PHYSICAL SECURITY OF THE CITY'S LOCAL AREA NETWORK

AUDIT REPORT #0106

DECEMBER 2000

CITY OF TALLAHASSEE

Copies of this report may be obtained by telephone (850 / 891-8397), by FAX (850 / 891-0912), by mail or in person (City Auditor, 300 S. Adams Street, Mail Box A-22, Tallahassee, FL 32301-1731), or by e-mail (dooleym@mail.ci.tlh.fl.us).

CITY OF TALLAHASSEE

CITY HALL
300 S. ADAMS ST.
TALLAHASSEE, FL
32301-1731
850/891-0010
TDD 1-800/955-8771

SCOTT MADDOX
Mayor
CHARLES F. BILLINGS
Mayor Pro Tem

JOHN PAUL SALLY
Commissioner
DEBBIE LIGHTSEY
Commissioner
STEVE MEISBURG
Commissioner

ANTHAR FAVORS
City Manager
ROBERT B. INZER
City Treasurer-Clerk

JAMES R. ENGLISH
City Attorney
SAM M. McCALL
City Auditor

MEMORANDUM

To: Mayor and Members of the City Commission

From: Sam M. McCall, City Auditor

Date: December 18, 2000

Subject: Audit Report on Physical Security of the City's Local Area Network (#0106)

We have completed an audit of the Physical Security of the City's Local Area Network (#0106). We submit this report that contains our audit issues and recommended actions and the response from the City Manager. We will periodically review the implementation of these recommended actions.

We thank the staff of the Department of Management and Administration, Information Systems Services, for their cooperation and assistance during this audit. If you have any questions or need a more detailed briefing on this audit, please contact me.

Respectfully submitted,

Sam M. McCall
City Auditor

SMM/mbd
attachment

Copy: Members of the Audit Committee
Appointed Officials
Executive Team
Donald C. DeLoach, Chief Information Systems Officer
Terald Baker, Technology Infrastructure Administrator
Paula G. Cook, Records Administrator

Table of Contents

Audit Report

CITY OF TALLAHASSEE

Sam M. McCall, CPA, CIA, CGFM
City Auditor

"Physical Security of the City's Local Area Network"

Report #0106 *December 18, 2000*

Executive Summary

Physical security over the City's local area network (LAN) needs to be improved to adequately protect the City's information technology resources. This also includes security over the inventory of equipment waiting to be installed as part of the City's LAN.

The City's Physical Security Needs to Increase as the Number of Locations Housing Information Technology Resources Increases

As the City evolves from a centralized computing environment to a more decentralized computing environment, the physical security needs to increase as the number of locations housing information technology resources increases. Physical security controls include restricting physical access to the information systems resources, protecting these resources from environmental hazards, and having the ability to restore operations should the resources become damaged or destroyed.

During March through September 2000, the Office of the City Auditor conducted an evaluation of the physical security controls that protect the City's LAN resources. The purpose of this report is to present the general issues identified and the associated recommendations. In addition, we will separately provide management with the identified security weaknesses for each location housing the City's LAN equipment. Evaluations of security programs for information technology resources are exempt from public records to prevent improper disclosure of information that could result in unauthorized

access, modification, and/or destruction of information resources, such as equipment, programs, and data. [1]

Critical Policies and Procedures Are Needed to Address Physical Security and Backup Strategies

The results of our audit indicate critical policies and procedures need to be developed and implemented to address physical security and backup strategies for the City's information technology resources. These policies and procedures should be distributed to departments housing LAN equipment.

Existing Physical Security Weaknesses Should Be Corrected At Locations Housing Major and Minor LAN Equipment

Our tests showed that there were physical security weaknesses at locations that house both major and minor LAN equipment throughout the City. Corrective actions should be taken to provide the appropriate level of physical security for the locations housing LAN equipment.

An Information Security Manager Should Be Designated

In addition, an information security manager should be designated to: oversee the implementation of the information security policy, assess security risks and recommend corrective actions, increase security awareness by City employees, and monitor security measures.

ISS Should Improve Their Process to Account for Computer-related Equipment Received, Distributed, and Stored

We also noted that Information Systems Services (ISS) should implement procedures to ensure that purchased networking equipment is recorded into inventory and that there is a clear chain of custody in order to safeguard against potential theft or loss.

Appendix A provides management's action plan to address these identified issues. We would like to thank staff from ISS and all the departments that house the City's LAN equipment for their support and assistance during this audit.

[1] Section 119.07(1)(o), *Florida Statutes*

Audit Report

CITY OF TALLAHASSEE

Sam M. McCall, CPA, CIA, CGFM
City Auditor

"Physical Security of the City's Local Area Network"

Report #0106 *December 18, 2000*

Purpose

The purpose of this report is to evaluate the physical security controls protecting the City's local area network (LAN) resources.

Scope and Objectives

The scope of this audit includes the physical security of all City LAN infrastructure equipment, including, but not limited to: network servers; hubs; switches; telecommunications devices, such as integrated services digital network (ISDN), and fiber optic connections; and purchased and stored computer equipment that is intended to be connected to the LAN. Fieldwork took place during March through September 2000.

