

# Office of Audit and Compliance

## IT Audit Themes at University Schools FY2001-FY2004

April 11, 2005

Susan Kennedy

Director, IT Audit



# Table of Contents

---

- Background and Scope
- Summary of Findings
- Effective Controls



# Scope

---

Assessments of IT Infrastructure, Security, and Administration between FY2001 and FY2004 were completed in 11 Schools:

- ⊗ Annenberg
- ⊗ Dental
- ⊗ Design
- ⊗ Grad Ed
- ⊗ Law
- ⊗ Nursing
- ⊗ SAS
- ⊗ SEAS
- ⊗ Social Work
- ⊗ Vet
- ⊗ Wharton

Note: SOM results are not included in this analysis.



# What is an IT and Network Assessment?

---

- The objective of an IT and Network Assessment is to conduct a general assessment of the security processes for the network and all attached computing equipment and to identify computer security best practices.



# Components of the IT and Network Assessment

---

- The IT and Network Assessment covers the following areas:
  - Understanding of current system architecture
  - Operations Management
  - Services and customer satisfaction assessment
  - Change management and systems development cycle
  - Network and system security
  - Software license assessment

Note: The IT and Network Assessment changes as technology and risk changes. Therefore, not all components were covered in each review.



# Summary of Findings

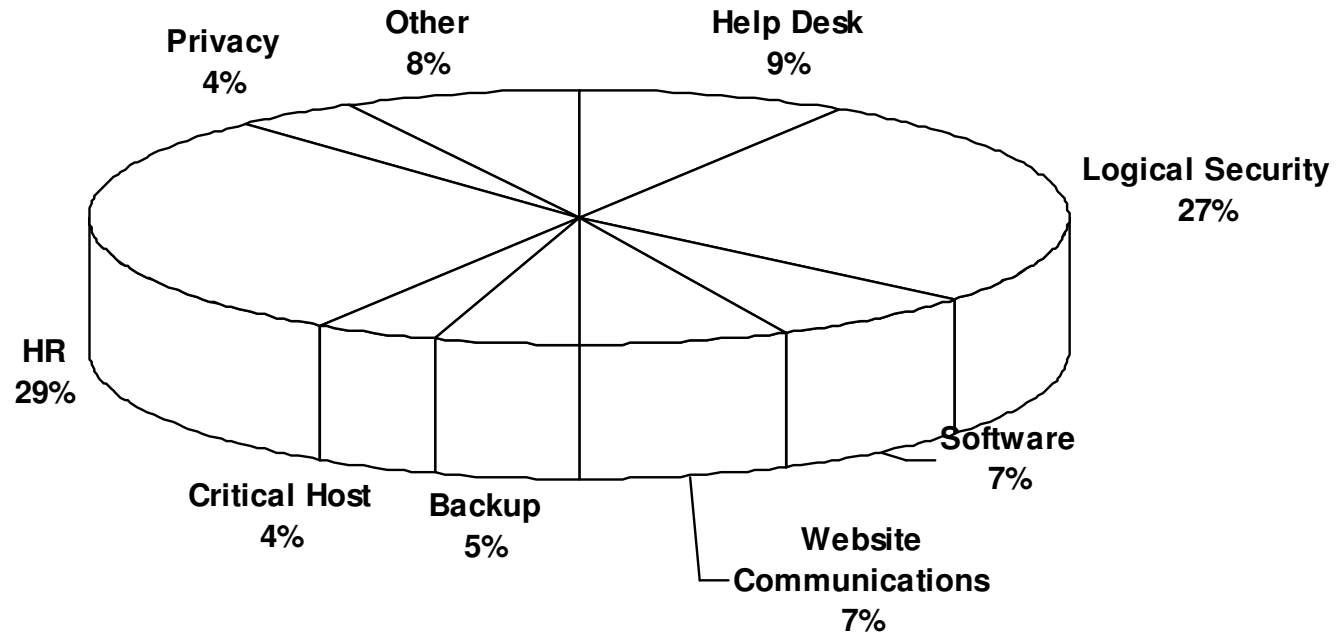
---

- **11 Schools and 250 Servers Scanned**
  - **Findings have been de-identified**
- **56 Effective Controls were identified throughout**
- **415 High, Medium, and Low risk observations were categorized**
- **Of these 415 observations,**
  - **321 were ISS vulnerabilities**
  - **94 were IT general Control vulnerabilities**
- **OAC distilled the effective controls and observations to understand their significance within the University, to identify common themes, and to offer recommendations so the University at large may strategically implement Best Practices and address common areas of risk where applicable.**
- **Overall, the purpose of this thematic analysis is to provide a management tool and resource that guides the development of strategic solutions to address universal risks and to enhance the University's collective ability to escalate common and recurring issues.**



