Florida Educational Entities Technology Today

- Brian Rue, Lead Senior Auditor, Information Technology Audits (brianrue@aud.state.fl.us)

Agenda

- Select Data Center Security Issues
- New Technologies
- Acquisition Best Practices

Systems Security -
To Provide Servers and Protect

Complexities in operating systems and new technologies lessens the chance that a system will ever be constructed that is 100% protected from vulnerabilities.

Figure 4
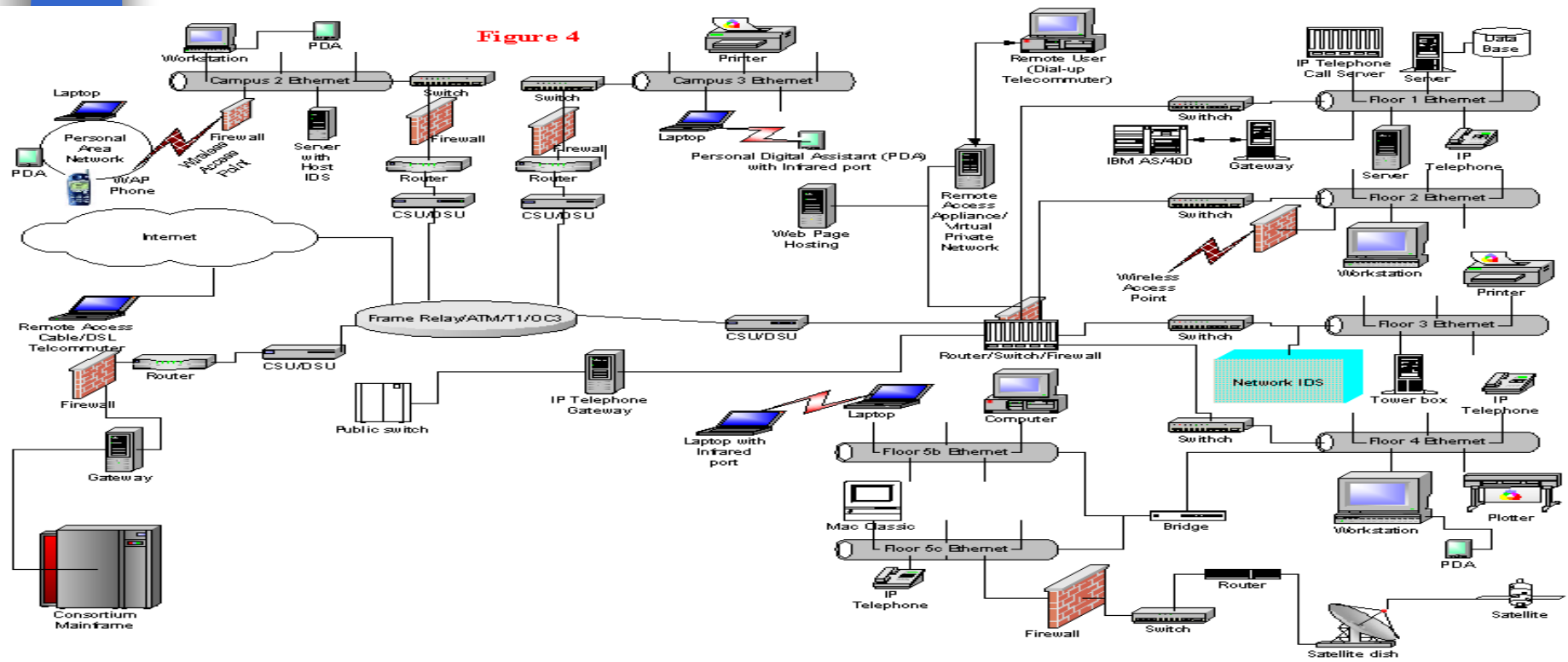
Impediments to Good Security

Stage 1 - Building a Foundation

Creating a formal Risk Assessment of applications and systems

*Identification, classification, and valuation of assets;

*Postulation and estimation of potential threats;

*Identification of vulnerabilities to threats; and

*Evaluation of the probable effectiveness of existing safeguards and the benefits of additional safeguards.

