county of ventura

J. MATTHEW CARROLL
Chief Information Officer

INFORMATION SERVICES DEPARTMENT
Hall of Administration L #1100
800 South Victoria Avenue
Ventura, California 93009
(805) 654-5013
FAX: (805) 654-3394

M. Lowry Gilbert
Assistant Chief Information Officer

August 29, 2003

Honorable Bruce A. Clark
Presiding Judge of the Superior Court
Ventura County Hall of Justice
800 South Victoria Avenue
Ventura, California 93009

Regarding: Response to the 2002-2003 Ventura County Grand Jury report entitled *County Information Technology Security*

Dear Judge Clark:

In accordance with California Penal Code section 933.05, I am providing the attached responses to the above subject Grand Jury report. Please note that in addition to responding to all findings and those recommendations specifically assigned to me, I am also responding to all conclusions reached. For those recommendations specifically assigned to me as the County Chief Information Officer, I have included recommended alternative approaches, next steps, and/or anticipated completion timeframes, as appropriate.

Grand Jury recommendations R-1 and R-4, the later of which is being responded to by the CEO, will be placed on the September agenda of the Information Technology Committee (ITC) for further discussion. I will forward additional information on the ITC's decisions in these areas as such decisions are reached. In the interim, please let me know if there is anything further I can do to respond to the issues raised within the subject report.

Sincerely,

J. Matthew Carroll
Chief Information Officer

Attachment

F:\ISD\Admin\Word\Matt\L_03_GrandJurySecurityResponse.doc

Response to 2002-2003 Ventura County Grand Jury Report Entitled
County Information Technology Security
August 29, 2003

Findings:

I materially concur with all findings documented within the report.

Conclusions:

C-1. The County network, as it is currently managed, is un-securable and has elements that are duplicative.

I concur with this conclusion. However, network security is a spectrum, as opposed to an end-state, and trade-offs must continually be made between network usability and security. No large government or modern corporate network is completely securable and the County's network is not dissimilar to those of the majority of large government organizations with a mix of central and decentralized IT environments.

Current County policy allows for agency and departmental administration of local area networks (personal computers and department servers). This approach facilitates flexibility and control on the part of individual agencies and departments. However, this approach does make it difficult, if not impractical, to ensure that every County department, vendor, and business partner are adhering to County IT security policies and guidelines at acceptable levels. The County's recent experience with the SQLSlammer and MSBlaster worm attacks give evidence to this fact. Lack of full adherence to the County's Virus Protection Policy and Program combined with likely transmission of both worms through trusted vendor, employee, or business partner connections are the root causes of these incidents materially impacting the County.

To address the above ongoing challenges, the County implemented a formal, Countywide IT Security Program in 2002. This program is one of the more comprehensive and progressive county-level programs within the state. This said, the program is in its infancy and while full security compliance remains an elusive and potentially cost prohibitive end state, there is and will continue to be significant opportunities for on-going improvements. Current areas the County IT Security program are focusing on include: staff education and awareness, software patch management, virus protection, network perimeter hardening, administrator and server certification, and IT Security related policy development. As a result of the County's recent experience with the MSBlaster worm, special emphasis will be immediately placed on patch management and virus protection.

With regard to duplication, agency and department administration of local area networks by its nature results in increasing duplicity in staff and computing resources across the County organization. Similar to network security, this is a range/spectrum issue that must be continually managed by the County and balanced against agency and department need for flexibility and control.

With the current financial constraints facing the County, increased attention should be given to the issue of duplication on the part of the ITC, Chief Information Officer (CIO), and County Executive Office. Identifying opportunities for cost and resource savings should be the highest priority of the ITC. An outside analysis of possibilities in this area, as stated in recommendation R-4, would be beneficial, yet costly, if the appropriate level of research and analysis required to make effective recommendations were done.

Adoption of a shared services model for many aspects of County IT service, where agencies and departments direct and manage IT service delivery from a common internal or external service delivery entity, holds perhaps the greatest promise to eliminate Countywide IT redundancy, while assuring agency and departmental control over their service delivery requirements, quality, and service levels.

C-2. Network Security and Application Security are distinct functions.

I concur with this conclusion. Application Security can and should be managed by departments; however, network security and all the security issues associated with ensuring network security should be the responsibility of a centralized security function.

C-3. Vendors and contractors need access controls that are as good as employee controls.

I concur with this conclusion. This is arguably the County's biggest security challenge. One of the primary IT Security Program initiatives for 2003-2004 is to improve security by increasing the level of coordination with every entity that connects to the County's network infrastructure, including departments that manage their own departmental servers and vendor/partners that need direct access to data sources on the County network. Our efforts will cover:

i. Improved access authentication
ii. Modified contracts that clearly explain vendor responsibility for server hardening, patch management, access control, employee turnover notification systems, and vendor security management responsibility guidelines.