Our objectives were to:

- obtain a general understanding of the network operations and the physical location of all network servers and other LAN infrastructure equipment;
- evaluate the physical control environment of the network servers and other LAN infrastructure equipment;
- evaluate the physical control environment of purchased LAN equipment waiting to be installed.

Background

City's Computing Environment

The City relies on computers and electronic data to perform functions that are necessary to provide services to the citizens of Tallahassee. Examples of these services include

police and fire dispatching and reporting; electric, water, gas and solid waste operations; public works operations (traffic, streets and drainage); growth management and permitting; bus operations; and financial reporting.

City is Migrating from a Centralized to a Decentralized Computing Environment

The City, like other government and private industries, is migrating from a centralized mainframe environment to a decentralized (or distributed) client/server environment. In a mainframe environment, all users are connected to one central location for the hardware, software, and data; and management, authority, budget, and responsibility are centralized in one location, typically within the Information Systems Services division. One central location makes it easier to provide a physically secure location with special building features to control and monitor access, monitor environmental conditions, and plan for emergencies.

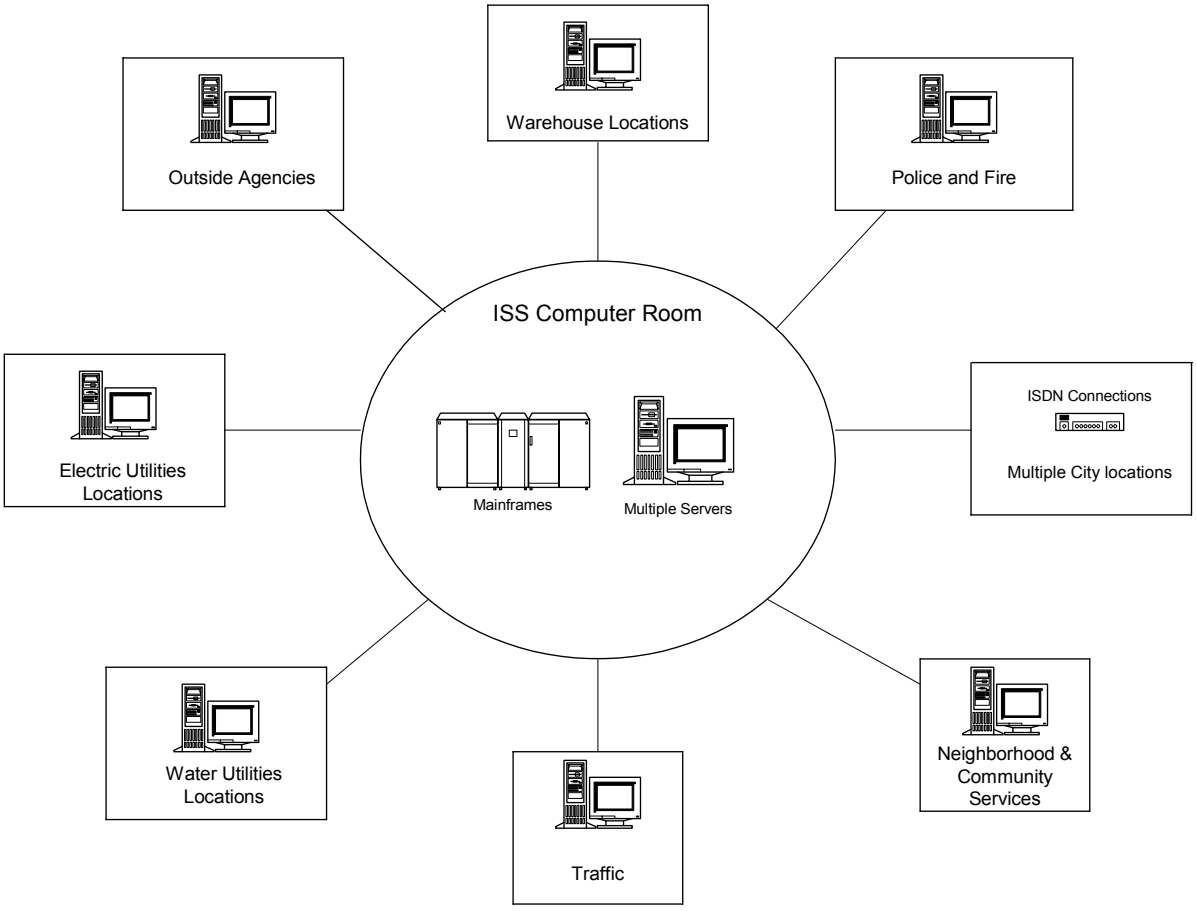
In the client/server environment, all users (also called clients) are connected to one or more servers. This client/server environment is replacing the mainframe environment that has been prevalent during the past 30-40 years. The design of the client/server environment distributes the functionality of the mainframe, including programs and data, primarily to the server and secondarily to the users' computers. This environment is based upon concurrent processing to increase the flexibility and power at the users' desktops.