Exhibit C-1. LAN Risk Assessment Worksheet.

Block A - LAN Administrative Information.

the LAN Administrator's:

Case	Justin	C.
(Last Name)	(First Name)	(Middle Initial)

(301) 555-1046   301   IC34
(Phone number)   (Building)   (Room number)

the ICD ISSO's:

Risk	Roger	N.
(Last Name)	(First Name)	(Middle Initial)

(301) 555-1227   4232   224
(Phone number)   (Building)   (Room number)

is the name of the LAN? ALBERT

LAN Administrator responsible for any other LANs? No [X] Yes [ ] How Many? [ ]

Institute, Center, or Division (ICD)
he LAN support? **National Institute of Scientific Excellence (NISE)**

s the Accrediting individual

Driver	Bernoulli	L.
(Last Name)	(First Name)	(Middle Initial)

Director or Designee)?

Buildings or portions of Buildings   **Buildings 301 and 42A**
pported by the LAN?

many servers support the LAN? [1]

many users does the LAN support? [30]

many users have received computer security awareness training? [30] [30]
(Introductory) (In-depth)

an X in the boxes that reflect the types of data maintained on the LAN.

istrative - [X] – General correspondence and information (e.g., property records and personnel information generally available to public).

inancial - [X] – Budget and expenditure information relating to NIH operations.

Contract - [ ] – Information relating to NIH grants and contracts.

Patient - [ ] – Information relating to a patient that is of a personal nature or developed as a result of tests and observations by NIH personnel, contractors, or subcontractors.

prietary - [ ] – Information that is not releasable to the public without the permission of the owner (e.g., a pharmaceutical patent).

esearch - [X] – Information resulting from or used to support NIH research activity.

acy Act - [ ] – Information (not generally available to the public) required to be protected under the Privacy Act of 1974, Public Law 93-579, 5 U.S.C. 552a (1974).

specify) - [ ] –

an X in the box matching the highest cost range shown in right-hand column of Exhibit 2-3.

Very Low	Low	Moderate	High	Very High
<$25,000	$25,001 - 50,000	$50,001 - 250,000	$250,001 - 500,000	>$500,000
[ ]	[ ]	[X]	[ ]	[ ]

te the date of the last risk assessment or
: the box labeled initial risk assessment.   (mo   day   yr)   [X] (Initial risk assessment)

LAN RISK ASSESSMENT

Block A - LAN Administrative Information.

A1. Enter the LAN Administrator's:

(Last Name)	(First Name)	(Middle Initial)

(Phone number)	(Building)	(Room number)

A2. Enter the ICD ISSO's:

(Last Name)	(First Name)	(Middle Initial)

(Phone number)	(Building)	(Room number)

A3. What is the name of the LAN?

A4. Is the LAN Administrator responsible for any other LANs? No ☐ Yes ☐ How Many? ☐

A5. Which Institute, Center, or Division (ICD) does the LAN support?

A6. Who is the Accrediting individual (ICD Director or Designee)?

(Last Name)	(First Name)	(Middle Initial)

A7. What Buildings or portions of Buildings are supported by the LAN?

A8. How many servers support the LAN? ☐

A9. How many users does the LAN support? ☐

A10. How many users have received computer security awareness training? ☐ (Introductory) ☐ (In-depth)

A11. Place an X in the boxes that reflect the types of data maintained on the LAN.

Administrative - ☐ — General correspondence and information (e.g., property records and personnel information generally available to public).

Financial - ☐ — Budget and expenditure information relating to NIH operations.

Grant/Contract - ☐ — Information relating to NIH grants and contracts.

Patient - ☐ — Information relating to a patient that is of a personal nature or developed as a result of tests and observations by NIH personnel, contractors, or subcontractors.

Proprietary - ☐ — Information that is not releasable to the public without the permission of the owner (e.g., a pharmaceutical patent).

Research - ☐ — Information resulting from or used to support NIH research activity.

Privacy Act - ☐ — Information (not generally available to the public) required to be protected under the Privacy Act of 1974, Public Law 93-579, 5 U.S.C. 552a (1974).

