2006-2007 :: 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 Replace the enterprise-level vulnerability assessment tool with an effective solution.: Identify options for vulnerability assessment tools (hardware/software), acquire evaluation systems and evaluate their value to UTD.

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 Replace open-source IDS with a robust commercial Intrusion Detection System (IDS).: Evaluate the industry leading IDS, Sourcefire (for which UT System has a contract), to determine how it performs in the UTD environment. Acquire Sourcefire if testing determines that it performs as needed.

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 Acquire training for Information Security Analysts and Administrators.: Train Information Security staff (both centralized and de-centralized) to facilitate the implementation of new UT System security initiatives.

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

2.4 Hire two additional Sr. Information Security Analysts and one backfill position.: Employ additional personnel to facilitate the implementation of new UT System security initiatives, PeopleSoft security and provide cross-training.

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

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

2.4.3 Standards and Associations: EDUCAUSE UT System INFOSEC

3. Measures & Findings:

3.1 Evaluate and acquire a suitable replacement product.: At least 3 on-site evaluations of different products before end of 2006.

3.1.1 Assessment Timeframe: annually

3.1.2 Success Criteria:
Evaluate Beyond Security, Rapid7 NeXpose, and ISS Proventia appliance. Select a suitable replacement product.

3.1.3 Related Objective(s): Replace the enterprise-level vulnerability assessment tool with an effective solution.

3.1.4 Results Related To Success Criteria:
Evaluated Beyond Security, Rapid7 NeXpose, ISS Proventia appliance. The first 2 products did not meet UTD requirements. The ISS Proventia appliance was purchased.

3.1.5 Numerical Results: 100%

3.1.6 Influencing Factors:
We were able to get the products in-house for hands on evaluation. Our experience with products that did not meet our needs provided us the knowledge necessary to evaluate these products to determine best fit in our environment.

3.1.7 Achievement Level: Met

3.1.8 Further Action: No

3.2 Scan a Class B network and produce relevant reports.: Produce usable reports of vulnerabilities for Info Security.

3.2.1 Assessment Timeframe: Monthly

3.2.2 Success Criteria: Network is scanned, reports are created and reviewed.

3.2.3 Related Objective(s): Replace the enterprise-level vulnerability assessment tool with an effective solution.

3.2.4 Results Related To Success Criteria:
Reports are used to analyze network activity and identify potential compromises.

3.2.5 Influencing Factors: The ISS Proventia appliance allowed for the successful scanning of the Class B network.

3.2.6 Achievement Level: Met

3.2.7 Further Action: No

3.3 Scan networks for de-centralized areas and create reports.: Produce usable reports of vulnerabilities for de-centralized departments.

3.3.1 Assessment Timeframe: Quarterly

3.3.2 Success Criteria: Network is scanned, reports are created and reviewed.

3.3.3 Related Objective(s): Replace the enterprise-level vulnerability assessment tool with an effective solution.

3.3.4 Results Related To Success Criteria:
Reports are used to analyze network activity and identify potential compromises.

3.3.5 Numerical Results: 100%

3.3.6 Influencing Factors: Availability of time and software, cooperation of departmental techs.

3.3.7 Achievement Level: Met

3.3.8 Further Action: No

3.4 Evaluate industry leading commercial IDS solutions: Select appropriate solution for UTD.

3.4.1 Assessment Timeframe: annually

3.4.2 Success Criteria: Sourcefire was tested and it met UTD needs.

3.4.3 Related Objective(s): Replace open-source IDS with a robust commercial Intrusion Detection System (IDS).

3.4.4 Results Related To Success Criteria:
Purchased the software in FY06 and hardware components in FY07. Sourcefire is installed and protecting UTD against network intrusions.

3.4.5 Influencing Factors: We were able to afford this product because of the UT System contract for Sourcefire.

3.4.6 Achievement Level: Met

3.4.7 Further Action: No

3.5 Installed and implemented commercial IDS system.: Installation and implementation finished and performance of system equals or exceeds that of the open-source system.

3.5.1 Assessment Timeframe: annually

3.5.2 Success Criteria:
The number of FTE's required to support Sourcefire is fewer than that needed for the open-source product.

3.5.3 Related Objective(s): Replace open-source IDS with a robust commercial Intrusion Detection System (IDS).

3.5.4 Results Related To Success Criteria:
The number of FTE's to manage Sourcefire is less than required for the open-source system.

3.5.5 Numerical Results: 100%

3.5.6 Influencing Factors: Priority task, availability of staff time.

3.5.7 Achievement Level: Met

3.5.8 Further Action: No

3.6 Monitor network for intrusion and provide reports to de-centralized administrators for investigation as needed.:
When attempted network intrusions are detected, reports are generated and provided to the appropriate de-centralized

administrators for further investigation and remediation if appropriate.