The City's LAN is Increasingly Providing the Backbone to House and Transmit Data to and from Multiple Locations Throughout the City

The distributed client/server environment operates on a LAN. A LAN is a communication network that serves many users within a geographical area and consists of servers, workstations, a network operating system, and a communications link. The City's LAN is increasingly

providing the backbone to house and transmit data to and from multiple locations throughout the City. Many users are connected to one server, and then servers are connected to each other creating a large client/server environment. Figure 1 provides a basic illustration of the multiple locations housing LAN equipment. Each location is connected to the primary domain server located in the ISS computer room.

Figure 1
City's Local Area Network



There is an Increased Need to Secure the LAN Equipment Just as the City has Previously Secured the Mainframe Equipment

While LANs provide increased flexibility and functionality, there are associated risks. Servers are smaller than mainframes and can be housed in multiple locations outside of the one computer room. Since LANs are now the backbone of business operations, there is an increased need to secure the LAN equipment just as we have previously secured the mainframe equipment. As shown in Figure 1, the City's LAN equipment is housed in many locations other than the ISS computer room. It becomes the responsibility of the departments to provide adequate security for the equipment housed in their buildings.

Defining Physical Security

Security for information systems can be defined as the "control structure established to manage the integrity, confidentiality, and availability of information systems data and resources."[2] There are two basic types of security controls that together can protect data and resources:

- ***Physical -*** restricting physical access to the information systems resources and protecting against environmental hazards; and
- ***Logical -*** restricting access into specific information systems so that only authorized individuals can perform functions on the system.

This audit is limited to the physical security of the City's LAN. Logical security of the City's LAN will be addressed in a subsequent audit.

[2] Systems Auditability and Control, Module 9 "Security," Institute of Internal Auditors Research Foundation

Activities that protect computer equipment from physical damage include:

- allowing only those persons responsible for maintaining the computer equipment into the rooms housing computer equipment;
- providing detection features to alarm staff of conditions related to heat, fire, smoke, water, dust/dirt, etc.;
- storing hazardous materials, such as cleaning chemicals, in separate locations from the computer equipment;
- providing an uninterruptible power supply to ensure continuity of the information systems and prevent damage from abrupt power outages or surges; and
- planning how to efficiently and effectively restore operations, including backing up programs and data.

Each Location Housing LAN Equipment Should Provide an Adequate Level of Physical Security Protection

Each location housing LAN equipment in a decentralized LAN environment should provide an adequate level of security to protect the computer equipment from damage. Such physical security controls should include limited access, environmental safeguards, uninterruptible power supplies, and reliable and sufficient backup and recovery procedures.

Methodology

During our review of the physical security controls related to the City's LAN, we identified all locations that house network equipment. Working with ISS, we classified the LAN equipment as "major" or "minor," with the understanding that major LAN equipment would require a greater level of security than minor LAN equipment. Major LAN equipment would include servers, since they perform the same functions as mainframe computers and require the same level of physical security. Minor LAN equipment would

include simple telecommunication connections, such as integrated services digital network (ISDN), fiber optic connections, modems, and telephone lines. Figure 2 describes the typical physical security features for locations housing minor and major LAN equipment.

Figure 2
Physical Security Features

For Locations Housing Minor LAN Equipment
√ Written standards that address physical security of network resources
√ Insurance coverage
√ Locked rooms allowing access to only authorized persons via keys, pass-codes, etc.; and management of granting and removing access
√ Service logs for monitoring who works on the equipment
√ Fire and smoke detection devices in the room
√ Fire extinguishers that have been recently inspected

For Locations Housing Major LAN Equipment (In addition to those features required for minor LAN equipment)
√ Policies and procedures addressing backup strategies and requirements
√ Locating the computer room in an interior room so no entry is possible via an exterior door or window
√ Access logs for monitoring who enters the location
√ Servers and equipment located off the floor to protect against flooding
√ Humidity and temperature controls within the room
√ Uninterruptible power supply (UPS) that provides adequate power and is tested periodically
√ Backups of needed programs and files stored securely on-site and off-site

To obtain a general understanding of the network operations and the physical location of all network servers and equipment, we interviewed key contacts from Information Systems Services and the departments that house City LAN equipment, reviewed infrastructure designs, network diagrams, and other relevant documentation.

To evaluate the physical control environment of the network servers and equipment and the storage location of purchased LAN equipment waiting to be installed, we: interviewed key individuals responsible for the location's maintenance and security; visited each location and evaluated the physical and environmental conditions relating to the physical security controls stated above; and conducted an inventory of the purchased and stored equipment to ensure physical controls were adequate to account for all equipment.

Fieldwork took place during March through September 2000. This audit was conducted in accordance with Generally Accepted Government Auditing Standards.

Significant Issues and Recommendations

The purpose of this report is to present the general issues identified and the associated recommendations. In addition, we will separately provide management with the identified security weaknesses for each location housing the City's LAN equipment. Evaluations of security programs for information technology resources are exempt from public records to prevent improper disclosure of information that could result in unauthorized access, modification, and/or destruction of information resources, such as equipment, programs, and data.[3]

[3] Section 119.07(1)(o), *Florida Statutes*

Below is a description of the general issues identified and categorized in the following areas: policies and procedures; physical security weaknesses at locations housing major and minor LAN equipment; information security management; and inventory controls over purchased computer-related equipment at ISS.