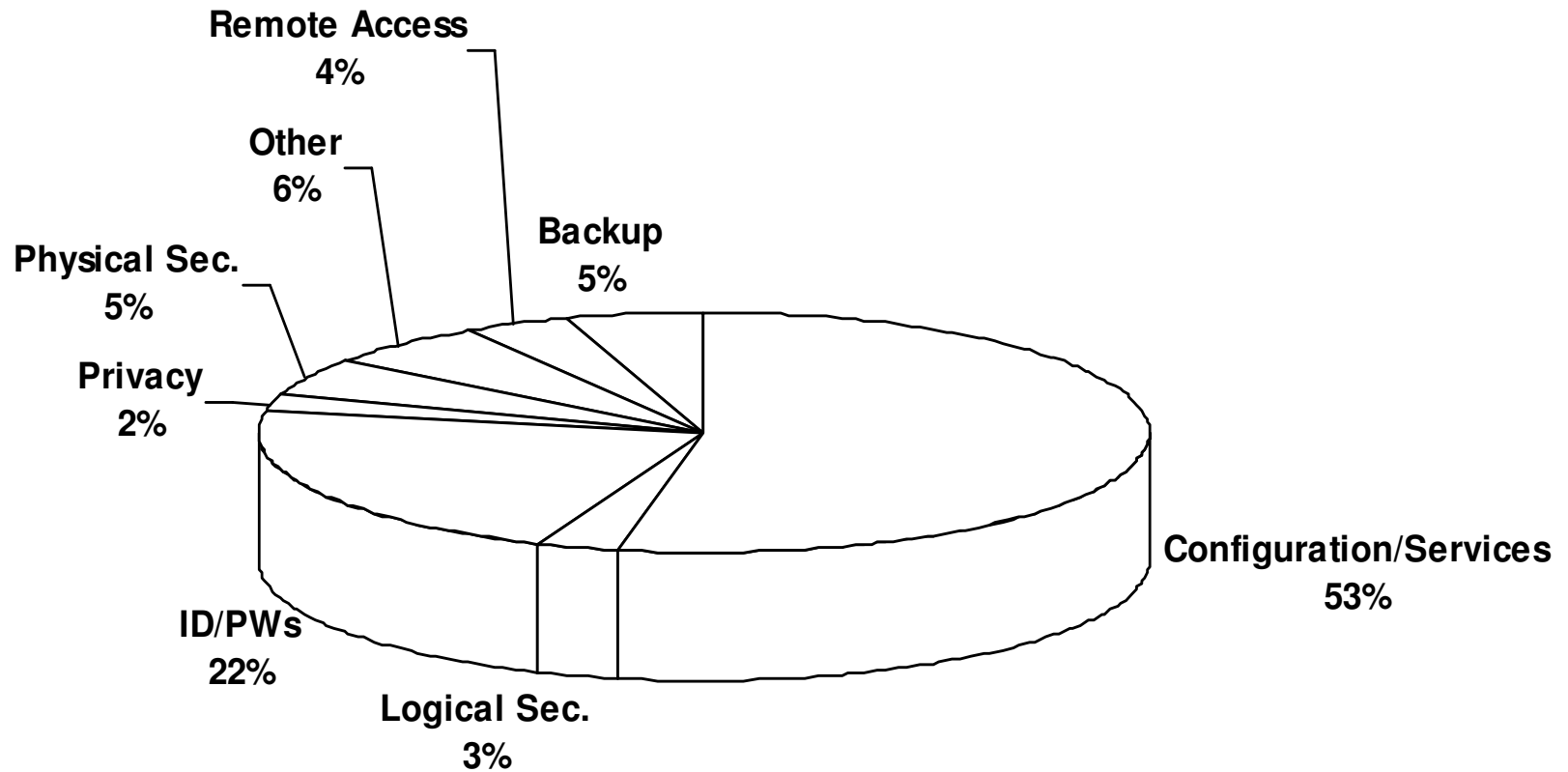
# Effective Controls Categories

---



# Opportunity For Improvement Categories

---



# Effective Controls Overview

---

Overall, strong results can be attributed to the University initiatives related to network, security, and privacy.

- Campus Computing Organizations and Advisory Groups
- Computing Policies, Guidelines, and Education – both School and Centrally based, such as:
  - Critical Host Registration
  - Acceptable Use
  - Authentication
  - Email and website usage/support
  - Anti-virus/SPAM
  - Confidentiality of Student Records
  - Networked services and devices
- Collaboration between technical support groups
- Resourceful and dedicated personnel



# Effective Controls Overview

---

The most common effective controls related to Logical Security and Personnel.

- HR category (29% of the best practices) - IT professionals typically have a keen awareness of information and systems security issues and recommended practices and display dedication and commitment to their mission.
- Logical Security Category (27% of the best practices) - implementing anti-virus and SPAM tools, firewalls, and authentication have been implemented to help secure domains.
- Additional strong practices include Help Desk services, Software License Tracking, Laptop Certification, and Website Communications.
- These Effective Controls were noted in a variety of schools and are promoted as goals for all IT programs.



# Specific Effective Controls observed in schools

---

- **Monitoring** of servers daily using tools and techniques to detect and prevent unauthorized intrusions.
- Providing a well structured and organized **help desk and desktop support** services.
- Creating organized and effective procedures to control **software licensing and compliance**.
- Requiring **strong password** protocol for **network** logins.
- Addressing **privacy** concerns and regulation, including HIPAA compliance, proactively.



# Specific Effective Controls cont'd

- Implementing software **firewalls** on critical host servers to deter unauthorized network access.