3.6.1 Assessment Timeframe: Quarterly

3.6.2 Success Criteria: Intrusions are identified and investigated in a timely fashion.

3.6.3 Related Objective(s): Replace open-source IDS with a robust commercial Intrusion Detection System (IDS).

3.6.4 Results Related To Success Criteria:
The de-centralized administrators now have information available to them that they did not have previously.

3.6.5 Numerical Results: 100%

3.6.6 Influencing Factors:
Additional staff training and tools, increased the quality of the information that they received.

3.6.7 Achievement Level: Met

3.6.8 Further Action: No

3.7 Register and attend training classes and conferences.: Attendance by Information Security staff at the following training classes and conferences: RNA Sourcefire, SANS InfoSec Boot Camp, SANS Web Security, PeopleSoft HEUG, Educause 2006, quarterly UTINFOSEC meetings.

3.7.1 Assessment Timeframe: annually

3.7.2 Success Criteria:
Classes and conferences attended provided knowledge gain on a variety of topics. 2 Information Security staff members attended each of the following : RNA Sourcefire, SANS InfoSec Boot Camp, SANS Web Security, Educause 2006, quarterly UTINFOSEC meetings.

3.7.3 Related Objective(s): Acquire training for Information Security Analysts and Administrators.

3.7.4 Results Related To Success Criteria:
Classes and conferences attended provided knowledge gain on a variety of topics.

3.7.5 Numerical Results: 100%

3.7.6 Influencing Factors:
The concerted effort of UT System & Department of Information Resouces for the State of TX to contract with vendors that provide training at reduced costs allowed us to send staff to needed training.

3.7.7 Achievement Level: Met

3.7.8 Further Action: No

3.8 Acquire Center for Information Security TechNet subscription to facilitate training of centralized and de-centralized staff.:
TechNet subscription provides best practices and benchmarks for installation of workstation, server and database software.

3.8.1 Assessment Timeframe: annually

3.8.2 Success Criteria:
Incorporate the information delivered in the TechNet subscription into university policies and procedures thereby facilitating the training of centralized and de-centralized staff.

3.8.3 Related Objective(s): Acquire training for Information Security Analysts and Administrators.

3.8.4 Results Related To Success Criteria: The information delivered in the TechNet subscription to university policies and procedures to enhance the implementation of best practices into our environment.

3.8.5 Numerical Results: 100%

3.8.6 Influencing Factors: Availability of time to implement.

3.8.7 Achievement Level: Met

3.8.8 Further Action: No

3.9 Acquire MicroSoft TechNet subscription to facilitate Information Security training.: MicroSoft TechNet subscription provides advanced copies of new MicroSoft products to allow us advanced training prior to their public release.

3.9.1 Assessment Timeframe: Quarterly

3.9.2 Success Criteria:
Three Information Security Analysts have reviewed the new MicroSoft Operating System to acquire training on the new security features to be able to determine potential problems in our environment.

3.9.3 Related Objective(s): Acquire training for Information Security Analysts and Administrators.

3.9.4 Results Related To Success Criteria:
The MicroSoft TechNet subscription provides additional information about MicroSoft products.

3.9.5 Numerical Results: 100%

3.9.6 Influencing Factors:
The acquisition of this product provided us the opportunity to preview VISTA and make the decision to delay the release of the product on campus because of it's inability to co-exist within the existing UTD infrastructure.

3.9.7 Achievement Level: Met

3.9.8 Further Action: No

3.10 Get positions approved, posted and filled.: Hire qualified employees for additional workload and cross-training.

3.10.1 Assessment Timeframe: November 2006

3.10.2 Success Criteria: Positions filled.

3.10.3 Related Objective(s): Hire two additional Sr. Information Security Analysts and one backfill position.

3.10.4 Results Related To Success Criteria: Positions filled. Cross-training in process.

3.10.5 Numerical Results: 100%

3.10.6 Influencing Factors: All positions were filled.

3.10.7 Achievement Level: Met

3.10.8 Further Action: No

3.11 Acquire office space and necessary equipment for new employees.: Have functional workspace for new employees.

3.11.1 Assessment Timeframe: November 2006

3.11.2 Success Criteria: Employees are able to work in functional space.

3.11.3 Related Objective(s): Hire two additional Sr. Information Security Analysts and one backfill position.

3.11.4 Results Related To Success Criteria:
Employees are able to work in the space provided, however, efficiency was compromised by having to share office space. Because of the nature of information security work an office mate would have to leave the room during certain confidential tasks. In addition, the environmental controls for the offices were unable to adapt to the increased equipment and personnel.