Other (specify) - ☐ —

A12. Place an X in the box matching the highest cost range shown in right-hand column of Exhibit 2-3.

	Very Low	Low	Moderate	High	Very High
Cost Rating					
Cost Range	<$25,000	$25,001 - 50,000	$50,001 - 250,000	$250,001 - 500,000	>$500,000
	☐	☐	☐	☐	☐

A13. Indicate the date of the last risk assessment or check the box labeled initial risk assessment.
(mo   day   yr)   (Initial risk assessment)

Block B - LAN Characterization.
Place an X in the boxes that best characterize your LAN.

B1. Frequency of backup for data and software on the server.

	Daily	Weekly	Monthly	None*	On installation or when modified	Other (Specify)
Software	☐	☐	☐	X	☐	
Data	☐	☐	☐	X	☐	

*If "None" is checked, include corrective action plan in Block E.

B2. Considering data sensitivity and processing criticality, the relative need to protect LAN availability, integrity, and confidentiality.

	Availability	Integrity	Confidentiality
Low	☐	☐	X
Moderate	X	☐	☐
High	☐	X	☐

B3. Using the scale and criteria below, place an X the box which best reflects the effectiveness of the LAN environment and existing safeguards in protecting LAN availability, integrity, and confidentiality.

Effectiveness of Protection Afforded LAN.

Criteria

Very Low - ☐ — Daily problems with LAN availability are encountered and/or very little, if any, assurance of maintaining data integrity and/or data confidentiality.

Low - X — Problems with LAN availability are not uncommon and/or limited assurance of maintaining data integrity and/or confidentiality.

Moderate - ☐ — LAN normally available to support operations and data integrity and/or confidentiality are well protected.

High - ☐ — LAN seldom unavailable and data integrity and confidentiality are well protected.

Very High - ☐ — LAN availability and data integrity and confidentiality are assured.

If not at least Moderate, the LAN is considered to be inadequately protected.

B4. This box indicates the highest rating checked in B2 above. This establishes the Security Level used to determine safeguard requirements in Block C.

Security Level

Low	Moderate	High
☐	☐	X
Level 1	Level 2	Level 3

NOTE: Item B4 will be completed automatically based on the response to Item B2.

ALBERT
Exhibit C-1.   LAN Risk Assessment Worksheet (continued).

Block C - Safeguard Requirements Matrix.

Place an X in the Yes or No column to indicate compliance status for mandatory safeguards. If a waiver has been approved for a requirement, enter WA in the Yes column. If a waiver has been requested (or included with this risk assessment), but not yet been approved, enter WR in the Yes column. The appropriate Security Level column is automatically filled in based on the security level indicated in B4, with an X indicating compliance is mandatory and an O indicating compliance is optional. If a safeguard is optional, a N/A is automatically placed in the yes column.

Safeguard	Security Level 3	Comply Yes	No
C1. A complete set of current system and application documentation is available to the LAN Administrator.	X	X	
C2. An employee security awareness and training program is in place.	X	X	
C3. Passwords (at least 6 characters) and log-on codes are used to protect LAN data from unauthorized use or disclosure and are changed at least every 6 months.	X	X	
C4. Software feature(s) is provided to automatically lock out a terminal if inactive for more than a reasonable time, for a specific time after normal closing, and if a password is not entered correctly after	X		X