- Registering a large number of **critical host** servers with ISC.
- Employing strong **authentication** methods for mission critical applications.
- Deploying **anti-virus and SPAM** software to combat potential viruses and denial of service attacks.
- Instituting **laptop certification** to gain network access.
- Diligent data and system **back up and storage offsite**.



# Common Areas for Improvement Overview

---

The most common areas for improvement lie in Configuration/Services and IDs/Password Management.

- Configuration/Services Category (53% of the total observations) – Configurations, such as file-sharing utilities, patch management, operating system upgrades, and unrelated business services, need additional management.
  - Efforts are currently underway to address some of these topics:
    - IT Orientation
    - User Groups
    - ISC & School Led Efforts
    - New Guidance and Policy such as PennNet Computer Security Policy & related guidelines.
  - Utilize pre-existing tools (such as server security checklists).
- Logical Security Category (22% of the total observations) - procedures and practices associated with account management, ID and password management, user privileges, and intrusion detection require enhancement.
  - In progress - Terminated Employee Report from Data Warehouse
  - UPHS Terminated Employee Report is available.



# Common Areas for Improvement: Configuration/Services

---

## Administrative Accounts

- Default Passwords
- No Passwords
- Non-complex Passwords
- Guest Accounts

## Unnecessary Services Running

- Chargen
- Echo
- Mountd Daemon
- DOS
- LDAP
- SMTP
- SNMP
- RPC
- NetBIOS



# SANS/FBI Top 20 & the University

The SANS (SysAdmin, Audit, Network, Security) Institute and the Federal Bureau of Investigation (FBI) have created a Top 20 Vulnerabilities List for operating systems. Ten of these vulnerabilities identify the most commonly exploited exposures for Windows operating systems and the other ten apply to UNIX operating system.