Policies and Procedures Addressing Physical Security of LAN Equipment Should be Developed and Distributed.

Policies and Procedures have not been Developed to Address the Physical Security of the City's Computing Environment

Currently, there are no written policies and procedures that address how to physically protect the City's computing environments, including the mainframe and client/server. Traditionally, the majority of major computing equipment has been housed in the ISS computer room, and, therefore, ISS would have experience protecting its computer equipment, programs and data. ISS does not have any written standards regarding what should be done to protect the City's computing environment. Since the City now has a distributed network environment with equipment housed in many different locations managed by different departments, ISS should develop and distribute written standards regarding how departments should protect their computer resources from potential damage, including loss of data, and disruption of critical operations and services.

Policies and Procedures have not been Developed to Address Backup and Recovery

Also, there are no written policies and procedures that address the City's strategy and requirements for backup and recovery of operational and critical data. The responsibility for whom is to backup specific programs and data varies. In most cases, ISS is responsible; however, there are situations where the executive owner is responsible. There have been isolated incidents during the previous year when backups were not conducted as the executive owner expected, and critical data was lost.

Internal Control Guidelines (Administrative Policies and Procedures #630) states that internal control may consist of procedures, policies, information guides, and department operation guides. "Policies establish the organization's direction, while procedures indicate how policies are to be implemented and followed.....Sound policies and procedures provide benchmarks against which compliance can be measured and contribute to an effective control environment."[4]

Without effective policies and procedures, there are no guidelines for City departments to follow to ensure that computer resources are protected against physical and environmental threats. Computer equipment that has not been adequately protected can be damaged, either inadvertently or maliciously, resulting in a disruption of critical operations and services.

Recommendations Related to Physical Security Policies and Procedures, Including Backup and Recovery

We recommend that ISS management develop, obtain approval, and distribute appropriate policies and procedures to protect the City's computer resources. Such policies and procedures should address physical security requirements for both major and minor computer facilities, as well as protection against environmental hazards.

In addition, we recommend that ISS work with executive owners to develop written policies and procedures to address the criteria for what is to be backed up, how often, by whom, and where the backup media will be stored. Such procedures should be implemented to ensure that: backups have been conducted as intended; backup media are

[4] Systems Auditability and Control, Module 2 "Audit and Control Environment," Institute of Internal Auditors Research Foundation

regularly stored at a secure off-site location; and the backup media are adequately protected from physical and environmental hazards.[5]

Physical Security at Locations Housing Major LAN Equipment Should Be Improved.

During our audit, we identified and visited nine locations housing major LAN equipment, such as servers. Figure 3, on the next page, shows weaknesses that were present in at least two locations. The most common physical security weaknesses at the locations housing major LAN equipment were:

Common Physical Security Weaknesses At Locations Housing Major LAN Equipment

- the lack of water detection devices should water come into the room. This risk is increased when the LAN equipment is located directly on a floor that is not raised.
- the lack of monitoring who accesses the room. This risk is increased with the lack of adequate control over who is allowed access to the room, the lack of control over the keys, and/or doors not being kept locked.
- the room housing the equipment is not located in an interior room increasing the risk that it can be accessed via an exterior door or window.

[5] Control Objectives for Information and Related Technology, Information Systems Audit and Control Foundation, 1996

Figure 3
Physical Security Weaknesses Identified at Locations Housing Major LAN Equipment