Network Diagrams -
Roadmaps to the LANs, WANs, WLANs, WWANs, and PANs
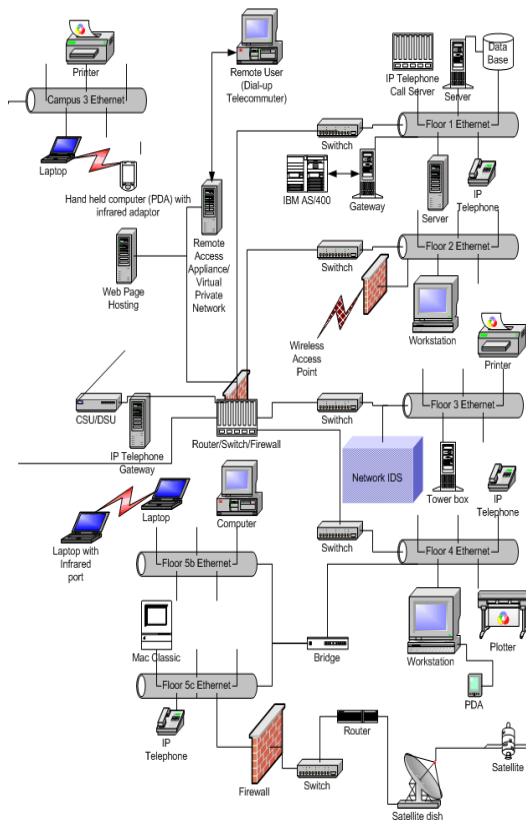
Vital document(s) for use in determining network access points to aid in the development of network security solutions.

7

Stage 2 - IT Policies and Procedures

IT Policies and Procedures Manual

Educational

Entity

IT Policies and Procedures

Manual

Updated 2001

Front line defense system to alert users to management's approved use of system resources including detailed instructions for maintaining proper security and confidentiality of data assets

End-User Agreements - Signed, Sealed, and Delivered

Internet

E-mail

Network

Signature (either actual, electronic, or class roster) reinforces end-users acknowledgement of management's directives, provides legal documentation of delivery, and should result in better security practices by system users.

Creating the Human Firewall

The completion of Stage 2 is providing constant user education in the safeguarding of data assets to prevent:

- Social Engineering

- Abuse of Access Rights

- Accidental Disclosure of Confidential Information

- Misuse of Network Assets

- Physical Security of Data Center Assets (From PDAs/Laptops to the Computer Rooms)

- Attacks on System Resources (E-mail attachments, Web initiated attacks via Java/Active X)

Stage 3 - Technology Barriers
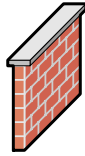
Firewalls 🧱 May I see your IP address please

Firewall

Firewalls should be used to secure untrusted access points including wireless access points, Internet, and any connection from an untrusted outside source.

Must be monitored and rule sets upgraded continuously.

Antivirus Software - Computer Defense Shield

- **Host Based: E-mail servers, firewalls, Internet servers, database servers, etc.**

- **Client Based: End-user workstations**

With new virus/worm warnings appearing on an almost daily basis, entity data centers must install and maintain antivirus software on appropriate servers (e-mail, firewall, database) and client machines to reduce the chance of network disruptions.

Disaster Recovery - Alternate Site Processing

Having an alternate site including a binding agreement, if necessary, is a corner stone of any disaster recovery program. Failure to secure a temporary processing location including a test run to validate its ability to process your critical systems can invalidate a disaster recovery program.

Florida had 59 reported hurricane and tropical storm events between January 1994 and December 2000 resulting in over 2 billion dollars in property damage.

Weather and other disasters such as a data center fire or sabotage/theft of equipment validate the need to secure and maintain adequate off site processing capabilities.

Computer Incident Response Team (CIRT)

Composed of entity management and staff responsible for responding to any attempted or actual unauthorized network access.

CIRT Duties Include but are not limited to:

✉Documenting the priority and sequence of actions to be taken when dealing with an intrusion.

✉Developing policy to indicate what types of intrusion response actions require management approval and which are pre-approved as well as other intrusion response policies.

✉Developing responses to handle intrusions, including configuring redundant equipment to preserve the compromised machine(s) for further study and for the preservation of evidence should there be legal proceedings.
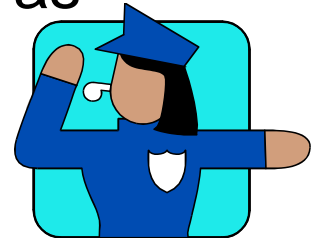
⊟Best Practices for Seizing Electronic Evidence - Presented by the Secret Service at:

www.treas.gov/usss/index.htm?electronic_evidence.htm&1

Security - A Multidimensional Approach

The Security World According to the SANS(sans.org)

(System Administration, Networking, and Security Institute)