Comparing our observations in these reviews with this list, in varying degrees of intensity throughout the schools reviewed, we found:

- 80% (8 of 10 vulnerabilities) of the Unix vulnerabilities and
- 50% (5 of 10 vulnerabilities) of the Windows vulnerabilities in 11 University Schools.

The University could achieve significant security improvements with limited resources if they focused their strategic efforts on addressing these specific vulnerabilities as a priority.



# SANS/FBI Top 20 & the University

According to published list prior to October 8, 2004

---

## Top 10 Vulnerabilities to Windows Systems

1. \* W1 Internet Information Services (IIS) (5 INSTANCES)
2. W2 Microsoft Data Access Components (MDAC) –  
Remote Data Services
3. W3 Microsoft SQL Server
4. W4 NETBIOS –  
Unprotected Windows Networking Shares
5. \* W5 Anonymous Logon – Null sessions
6. W6 LAN Manager Authentication –  
Weak LM Hashing
7. \* W7 General Windows Authentication –  
Accounts with no passwords or weak passwords
8. W8 Internet Explorer
9. \* W9 Remote Registry Access
10. \* W10 Windows Scripting Host

\* Identifies vulnerabilities found in 11 University IT Assessments: 5 out of the 10 top Vulnerabilities for Windows Systems were found during the course of these reviews.

## Top 10 Vulnerabilities to Unix Systems

1. \* U1 Remote Procedure Calls (RPC)
2. \* U2 Apache Web Server
3. \* U3 Secure Shell (SSH)
4. \* U4 Simple Network Management Protocol
5. \* U5 File Transfer Protocol (FTP)
6. U6 R-Services – Trust Relationships
7. U7 Line Printer Daemon (LPD)
8. \* U8 Sendmail
9. \* U9 BIND/DNS
10. \* U10 General Unix Authentication – Accounts  
with no passwords or weak passwords

\* identifies vulnerabilities found in 11 University IT Assessments: 8 out of the 10 top Vulnerabilities for Unix Systems were found during the course of these reviews.



# SANS/FBI Top 20 & the University

New Listing Published List on October 8, 2004 to focus on

---

## Top 10 Vulnerabilities to Windows Systems

1. W1 Web Servers & Services
2. W2 Workstation Service
3. W3 Windows Remote Access Services
4. W4 Microsoft SQL Server (MSSQL)
5. W5 Windows Authentication
6. W6 Web Browsers
7. W7 File-Sharing Applications
8. W8 LSAS Exposures
9. W9 Mail Client
10. W10 Instant Messaging

## Top 10 Vulnerabilities to UNIX Systems

1. U1 BIND Domain Name System
2. U2 Web Server
3. U3 Authentication
4. U4 Version Control Systems
5. U5 Mail Transport Service
6. U6 Simple Network Management Protocol (SNMP)
7. U7 Open Secure Sockets Layer (SSL)
8. U8 Misconfiguration of Enterprise Services NIS/NFS
9. U9 Databases
10. U10 Kernel



# Common Areas for Improvement:

---

## Security Patches

- Regular/Timely Process of applying security patches:
  - Patches are made available by the vendor to address security weaknesses in the operating system. Because patches must be applied by the system administrators manually, security vulnerabilities may exist unnecessarily for extended periods of time allowing additional time and opportunity for unauthorized parties to compromise sensitive University resources and data.
- Situation Observed:
  - Patches are not applied timely or regularly



# Common Areas for Improvement:

---

## Critical Hosts

- Unregistered Critical Hosts:
  - The Critical Host Policy directs that all critical systems installed on PennNet are to be maintained at appropriate levels of security, while at the same time not impeding the ability of users and support staff to perform their work. A critical host is a server that, if compromised, could significantly harm the University. Schools and Centers may optionally designate any hosts as critical if its compromise could significantly harm the local unit. Examples of significant harm could include legal liability, reputational damage, interruption of critical business functions, and disclosure of confidential information.
- Situation Observed:
  - Servers that store critical and confidential information not yet registered with the University's Information Systems Computing Group as established by the University's Critical Host Policy.