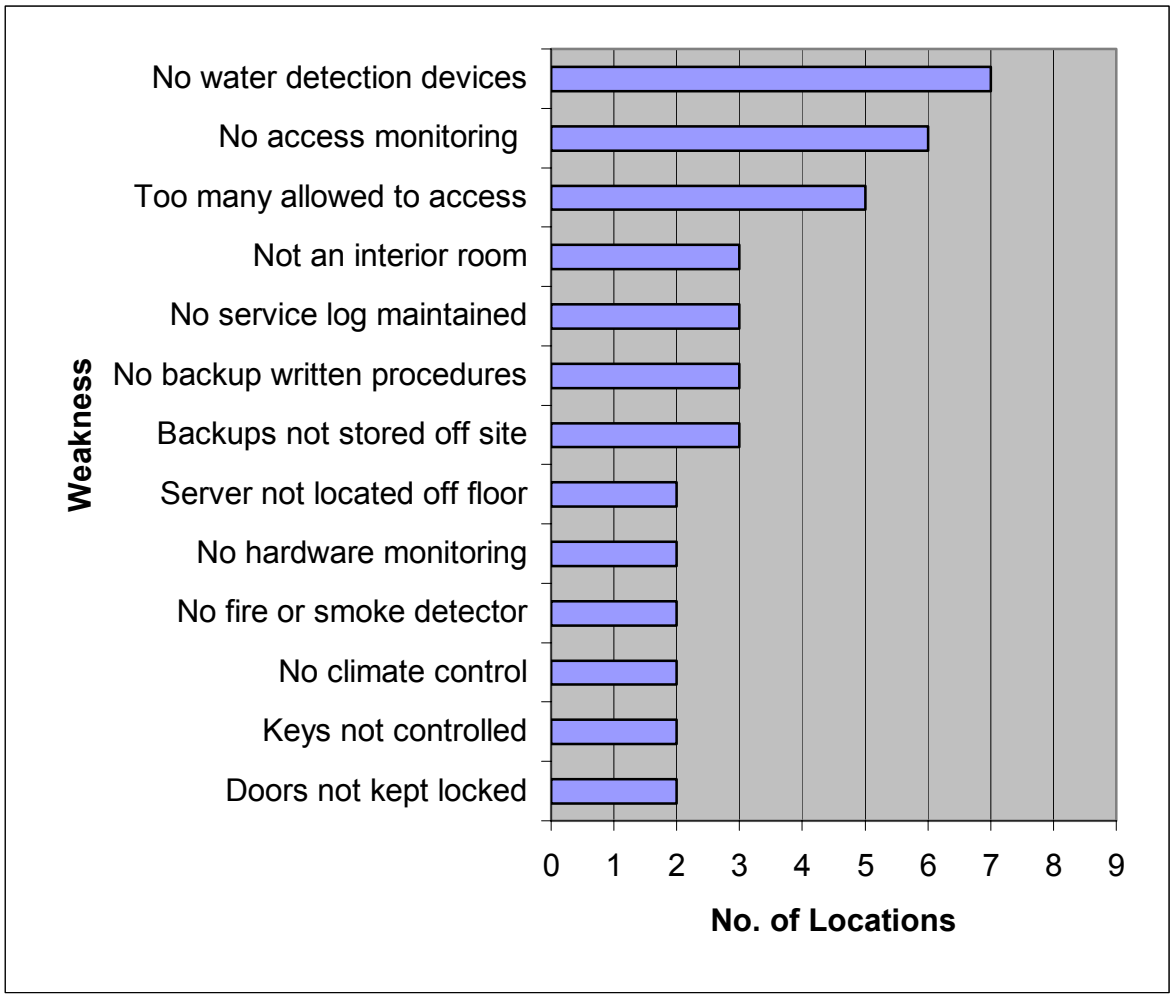
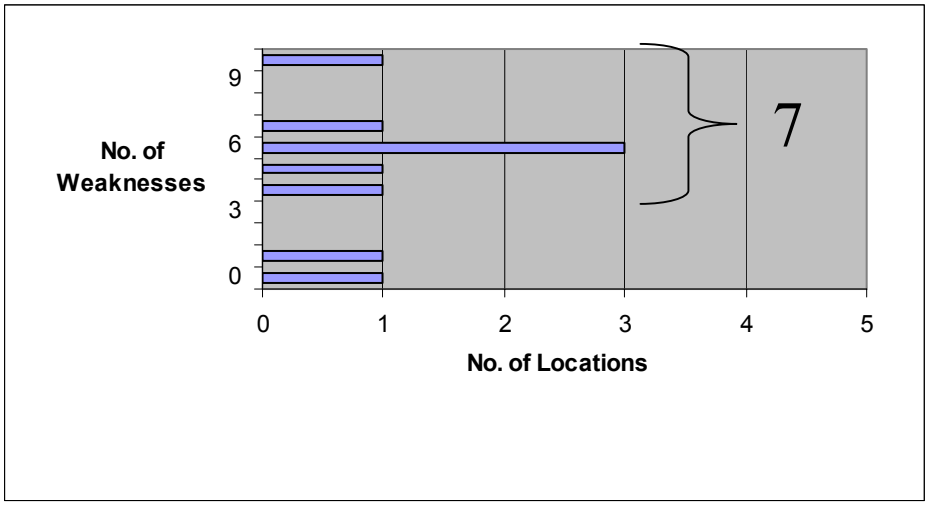


Figure 4, on the next page, shows the number of locations housing major LAN equipment and the number of weaknesses at each location. Overall, of the nine locations, there were seven locations housing major LAN equipment that had at least four physical security weaknesses. Specifically, we identified four weaknesses at one location, five weaknesses at one location, six weaknesses at three locations, seven weaknesses at one location, and ten weaknesses at one location.

Figure 4
Number of Locations Housing Major LAN Equipment with Physical Security Weaknesses



Physical Security at Locations Housing Minor LAN Equipment Should Be Improved.

Also during our audit, we identified and visited 23 locations housing minor LAN equipment, such as simple telecommunication connections (i.e., ISDN, fiber optic connections, modems, and telephone lines). Figure 5, on the next page, shows weaknesses that were present in at least two locations. The most common physical security weaknesses at the locations housing minor LAN equipment were:

Common Physical Security Weaknesses at Locations Housing Minor LAN Equipment

- The lack of fire/smoke detection devices in the room.
- Allowing too many persons to enter the room and not monitoring access. Additional risks include keeping the door unlocked, not controlling who has keys, and using the room for storage.
- Room being excessively dusty and dirty which can negatively impact the functioning of equipment.

