County Information Technology Security

Background

The County government is dependent on information technology to perform most of its responsibilities. This involves a complex web of technology that sits behind what, to a casual viewer, would seem to be a set of ordinary personal computers (PCs). The complexity of this system is illustrated in Figure 1. The system resides at different layers. The first layer is a communications network that connects all elements. The second is a series of servers and mainframe computers upon which reside significant application programs like the financial and court systems. The third and visible layer is the set of networked PC s sitting on individual desks. These PCs act somewhat similarly to a home computer but the software behind them has more complex tasks to perform than a home machine.

The security of information technology and the data embedded in the system is a management responsibility that has both performance and legal consequences for the County. For example the Health Insurance Portability and Accountability Act (HIPAA) requires health providers to secure all information that can be identified back to an individual. Penalties to the County include fines up to $250,000. Most transgressions are associated with data theft, identity theft, industrial espionage and privacy law violation.

An important element of this system is the necessity to permit contractors and agencies not under the control of the County to have access to the network. This access is usually accomplished by giving the contractor hardware or software security tokens that allow unfettered access to the County network. These tokens provide a continually changing password that is synchronized to the County network. Each token is serialized and should be under the control of an individual who is held accountable for the token.

Information security exists when information is accessible only to those authorized to have access, the information processing methods are accurate and complete and users have access to data and information assets when required.

Security can be defined as the state of being free from unacceptable risk. The risk in this framework concerns the following categories of losses:

- Confidentiality of Information
- Integrity of Data
- Assets
- Efficient and Appropriate Use
- System Availability

Confidentiality refers to the privacy of personal or corporate information. This includes issues of copyright.

Integrity refers to the accuracy of data. Loss of data integrity may be gross and evident, as when a computer disc fails, or subtle, as when a character in a file is altered.

Assets, efficient and appropriate use and system availability are self explanatory.

There are three pillars upon which information security resides. The first pillar is management initiated procedures, checks and balances. The second is proper technology use by a knowledgeable set of users and support personnel. The last is proper acquisition, maintenance and operation of the technology. The first two items are solely the responsibility of line management. The last item is the responsibility of technologists, most of whom reside in the County Information Systems Department (ISD).

Methodology

The Grand Jury reviewed all of the line department strategic information system plans that were on file with the ISD. The Grand Jury attended meetings of the County Information Technology Committee as well as meetings of operational personnel that addressed security issues and met with line department and ISD personnel. The Grand Jury then reviewed information security related policy and the international published standards for information security.

Findings

F-1. The County "network" is a heterogeneous mix of equipment that is partially managed by the ISD and partially managed by numerous line departments. There are a high number of independently managed data-center/server rooms that duplicate basic services.

F-2. Two significant security management controls are the management of passwords and the restriction of an individual to the appropriate level of control of information resources.

F-3. Some key control deficiencies are lack of an automatic method to terminate a password when an individual leaves the organization and lack of periodic reviews of the status of employees to determine proper access level.

F-4. Each department has network elements that are common and applications that are unique.

F-5. Many of the department strategic information system plans do not consistently and clearly identify the hierarchy of importance of departmental programs and applications. This deficiency diminishes the ability to coordinate disaster recovery efforts due to a lack of recognized priorities.

F-6. There are gross inconsistencies in the level of experience and technical knowledge among non-ISD server administrators. These inconsistencies lead to an inability to properly secure the County-wide network because these departmental systems, while allowing access to the County network, are not being hardened properly. For example, the use of initial software manufacturer default settings and passwords and laxity in making critical updates from software vendors leave an open door for intrusion into the County network.

F-7. Many departments have contractors that are allowed access to the County network. There are limited contract controls in place to administer third party compliance with County security requirements. These deficiencies include:

a. Contract and Policy Compliance

   i. Many third party businesses share a single (or limited number) of access tokens between employees, thereby granting untraceable access to the County network. This arrangement would never be accepted for County employees, yet is somehow adequate for employees of third party businesses with access to County infrastructures. Most of these third party employees are neither given any background checks nor are they required to be bonded.

   ii. There is no methodology for third party businesses to notify the County when employees leave or are fired.

   iii. There is no methodology to ensure that third party businesses are abiding by acceptable use and proper security for access tokens.

   iv. There are no clear mandatory guidelines for County legal recourse in the event a third party business provides an access point for illegal activity on the County's network infrastructure.

b. Technical and Procedural Compliance

   i. Security tokens that are improperly administered by outside trusted network administrators can lead to security compromises.

   ii. Third party servers that are not in compliance with County patch management procedures create vulnerabilities to the County network.