1. Organization Wide Security Policies (including a strong effort to continuously educate users on security issues)

2. Strengthen Host Security (Apply Patches, Harden OS)

3. Constant Auditing of Systems

4. Router Security (IOS Patches, Configuration, Monitoring)

5. Proper use of Firewalls (Placement, Updates, Monitoring)

6. Installation of Intrusion Detection Systems (Host, Network)

7. Incident Response Plans (Policies, Action - CIRT)

New Security Trends

- HIPAA

- New Legal Issues

Getting HIPAA

◻ Applies to institutions that maintain and transmit an individuals medical information and extends to any third party providers used by an institution to provide these services.

◻ Specifies the coding of medical transactions and the method used to transmit this information.

◻ Establishes privacy, security and auditing guidelines for medical records.

Possible Security Provisions of HIPPA

■Administrative Procedures - Must maintain formally documented network/user security procedures including providing specific details to entity personnel on procedures to be used to maintain security of data covered under the Act.

■Physical Safeguards - Active protection of data hardware (lock the server/computer room door(s), escort vendor techs).

■Technical Security Services - Active logging and monitoring of network activity.

■Technical Security Mechanisms - Encryption of medical data transmitted within network or to third party, verifiable audit trails.

HIPAA Compliance Dates

✉ **Transaction Rule - October 2002**

✉ **Privacy Rule - April 2003**

✉ **Security Rule - 2 years and 60 days after being published in Federal Register**

New Legal Issues

If an entity fails to use due diligence in securing network resources, the entity faces the increases risk of legal action against it.

Security breaches including the use of an network to initiate or participate in denial of service attacks, spreading a virus or worm, or a yet to be conceived method of disabling another Web site could create liabilities for institutions.

22

Emerging Technologies

Intrusion Detection Systems (IDS) - a network burglar-alarm system

IDS is software designed to dynamically detect inappropriate, incorrect or anomalous activity on hosts and networks. Functions include monitoring and reporting user and system activity, auditing system configurations and vulnerabilities, checking file integrity, using statistical analysis and attack-pattern recognition, and auditing user activity for policy violations.
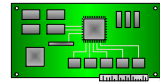
TYPES OF IDS

HOST IDS: Can be deployed on network servers including firewall, database, and Web servers. Creates snapshot of server under parameters set by administrator. Compares file activity to snapshot using rules sets to determine if activity on server meets acceptable use as set by entity.

Network IDS: Operates by monitoring network traffic through a network interface card placed in a particular segment of a network. When data traffic matches a rule set considered outside normal parameters, the IDS can create an alert to the network administrator and log the activity for further investigation.

Countering the Blended Threat

- CODE RED
- NIMDA

IDSs can become a tool used to supplement anti virus and firewall barriers. IDSs, with the proper rule sets, may be able to provide early warning to data center personnel if a blended threat breaches the perimeter security measures in place. Host IDS can be used to assess changes to a machines file structure to correct damage to system.

LIMITATIONS OF SELECT IDSs

⇩**Not able to operate properly in high bandwidth (gigabit) networks**

⇩**Currently unable to detect encrypted hacker code**

⇩**A new technology with a small number of rules compared to the number of rules found in an antivirus product**
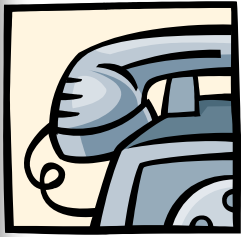
Internet Protocol Telephony

