2005-2006 :: Information Security

1. Mission Statement:

The mission of the UTD Information Security Office (ISO) is to provide proactive security analysis, develop robust security architecture and ingrain security awareness into the university's environment. ISO works in partnership with the various Information Resources departments, Internal Audit, Compliance and Information Technology representatives from each school to support teaching and learning activities for UTD students, faculty and staff in cooperation with the university's mission to become a global leader in innovative, high quality science, engineering, and business education and research.

2. Objectives:

2.1 Use McAfee EPO to audit anti-virus environment.: Deploy anti-virus software to UTD computers running Windows and collect deployment statistics Identify method of deployment for anti-virus software to UTD computers running non-Windows OS and collect deployment statistics

2.1.1 Related Strategic Plan Item(s): III-1 Dynamic Change Management; IV-1 National and Global Security

2.1.2 Related Institutional Priority Item(s): COM-3 Sustain Progress toward Tier One Status in terms of programs, research and faculty quality

2.1.3 Standards and Associations: EDUCAUSE UT System INFOSEC

2.2 Better investigate compromised computer systems.: Install a Forensics Computer System to improve the turnaround time it takes to evaluate and investigate compromised computer systems

2.2.1 Related Strategic Plan Item(s): III-1 Dynamic Change Management; IV-1 National and Global Security

2.2.2 Related Institutional Priority Item(s): COM-3 Sustain Progress toward Tier One Status in terms of programs, research and faculty quality

2.2.3 Standards and Associations: EDUCAUSE UT System INFOSEC

2.3 Replace outdated hardware: Replace outdated hardware to reduce or prevent equipment failure.

2.3.1 Related Strategic Plan Item(s): III-1 Dynamic Change Management; IV-1 National and Global Security

2.3.2 Related Institutional Priority Item(s): COM-3 Sustain Progress toward Tier One Status in terms of programs, research and faculty quality

2.3.3 Standards and Associations: EDUCAUSE UT System INFOSEC

3. Measures & Findings:

3.1 Deployment statistic report : Deployment statistic report

3.1.1 Success Criteria: 75% + coverage of managed Windows computers

3.1.2 Related Objective(s): Use McAfee EPO to audit anti-virus environment.

3.1.3 Results Related To Success Criteria: 89% managed Windows deployment reached end of Aug., 2006

3.1.4 Achievement Level: Met

3.1.5 Further Action: Yes

3.2 How to deploy anti-virus to non-Windows computers: Investigate methods to deploy anti-virus to non-Windows computers

3.2.1 Success Criteria: Create report on method to deploy anti-virus

3.2.2 Related Objective(s): Use McAfee EPO to audit anti-virus environment.

3.2.3 Results Related To Success Criteria:
Report on how to deploy AV to non-Windows computers will be completed in FY07 and IS will begin deployment when reach 75% deployment of anti-virus to managed Windows computers.

3.2.4 Achievement Level: Not Met

3.2.5 Further Action: Yes

3.3 Report on installation of forensic computer system: Report on installation of forensic computer system

3.3.1 Success Criteria: Forensic computer system installed.

3.3.2 Related Objective(s): Better investigate compromised computer systems.

3.3.3 Results Related To Success Criteria: System installed 04/06

3.3.4 Achievement Level: Met

3.3.5 Further Action: Yes

3.4 Monitor time to investigate computer incident: Monitor turnaround time it takes to investigate a computer incident

3.4.1 Success Criteria: More than 50 % faster turnaround on investigation

3.4.2 Related Objective(s): Better investigate compromised computer systems.

3.4.3 Results Related To Success Criteria: We have done one investigation since the installation and it was 100% faster than time taken to complete previous investigations

3.4.4 Achievement Level: Met

3.4.5 Further Action: Yes

3.5 Analyze equipment age reports: Analyze equipment age reports

3.5.1 Success Criteria: All outdated hardware replaced

3.5.2 Related Objective(s): Replace outdated hardware

3.5.3 Results Related To Success Criteria:
8 components at end of maintenance life August, 2005; all equipment replaced.

3.5.4 Achievement Level: Met

3.5.5 Further Action: Yes

3.6 Document and monitor equipment failures.: Document and monitor equipment failures.

3.6.1 Success Criteria: Decrease equipment failures by 50%

3.6.2 Related Objective(s): Replace outdated hardware

3.6.3 Results Related To Success Criteria: No equipment failures this year

3.6.4 Achievement Level: Met

3.6.5 Further Action: Yes

5. Closing the Loop:

5.1 Continue Windows deployment & begin Unix method: Continue with Windows deployment and begin identifying UNIX deployment strategy

5.1.1 Related Objective(s): Use McAfee EPO to audit anti-virus environment.

5.1.2 Related Measure(s): Deployment statistic report

5.1.3 Responsible Person: Information Security Officer responsible for anti-virus.

5.1.4 Target Date: Summer `07

5.1.5 Priority: Medium Priority

5.2 Deploy anti-virus to non-Windows computers: Define the timetable and schedule the deployment after determination is made of how to deploy the EPO agents.