F-8. Physical security (building access, hallway access, departmental access, and cubicle access) is largely non-existent in most administrative areas. The public is granted unfettered right-of-way to almost every area. This is of particular significance because of the general lack of staff awareness and suspicion of criminal information gatherers.

F-9. The County information systems have poor password management. Theft or compromise of passwords is the Achilles heel of information technology. Staff members are generally unaware of the implications of individuals gathering seemingly innocuous information for the criminal purpose of allowing the perpetrator to impersonate a valid system user.

F-10. The issue associated with securing computerized information is common throughout developed countries. The International Standards Organization (ISO) standard 17799 provides an effective template for addressing this issue. A checklist based on ISO 17799 is included in Appendix A.

Conclusions

C-1. The County network, as it is currently managed, is unsecurable and has elements that are duplicative. F-1, F-2, F-3, F-6, F-7, F-8, F-9

C-2. Although computer applications and the network work together, the management and security of application programs needs to be addressed distinctly from management and security of the network. F-1, F-4

C-3. Contractors have access to the network without the controls on network access that are normally applied to County employees. F-6, F-7

C-4. At present, the majority of security vulnerabilities are associated with training, procedures and internal controls rather than with the quality and performance of the technology itself. F-2, F-5, F-6, F-7, F-8, F-9, F-10

Recommendations

R-1. The Information Technology Committee, with technical support from the ISD, sponsor the risk analysis of a major agency's systems based on ISO 17799. This study would provide a baseline for a risk analysis procedure for all of the County agency's applications.

R-2. That the Information Technology Committee revise the approach for Information System Planning to reflect the criticality of specific systems to the County and the management approaches used to mitigate risk.

R-3. That the Auditor-Controller review ISO 17799 as the basis for an information system internal control program for the County. The internal controls so developed could then be included as part of the management controls for various departments.

R-4. That the County Executive Officer initiate a study to determine if the complete County network needs to be managed like a utility with a single agency having responsibility. The purpose of such a study would be to gain a securable network and lower operating costs.

R-5. That County Counsel develop, with the help of the ISD, standard language to be inserted into contracts that allow third party access to address the issues identified in F-9.

R-6. That GSA review all contracts that allow access to the County network and insure these contracts are revised in accordance with the language developed by the County Counsel. That GSA modifies its procedures to insure that future relevant contracts are not permitted without the appropriate contract language.

R-7. ISD provide a standard training package for all employees who are normal users to instruct them as to their responsibilities in maintaining security of information assets and data.

R-8. ISD provide a mechanism for certification and training of all server administrators whose servers access the County network.

Responses Required

County Executive Officer (R-4)
Auditor-Controller (R-3)
County Counsel (R-5)
Director, General Services Agency (R-6)
Chief Information Officer (R-1, R-2, R-3, R-5, R-7, R-8)
Chair of the Information Technology Committee (R-1, R-2)

