including;
 - a) Number, operating system, and function of servers managed by your department.
 - b) Number of personal computers deployed.
 - c) Any and all security features.
 - d) How your network interfaces with the county's network.
- 2) What is the scope of your departments IT responsibilities?
- 3) Departmental IT integration with San Joaquin County (SJC) Information Systems Division (ISD)
 - a) What factors require that your department maintain separate IT department and network from the county's ISD?
 - b) How does your department work with ISD?
 - c) Does your department regularly participate in ISD monthly security meetings?
- 4) Does your department share the same IT Security Policy as that used by ISD?
 - a) Are there any unique policies to your department?
- 5) Data confidentiality
 - a) How is a user's level of access to information determined?
 - b) How is the sensitivity of data determined?
 - c) Is your department participating in the ISD online IT security training for all personnel?
 - i) If not, why, and what alternative is employed?
 - ii) What percent of end users have completed IT security training?
- 6) Please describe how the following are secured for data integrity
 - a) The network; wired and wireless.
 - b) Servers
 - c) Clients/workstations
 - i) To what extent is critical or confidential data being stored on local workstations?
 - ii) Are there controls on portable and mobile devices (Laptops, thumb drives, ...) to protect confidentiality?
- 7) Disaster Preparedness
 - a) Describe your department's disaster plan for natural or man made disaster (i.e. loss of power, network connectivity, system failure, flood or earthquake).
 - b) Has it been tested and how often?
 - c) Describe your plans for business continuity.
 - d) What is the most serious system failure to date?
 - i) What was your time to full recovery?
 - ii) What lessons were learned?

Name of person completing questionnaire: _____

Phone number: _____

Email address: _____

Appendix B - Sample questions asked of cities IT representatives:

1) Overview

- a) Please provide us with a brief background of your self
 - i) City: _____
 - ii) Name: _____
 - iii) Position: _____
- b) What is the scope of your IT Division responsibilities?
 - i) Are all of your city's departments subject to ISD over site and policies?
 - ii) Are there any significant data systems that exist within county government that do not fall within your direct authority and responsibility?
- c) Organization Chart
- d) Network diagram

2) IT Security

- a) Data confidentiality
 - i) How is a users level of access to information determined?
 - ii) How is the sensitivity of data determined?
 - iii) Do all departments follow uniform standards?
 - iv) How are new employees trained with regards to data confidentiality and security?
 - (1) Is there follow up training?
- b) Data Security (Malware, Hacking, Corruption)
 - i) Network
 - (1) Wired
 - (2) Wireless
 - ii) Servers
 - iii) Clients/workstations
 - (1) To what extent is critical or confidential data being stored on local workstations?
 - (2) Are their controls on portable and mobile devices (Laptops, thumb drives, ...) to protect confidentiality?
- c) Disaster Preparedness (Availability)
 - i) Preparations
 - (1) Standby generator
 - (2) Redundant Power and Network source
 - (3) Off site backups
 - ii) Recovery
 - (1) Has it been tested
 - iii) Business continuity
 - (1) Is there a documented plan?
 - (a) How is it distributed?
 - (2) What is your estimated time to essential services?
 - iv) What is the most serious system failure to date?
 - (1) What was your time to full recovery?
 - (2) What lessons were learned?