5.2.1 Related Objective(s): Use McAfee EPO to audit anti-virus environment.

5.2.2 Related Measure(s): How to deploy anti-virus to non-Windows computers

5.2.3 Responsible Person: Information Security Officer responsible for anti-virus.

5.2.4 Target Date: Summer `07

5.2.5 Priority: Medium Priority

5.3 Analyze equipment age reports: Replace outdated equipment each year

5.3.1 Related Objective(s): Replace outdated hardware

5.3.2 Related Measure(s): Analyze equipment age reports

5.3.3 Responsible Person: Director, Information Security

5.3.4 Target Date: January `07

5.3.5 Priority: Low Priority

5.4 Document and monitor equipment failures: Continue replacing equipment with expiring maintenance on a yearly basis.

5.4.1 Related Objective(s): Replace outdated hardware

5.4.2 Related Measure(s): Document and monitor equipment failures.

5.4.3 Responsible Person: Director, Information Security

5.4.4 Target Date: January `07

5.4.5 Priority: Low Priority

5.5 Monitor effectiveness of forensic computer system: Monitor how the software and hardware are being used to investigate incidents. If adjustments are needed, document resources needed.

5.5.1 Related Objective(s): Better investigate compromised computer systems.

5.5.2 Related Measure(s):
Report on installation of forensic computer system; Monitor time to investigate computer incident

5.5.3 Responsible Person: Information Security Incident Response Team

5.5.4 Target Date: December, 2006

5.5.5 Priority: Low Priority

5.6 Monitor time to investigate computer incident:
Monitor how the software and hardware are being used to investigate incidents. If adjustments are needed, document resources needed.

5.6.1 Related Objective(s): Better investigate compromised computer systems.

5.6.2 Related Measure(s):
Report on installation of forensic computer system; Monitor time to investigate computer incident

5.6.3 Responsible Person: Information Security Incident Response Team

5.6.4 Target Date: December, 2006

5.6.5 Priority: Low Priority

6. Analysis:

6.1 Program/Unit Strengths:

6.1.1 Objectives/Outcomes Exceeded or Met: Items that relied solely on Information Security personnel were relatively easy to implement and target outcomes were achieved.

6.2 Program / Unit Weakneses:

6.2.1 Objectives / Outcomes Partially or Not Met: Items that required co-operation by decentralized departments to accomplish goals were difficult to meet. This emphasized the need for central authority for implementation of security rules and regulations over de-centralized areas and the need for executive management support of the initiatives.

7. Report:

7.1 Executive Summary:
FY 06 was a year centered around planning for an ERP system while continuing to enhance and maintain security at and within our network edge.

7.2 Top 3 Program/Unit Accomplishments: Information Security:
Works in partnership with the various departments of Information Resources, the support components in schools and departments, as well as internal audit and business continuity planning groups, to ensure the integrity, authenticity, confidentiality and availability of computer-based data resources; develops, maintains and reviews policies and procedures; performs risk assessment and compliance auditing; co-ordinate disaster recovery planning; develops campus security strategies including edge and internal security; performs network and vulnerability scanning and assessment; responsible for HIPAA security implementation; provides malicious code detection and prevention; conducts break-in investigations (including forensics); provide public security awareness programs; works to ensure awareness and compliance with local, state and federal laws.

7.3 Research Activities or Publications: Nothing to report.

7.4 Instructional/Training Activities (presented or received): RA/TA information security orientation is given each long semester.

7.5 Public Service:

TheInformation Security Director sponsors the North Texas Snort Users Group (open source intrusion detection system) which meets monthly at UTD. Paul Schmehl, Sr. Information Security Analyst is a founding member and continuing contributor to AVIEN(anti-virus identification/remediation group/information sharing).

7.6 Other External Activities: AVIEN is an international organization.

7.7 Contributions to UTD: 1. Expanded security audit of servers covered by Server Management Policy.

2. Expanded Tippingpoint IPS monitor to cover peer to peer and phishing scam exploits.

3. Commenced deployment of McAfee's E-Policy Orchestrator to enhance automation of anti-virus protection (Windows only).

4. Obtained approval for expanding the Information Security Acceptable Use Policy to include students.

5. Completed the purchase of an enterprise wide Imaging System.

6. Started development of security infrastructure for new ERP system. (System and Application).

7. Attended extensive training for the new ERP system.

8. Participated in planning and development of implementation strategies for the new ERP system.

9. Completed the purchase of the Tivoli Access Manager for Operating Systems for the IBM AIX systems supporting the ERP system.

10. Continued the Quarterly verification access audits by department, as well as expanded the scope.

11. Conducted RA/TA Orientation Sessions.

12. Mitigated renewal problems with dual digital certificates.

13. Expanded Verisign Digital Certificate program to include UNIX and MAC users.

14. Conducted successful Disaster Recovery Test of UNVAPPS (Windows server), as well as the mainframe.

15. Vetted security of purchased software for various departments.

16. Began the purchase of a state of the art commercial intrusion detection system. This purcahse will be completed in FY 07. This will give us additional insight into the condition of our network, as well as free up personnel for other tasks.

7.8 Top 3 Program / Unit Challenges:

Banner implementation required dedicated staff which Information Security department did not have.