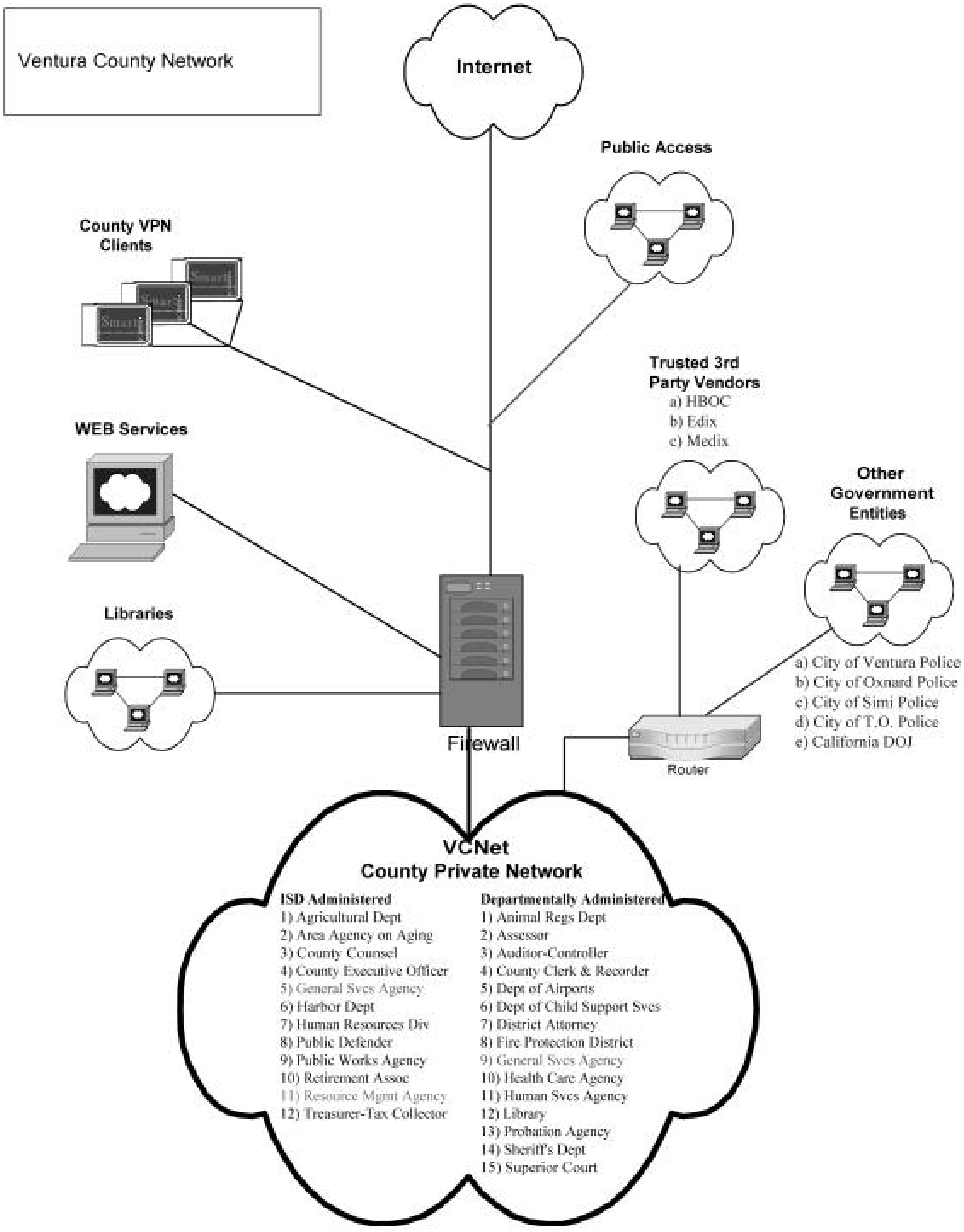

Figure 1. Ventura County Network

Appendix A
ISO 17799 Check List

ISSUES	Significance			Documentation		Comments
	V	L	NA	IT	D	
Information security policy						
Security organization						
Information security infrastructure						
Security of third party access						
Security for Outsourced Work						
Asset classification and control						
Accountability for assets						
Information classification						
Personnel security						
Security in job definition and resourcing						
User training						
Responding to security incidents and malfunctions						
Physical and environmental security						
Secure areas						

Equipment security						
General Controls						
ISSUES	**Significance**			**Documentation**		**Comments**
	V	**L**	**NA**	**IT**	**D**	
Computer and Network Management						
Operational procedures and responsibilities						
System planning and acceptance						
Protection against malicious software						
Housekeeping						
Network management						
Media handling and security						
Exchanges of media and software						
Access control						
Departmental requirement for access control						
User access management						
User responsibilities						
Network access control						
Operating system access control						
Application access control						

Monitoring system access and use						
Mobile computing and teleworking						
ISSUES	**Significance**			**Documentation**		**Comments**
	V	**L**	**NA**	**IT**	**D**	
Systems Development, Maintenance and Configuration Management						
Security requirements of systems						
Security in application systems						
Cryptographic controls						
Security of system files						
Security in development and support processes						
Department continuity management						
Disaster Recovery						
Backup and recovery						
Compliance						
Compliance with legal requirements						
Review of security policy and technical compliance						
System audit considerations						

KEY:

V= Very Significant, L= Less Significant, NA= Not Applicable
IT= Information Systems Department responsibility for documentation.
D= Using department responsibility for documentation.