# Common Areas for Improvement:

---

## IDs and Passwords

- User IDs & Passwords:
  - User ID and Passwords are established to ensure system security and safeguard information against unauthorized use, disclosure, or modification, damage, or loss.
- Situation Observed :
  - Complexity of Passwords
  - Regular Changes
  - Network IDs and Passwords – move toward PennKey Authentication



# Common Areas for Improvement:

---

## Logical Access

- Removing Network and Application Privileges for Terminated/Transferred Employees:
  - User accounts are managed timely to review and confirm access rights periodically. Individuals who are no longer authorized may continue to maintain access privileges to sensitive and critical data and resources.
- Situation Observed:
  - Accounts are not reviewed periodically
  - Terminated employees' accounts continue to exist



# Common Areas for Improvement:

---

## Physical Security

- Environmental Controls & Physical Security:
  - Facilities are managed to provide a suitable physical surrounding which protects the IT equipment and people against man-made and natural hazards.
  - Points for consideration:
    - Access to facilities
    - Site Identification
    - Physical security
    - Personnel health and safety
    - Environmental threat protection
- Situation Observed:
  - Environmental control equipment is not implemented
  - Physical security is not implemented



# Common Areas for Improvement:

---

## System Backup

- System Backup:
  - Backup procedures ensure that system files, programs, and incremental backups are performed properly and on a regular basis to ensure that data remains complete, accurate, and valid during its storage. If successful backups are not performed, critical research and operational data could be lost in the event of a computer failure or physical site disaster.
- Situation Observed:
  - Backup Processes are not consistently documented
  - Backup Employee is not trained for key/critical systems
  - Backups are not regularly performed



# Common Areas for Improvement: System Backup Storage

---

- Offsite Storage of Backup Media:
  - Backup copies of system, programs and data files are rotated to a secure off-site storage location on a scheduled basis to make data available and to ensure a minimum business impact in the event of a major disruption. Failure to rotate the backup media to a secure off-site location increases the risk of not being able to recover systems and information.
- Situation Observed:
  - Backup tapes are stored in same location as server
  - Backup tapes are taken home with system administrators



# Common Areas for Improvement: Backup Media Restoration

---

- Restoration from Backup Media:
  - Restoration tests are performed to ensure backup and recovery procedures are effective. Although a manual or automatic backup may have been successfully completed, it is possible that the data was not successfully copied as intended to the backup media. Hardware or software data errors can prevent a successful backup and this situation may not be detected until recovery is attempted with the media in a true outage. Such errors are often discovered after a hacker has entered systems and destroyed or otherwise ruined data.
- Situation Observed:
  - Restorations are not performed from backup media regularly.



# Common Areas for Improvement: DRP & BCP

---

- Disaster Recovery Plans (DRP) & Business Continuity Plans (BCP):
  - Plans to govern the restoration and continuation of business functions and computer support in the event of a disaster or business interruption to ensure minimum business impact in the event of a major disruption. Without formal and tested plans, recovery of critical data and hardware may not be possible in a reasonable timeframe, if at all.
- Situation Observed:
  - DRPs have not been created, documented, and tested
  - DRPs have not been incorporated into the school's larger Business Continuity Plans



# Common Areas for Improvement:

---

## Privacy

- Privacy:
  - The use of sensitive data may be necessary, but creates potential liability for the institution if the data was compromised. In light of the growing identity theft crimes, wherein a person's SSN is often a key piece of information used to commit the theft, sensitive data collection and storage pose a risk to the School and the Institution as a whole.
- Situation Observed:
  - Sensitive data is sent in clear text
  - Sensitive data is collected unnecessarily
  - Sensitive data is stored insecurely