Figure 5
Physical Security Weaknesses Identified at Locations Housing Minor LAN Equipment

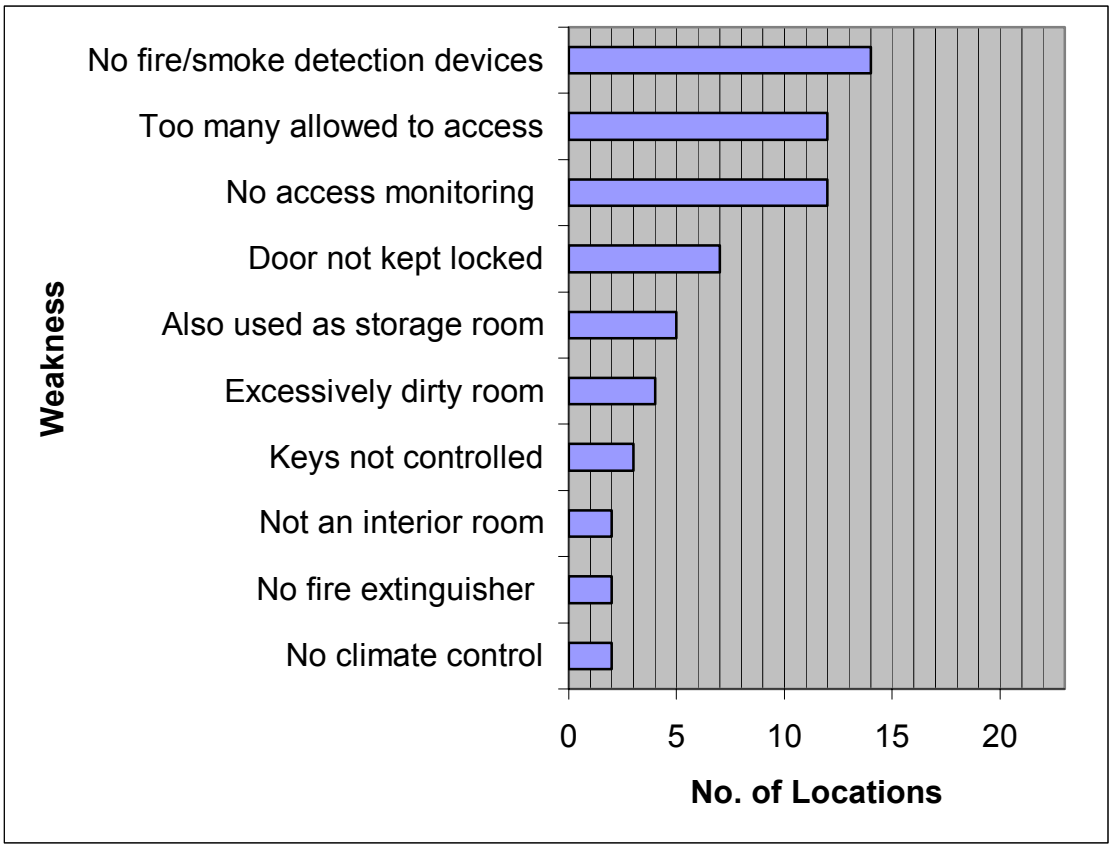
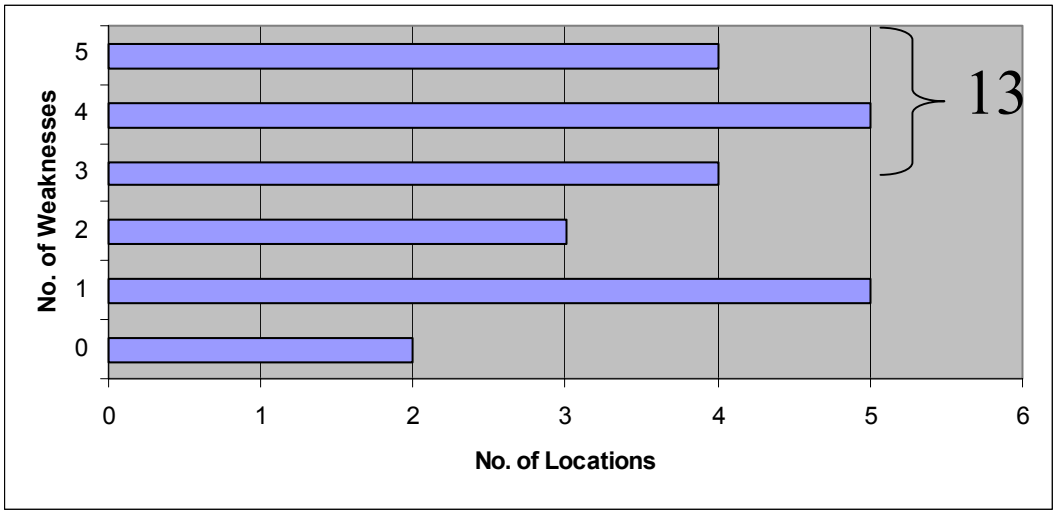


Figure 6, on the next page, shows the number of locations housing minor LAN equipment and the number of weaknesses at each location. Overall, of 23 locations, 13 separate locations had between 3 and 5 physical security weaknesses. Specifically, we identified three weaknesses at four locations, four weaknesses at five locations, and five weaknesses at four locations.