In addition to the need for improved vendor access controls, there is also the need to improve employee access controls. As a result of both manpower constraints and the growing number of unique County systems and related authentication directories, agencies and departments are struggling to maintain current employee access controls. In many cases, employees who have left County employment remain as authorized users of one or more County systems for an extended or indefinite period of time. Implementation of a Countywide master employee directory maintained by the primary County Human Resources/Payroll system is being investigated as a solution to this issue. In the future, this directory would replace or interface with unique agency and department

directories, assuring employees are added or deleted from such directories as they are terminated within the main County HR/Payroll system.

C-4. Security vulnerabilities exist in the areas of training, procedures, and internal controls, not in the technology itself.

I concur with this conclusion.

Recommendations:

R-1. The ITC should sponsor an ISO 17799-based risk analysis of a major agency's systems as a means of creating a Countywide risk analysis procedure based on 17799.

I concur in principle with this recommendation. However, it must be pointed out that International Standards Organization (ISO) compliance is a time consuming and expensive process traditionally beyond the financial and resource means of most local government organizations. ISO 17799, like the many other ISO standards, entails complicated analysis, planning, documentation, and audit process spanning 10 different areas including security, personnel safety, and access controls, among others.

Alternatively, the County's Information Technology Program, initiated in 2002, is focusing on several subset areas of ISO 17799 where it has been identified the County is most currently at risk. These areas include server hardening, server patch management, user awareness training, password management, wireless network access, third party network access procedures, network vulnerability assessment and remediation, and IT security incident response, among others.

This recommendation will be discussed at the upcoming September meeting of the County ITC to determine if further expanding the County's IT Security Program to address additional areas of ISO 17799 and conducting an ISO 17799 risk analysis pilot are practical.

R-2. ITC should create a system that better identifies system criticality.

I concur with this recommendation. An application/system criticality rating will be added to the requirements for Departmental Annual IT Plans due in the fall of 2003 .

R-3. Auditor/Controller should base IT audits on 17799.

As noted in my response to recommendation R-1, I concur in principle with this recommendation; however, due to concerns regarding its fiscal practicality for local government, I recommend continuing with the Auditor-Controller's recently

implemented IT Policy Audit Program. This Program calls for annual audits of all agencies and departments on specific, changing IT policy issue areas. As noted in my response to recommendation R-1, this topic will be on the agenda of the September 2003 ITC meeting.

R-5. County Counsel should develop, with the help of ISD, contract language to be inserted into standard County contracts to deal with security issues.

I concur with this recommendation. ISD staff are currently working with County Counsel to incorporate language to address the following issues and exposure areas relative to vendor and business party security:

- Token sharing
- Notification when vendor employees leave
- Management system for proper use of vendor tokens
- Legal recourse for County if vendor is not in compliance
- Vendor server, computer administration, and virus protection procedures.

The appropriate text should be developed and available for inclusion in County contracts by September 30, 2003.

R-7. ISD should provide a Countywide security training package for County employees.

I concur with this recommendation. ISD staff are currently working with the Human Resources Division to develop an Information Security Awareness training module that will be integrated into the periodic Countywide Security Awareness training required of all County employees and the new employee orientation/training required upon initial employment with the County. The Information Security Awareness module will consist of classroom training, demonstration activities, and information pamphlets for employees.

Additionally, ISD has implemented an ongoing Security Forum that discusses Information Security for system administrators. This forum presents information in a highly technical format that is appropriate for advanced administrator professionals. Attendance at this forum will be a recommended requirement of the administrator certification program discussed in response to recommendation R-8 below.

The Security Forum is currently being conducted on a monthly basis. Completion of the User IT Security module and related material is scheduled for completion by September 30, 2003

R-8. ISD should create a system to certify Trusted Net Administrators and Systems.

I concur with this recommendation. As part of the Countywide IT Security Program, ISD is working with an ITC subcommittee, the County Business Technology Committee (BTC), to develop an updated list of hardware and software standards with which County vendors, business partners, internal servers, and in some cases desktops must comply (or risk becoming disconnected from the County's infrastructure). These standards include the following:

i. Patch management procedures
ii. Server hardening procedures
iii. Token management and authentication procedures
iv. Antivirus/worm software standards
    1. Virus/worm notification procedures
v. Vulnerability testing procedures
vi. Physical security standards
vii. Others areas and procedures to be determined

ISD will also be working with the BTC subcommittee to develop a Certification Guideline for system administrators who are responsible for servers that connect to the County's Network Infrastructure. These will include:

i. Training/experience guidelines for administrators
ii. Security Forum attendance requirements
iii. Reporting requirements on security related system issues
iv. Certification tests for administrators

Both the administrator certification programs and the updated standards will be in place by the end of the current calendar year.