IP Telephony is the transportation of voice communications over a data network allowing many educational entities to take advantage of their network structures to provide voice services.
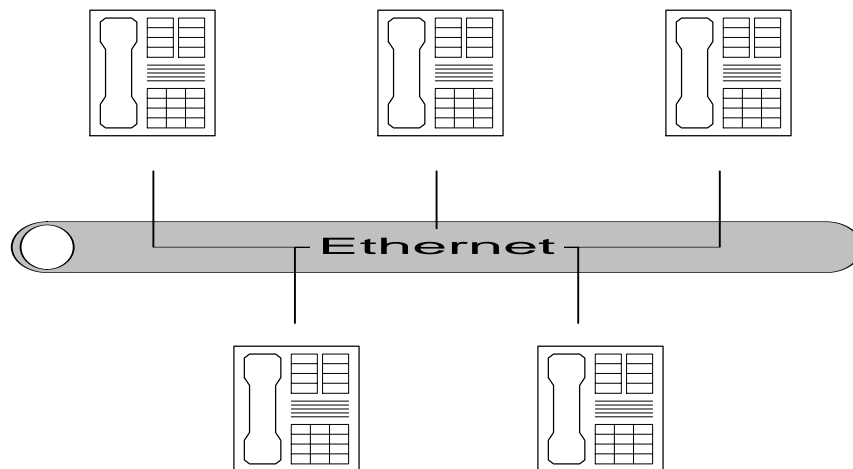
IP Telephone Security Issues

■**Authentication** - When a call is placed, has the reached the desired destination without being diverted to an unintended receiver?

■**Nonrepudiation** - When a call has been made, is the connection logged to substantiate the receipt of the call?

■**Accuracy** - Was the call secure from the sender to the receiver of the call without being intercepted and possibly altered before being completed to the intended receiver?

Defenses - Encryption of Voice Traffic and use of IP Telephone Capable Firewalls

Wireless Networks -
Air Connections

Wireless Wide Are Networks (WWANs), Wireless Local Area Networks (WLANs), and Personal Area Networks (PANs) provide network connectivity over a limited physical area with the use of radio waves, microwaves, or infrared light. Bluetooth and 802.11x represent two of the principal standards for the delivery of wireless services.
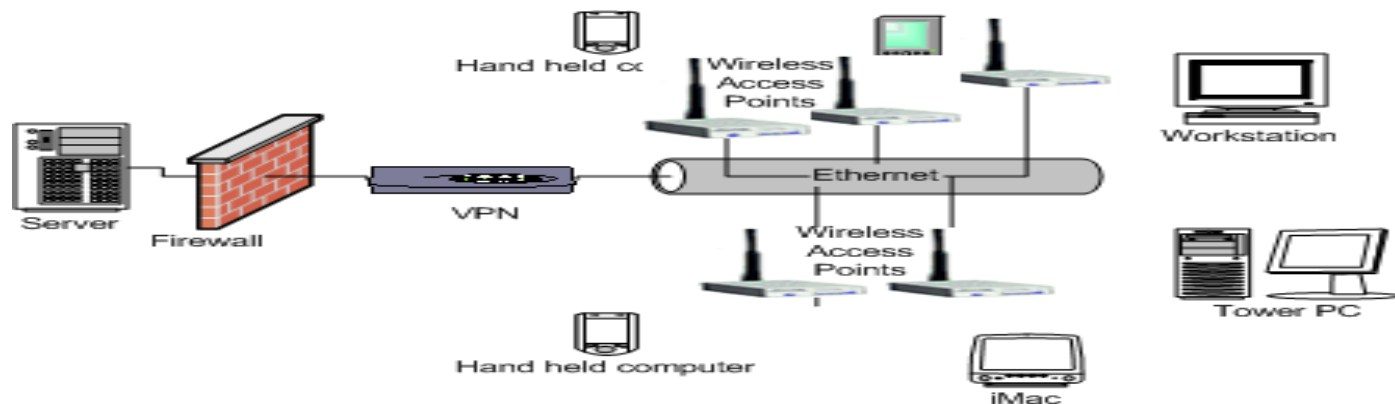
Wireless Security Threats

⊟ **Eavesdropping** - The ability to intercept and capture data transmissions over a wireless networks

⊟ **Transitive Trust** - The ability for a perpetrator to setup false wireless access points that are used to acquire user IDs and passwords when a authorized users device is diverted to the unauthorized access upon the users logon attempt.

⊟ **Denial of Service** - Due to nature of radio transmissions, wireless networks are very vulnerable to denial of service attacks. Attacks can be carried out by using a high-powered transceiver or incompatible wireless devices (Bluetooth on an 802.11x network or visa versa).

⊟ **Poor security in default installations** of wireless networks.