Figure 6
Number of Locations Housing Minor LAN Equipment with Physical Security Weaknesses



Controls should be in place to limit access to data, programs, and hardware to those individuals authorized to operate or maintain specific systems. Such controls should also include protection from environmental conditions, such as heat, humidity, excessive dust, and static electricity.[6] Owners of computer facilities and equipment are responsible for the physical protection of these resources. If a resource has multiple persons responsible, then policies should clearly describe the minimum security requirements to be implemented.[7]

Without adequate physical security controls in place to protect locations housing both major and minor LAN equipment, there is an increased risk that computer resources can be damaged physically, either inadvertently or maliciously, or environmentally resulting in a disruption of

[6] Systems Auditability and Control, Module 9 "Security," Institute of Internal Auditors Research Foundation
[7] Federal Systems Controls Audit Manual, Volume 1, "Financial Statement Audits," U.S. General Accounting Office

critical operations and services.

Recommendations Related to the Existing Physical Security Weaknesses

We recommend that management take corrective actions to provide the appropriate level of physical security for the locations housing major and minor LAN equipment. Such actions should include periodically evaluating the physical security features at each location, including:[8]

- locating the equipment in an interior room;
- limiting access to only authorized persons;
- providing fire/smoke detection devices and fire extinguishers;
- keeping the room free of excessive dust and dirt; and
- having a working cooling system.

An Information Security Manager Should be Formally Designated to Manage Information Security Activities in the City.

There is No One Person or Section Designated to Manage Information Security Activities Throughout the City

ISS provides some network security activities, and some executive owners provide some security activities over their application system, but there is no person or section designated to manage the information security activities throughout the City.

Security-related responsibilities of offices and individuals throughout an entity that should be clearly defined include (1) information resource owners and users, (2) information resources management and data processing personnel, (3) senior management, and (4) security administration.[9]

Without a person designated to be responsible for the information security activities, there is no assurance that information security is being considered, evaluated, or monitored in the City. This increases the risk that the City's

[8] Federal Systems Controls Audit Manual, Volume 1, "Financial Statement Audits," U.S. General Accounting Office

[9] Federal Systems Controls Audit Manual, Volume 1, "Financial Statement Audits," U.S. General Accounting Office

information technology resources could be damaged or destroyed by unauthorized persons.

Recommendation Related to Managing Information Security

We recommend that management formally assign the responsibility for assuring security of the City's information resources to an information security manager, reporting to senior management.[10] This person should be independent of the departments that manage and maintain the systems and facilities that require information security. Such responsibilities would include: overseeing the implementation of information security policies and procedures, assessing security risks and recommending corrective actions, increasing security awareness by City employees, and monitoring security measures.

ISS Should Improve Inventory Processes for LAN Equipment Under Their Control and Waiting to be Installed.

Weaknesses in Internal Controls Over Inventory

As stated previously, ISS is responsible for purchasing and installing all computer hardware and software for City departments. When a vendor delivers the purchased equipment, it is received by ISS and stored in a designated storage room. ISS is solely responsible for the security and accountability for this computer equipment. According to ISS management, it is their intent for this to be a staging area, meaning that the equipment would be installed in the departments shortly after it is received. Some of the purchased equipment has remained in the storage area for extended periods, creating an inventory of computer equipment. ISS has not implemented procedures to provide proper inventory controls over this computer equipment. Specifically:

[10] Control Objectives for Information and Related Technology, Information Systems Audit and Control Foundation, 1996

1. Internal controls over the purchased computer equipment were deficient, i.e.:
   - no perpetual inventory records;
   - no periodic count or inventory;
   - lack of segregation of duties; and
   - chain of custody not maintained.
2. We noted that adequate records were not always maintained to indicate what equipment had been received, delivered to the departments, or was being held. To date, ISS has used a "control document" to track the physical location of the computer equipment while it is in the ISS inventory. We identified instances of equipment on hand in the ISS staging area, and there was no accompanying control document. Conversely, we also noted instances of control documents on hand in ISS, and there was no accompanying equipment in the ISS staging area.
3. There was no organization within the storage room. Equipment ordered for departments was stored along with surplus equipment, spare parts, and replacement equipment.

Subsequent to our review, ISS management has taken steps to locate the control documents and equipment that we were not initially able to locate during our fieldwork. The majority of the equipment had been delivered to the departments or was to be used as spare parts, but the documentation had not been completed. ISS management concluded that the discrepancies noted indicated the need for procedural changes, including, but not limited to:

- keeping replacement stock separated from equipment ordered for departmental use;
- establishing procedures to age inventory in the staging area to ensure that it is delivered in a timely manner; and
- verifying order completeness at the time the equipment is received.

In addition, ISS has implemented a new helpdesk software application that will provide a tool enabling them to better

monitor the status and location of ordered computer equipment and manage their inventory records.