Steps to Protect Networks When Wireless Networks are Present

Enact security provisions to strengthen logon protocols from default installation settings

Use of a Virtual Private Network to encrypt data transmission between access points and client machines and firewalls on client machines.

Use firewalls between Local Area Segments using wireless access from production network segments

Enact Information and technology policies and procedures to regulate the installation of wireless networks (prevent renegade wireless access points)

Personal Digital Assistants (PDAs)
- Do You Know What Your Users are Doing with their PDAs on Your Network?

Palm Operating System, Pocket PC, and Blackberry dominate the handheld devices used.

The PDA Security Risks

There are four principal threats PDA's pose for entity networks.

■1. Users synchronize their PDAs through USB, Serial, and Infrared connections to their desktop or mobile computer. During this process, there is a potential threat to the entity network that the PDA may have a <u>virus or worm and download it to the users computer connected to the network</u>. If the desktop does not have antivirus software or it fails to detect the virus, the virus could infect the users machine and be transported to other machines on the network.

■2. Users could transfer confidential entity information to their handhelds such as e-mails, password list, etc.. Since the <u>devices are easy to lose or be stolen</u>, this posses a security risk to the entity.

The PDA Security Risks, continued

3. Unless a user obtains a third party application to encrypt data, all <u>data on handhelds is stored in an unencrypted format</u>.

4. The operating system security is not robust on most PDAs making them <u>highly susceptible to unauthorized access</u> to data stored on the devices. In particular, older Palm Operating Systems, 3.5 and earlier, allowed the use of developer kits to bypass user security settings to access data on such a device. Additionally, the current Pocket PC password system defaults to a four digit numerical password.

PDA Security Solutions

- Enact written **policies and procedures** to specify how PDAs may be used on your network.

- If confidential data is allowed on PDAs, buy third party software to **encrypt** this data.

- Ensure all workstations used to sync a PDA use an **antivirus** program that is effective against handheld delivered viruses, etc..

Application

Acquisitions

Purchasing Best Practices

■**Base Procurement on Best Value, Not Lowest Cost** - Compare vendors bids in combination with the proposed technology solution, experience, financial strength of vendor, and experience of vendor staff or consultants proposed for use on project.

■**Outline Business Problem Then Allow Vendor to Propose Solutions** - Present the business processes and have vendors develop a solution using their technology rather than proposing a technology solution the vendors must meet.

■**Develop Smaller Projects with Milestones** - If possible, develop smaller projects with definite milestones rather than a large multiyear project.

■**Prioritize Project Elements Up Front** - Project manager should have good understanding of entity priorities concerning the three major project components 1) the budget, 2) the schedule, and 3) the functionality of the system.

Purchasing Best Practices - Part 2

■ **Establish Measurable Objectives for the Project -** Projects should have measurable objectives (deliverables) to ensure project meets objectives of entity before payment made to vendor.

■ **Require the Use of Project Management Methodology** - Provides components (a strategic plan, use of cost accounting system, establishing a dispute resolution and change management process) used by the project manager to track the project and reduce the chance of operation failure and cost overruns.

■ **Require Letter of Credit from Vendors on Larger Projects** - If project fails, a letter of credit allows collection in a shorter time period than performance bond but may increase cost.

■ **Use a Quality Assurance Contractor** - Helps entity identify and assess problems that can occur in a project and propose solutions to correct these problems.

Purchasing Best Practices - Part 3

■**Pay Vendor Only Upon Acceptance of Tested Project Deliverables** - Payment should not be released until the entity verifies the completion of the deliverable.

■**Write Stronger Contracts to Protect the Entity** - Contract should be written the needs of the technology purchased including clear responsibilities between vendor and entity.

■**Enforce the Terms of the Contract** - Failure to enforce terms of contract during the project puts entity at risk of not receiving an end product that meets the contracted functionality desired.

So You Want to Install an ERP

✉Maintain adequate staff to backfill a project members legacy position and limit the amount of time critical staff of the ERP project spend in maintaining legacy system.

✉Do not underestimate the time and materials needed to train end-users to facilitate a smoother transition from the legacy to the ERP system.

✉Maintain management support of the project

The End