City Administrative Policy and Procedure #630, "Internal Control Guidelines," requires that "equipment, inventories, securities, cash and other assets should be secured physically (by location, tagging, restricted access), and periodically counted and compared with amounts shown on control records."

Without adequate inventory controls, there is an increased risk that the loss or theft of networking equipment would not be detected in a timely manner.

Recommendation Related to Inventory Controls

We recommend that ISS management continue their efforts to implement proper procedures to ensure that: purchased networking equipment is received and recorded into inventory; there is periodic comparison of equipment on hand to equipment of record; there is a proper segregation of duties; and there is a clear chain of custody to safeguard against potential theft or loss.

Conclusion

It is our opinion that the physical security controls over the City's LAN infrastructure equipment need to be improved to adequately protect the City's information technology resources. This includes: developing and implementing physical security policies and procedures, including backup and recovery of the City's programs and data; correcting the existing physical security weaknesses at locations housing major and minor LAN equipment; designating an information security manager; and improving ISS's process to account for computer-related equipment received, distributed, and stored.

Management's action plan to address the significant issues identified in this report is presented in Appendix A. We would like to thank staff from ISS and all the departments that house the City's LAN equipment for their support and assistance during this audit.

Response from Appointed Official

City Manager:

We appreciate the City Auditor's office partnering with us on improving the physical security of our City data assets. We recognize the importance of providing safeguards to insure the City's protection against data loss.

The decentralization of the computing hardware environment has presented us with new challenges and has increased our awareness of providing acceptable physical security standards. DMS/ISS is making every effort to coordinate and plan for the future policy changes needed to insure our physical assets are protected against potential loss.

Copies of this audit report may be obtained by telephone (850 / 891-8397), by FAX (850 / 891-0912), by mail or in person (City Auditor, 300 S. Adams Street, Mail Box A-22, Tallahassee, FL 32301-1731), or by e-mail (dooleym@mail.ci.tlh.fl.us).

Audit conducted by:
Beth Breier, CPA, CISA, Information Technology Auditor
Sam M. McCall, CPA, CIA, CGFM, City Auditor

Appendix A - Action Plan		
Objectives and Action Steps	**Responsible Employee**	**Target Date**
A. Objective: ***Designate an information security manager to manage and monitor the City's information security policies and procedures.***		
1. Obtain approval for an information security manager position and fill position.	Don DeLoach David Reid	10/2001
B. Objective: ***Develop, obtain approval, and distribute appropriate information security policies and procedures. Educate and train department staff regarding the information security policies and procedures in order to protect the City's computer resources.***		
1. Develop information security policies and procedures that address physical security of LAN equipment throughout the City.	Terry Baker	06/2001
2. Obtain approval, including: ISS, DMA, and City Manager.	Terry Baker Don DeLoach	08/2001
3. Identify and obtain funding to implement security requirements per the approved information security policy.	Terry Baker Don DeLoach David Reid	10/2001
4. Implement approved policy within ISS and affected departments, including policy distribution and training.	Terry Baker Don DeLoach	10/2001
C. Objective: ***Develop written policies and procedures to address the criteria for what is to be backed up, how often, by whom, and where the backup media will be stored. Ensure that backups have been conducted as intended and that the backup media are adequately protected from physical and environmental hazards.***		
1. Develop written ISS policies and procedures and timelines for backing up mainframe/servers under the responsibility of ISS. This will also involve the application system development team.	Mike Seagraves Joe Kaparek Terry Baker	03/2001
2. Identify resources, including funding and personnel to implement approved policy and procedures.	Terry Baker Don DeLoach David Reid	04/2001
3. Educate staff regarding the backup procedures and their responsibilities, including computer operators.	Terry Baker Mike Seagraves	05/2001
4. Determine responsibility for ensuring that the backup policies and procedures are performed by proper personnel and staff.	Mike Seagraves Don DeLoach	03/2001

D. Objective: ***Implement corrective measures to strengthen the physical security weaknesses noted at the locations housing LAN equipment.***		
1. Determine who controls the equipment rooms at the locations housing LAN equipment outside City Hall.	Terry Baker Don DeLoach E-Team	02/2001
2. Determine who is responsible for strengthening the physical security.	Terry Baker Don DeLoach E-Team	06/2001
3. Identify resources, including funding and personnel to bring the locations up to approved policy and procedures.	Terry Baker Don DeLoach David Reid	10/2001
E. Objective: ***Implement proper accounting procedures to ensure that purchased computer equipment is safeguarded against potential theft or loss.***		
1. Develop and implement written procedures to provide proper inventory controls over purchased computer equipment. Such procedures will address: ♦ maintaining a perpetual inventory ♦ segregating job responsibilities ♦ conducting physical counts and reconciling records to equipment ♦ maintaining a chain of custody of equipment ♦ monitoring the length of time the equipment is stored by ISS to provide for timely installation of equipment	Mike Seagraves	12/15/00


OFFICE OF THE
CITY OF TALLAHASSEE
REPORTING ON ACCOUNTABILITY WITH A CITIZEN FOCUS
CITY AUDITOR