3.11.5 Numerical Results: 100%

3.11.6 Influencing Factors:
Sharing office space does not provide an efficient work environment for the type of work done in Information Security.

3.11.7 Achievement Level: Met

3.11.8 Further Action: No

3.12 Train newly hired employees.:
Provide training on the requirements of the new security initiatives and other job functions for cross-training purposes.

3.12.1 Assessment Timeframe: August 2007

3.12.2 Success Criteria:
All training on the requirements of the new security initiatives and other job functions for cross-training purposes finish in about 6 weeks after the employee start his/her job.

3.12.3 Related Objective(s): Hire two additional Sr. Information Security Analysts and one backfill position.

3.12.4 Results Related To Success Criteria:
New employees are contributing to the success of the new security initiatives by auditing key functionality and preparing security awareness training for departments.

3.12.5 Numerical Results: 100%

3.12.6 Influencing Factors: Time and priority devoted to task.

3.12.7 Achievement Level: Met

3.12.8 Further Action: No

5. Closing the Loop:

5.1 Scan the Class B network and report on any vulnerabilities found.: Scan the class B network and create reports for the cental and decentralized areas on vulnerabilities found.

5.1.1 Related Objective(s): Replace the enterprise-level vulnerability assessment tool with an effective solution.

5.1.2 Related Measure(s): Scan networks for de-centralized areas and create reports.

5.1.3 Responsible Person: Information Security Office Personnell

5.1.4 Target Date: Quarterly

5.1.5 Priority: Medium Priority

5.2 Continue to monitor network for intrusion and provide reports to de-centralized administrators for investigation as needed.:
When attempted network intrusions are detected, reports are generated and provided to the appropriate de-centralized administrators for further investigation and remediation if appropriate.

5.2.1 Related Objective(s): Replace open-source IDS with a robust commercial Intrusion Detection System (IDS).

5.2.2 Related Measure(s):
Monitor network for intrusion and provide reports to de-centralized administrators for investigation as needed.

5.2.3 Responsible Person: Information Security Office

5.2.4 Target Date: Ongoing activity

5.2.5 Priority: Medium Priority

5.3 Hire Sr. Information Security Analyst.:
Replace the Sr. Information Security Analyst that moved out of Information Security into Compliance by 9/1/2007.

5.3.1 Related Objective(s): Hire two additional Sr. Information Security Analysts and one backfill position.

5.3.2 Related Measure(s): Get positions approved, posted and filled.

5.3.3 Responsible Person: Director, Information Security

5.3.4 Target Date: 9/1/2007

5.3.5 Priority: High Priority

5.4 Acquire office space.:
Acquired office space and equipment for additional Sr. Information Security Officers hired by 9/1/2007.

5.4.1 Related Objective(s): Hire two additional Sr. Information Security Analysts and one backfill position.

5.4.2 Related Measure(s): Acquire office space and necessary equipment for new employees.

5.4.3 Responsible Person: Director, Information Security

5.4.4 Target Date: 9/1/2007

5.4.5 Priority: High 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.

6.1.2 Other Strengths:
Information Security leaders demonstrated their ability to draw the decentralized technical staff together into a cohesive group in the face of a University crisis.

6.2 Program / Unit Weakneses:

6.2.1 Objectives / Outcomes Partially or Not Met: Items that required co-operation by decentralized departments to accomplish non-emergency 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 07 was a year centered around planning for an enhanced UT System-wide Security Action Plan while continuing to enhance and maintain security at and within our network edge. There is no available method for

automated deployment of anti-virus software by McAfee to UTD computers running non-Windows OS's so that objective was closed. The overall workload continues to be a substantial challenge as the University rapidly evolves its information security posture.

7.2 Top 3 Program/Unit Accomplishments:

1.Managed the response and investigation of a University exposure of sensitive information.

2. Implemented a pilot project for encryption of confidential information on laptops, workstations and file servers to be rolled out to campus in response to UT System Security Bulletin #1.

3. Created an Information Security Coordinator group in response to the UT System-wide Action Plan to improve communication about information security initiatives to campus.

7.3 Research Activities or Publications: Nothing to report.

7.4 Instructional/Training Activities (presented or received): Leah Teutsch and Carl Ratliff passed examination for Certified Information Security Auditor (CISA).

RA/TA Information security orientation is given in each long semester.

7.5 Public Service:

The Information 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. Enhanced functionality of the Server Management Registry.

2. Expanded Tippingpoint IPS monitor to cover spam blocking.

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

4. Conducted RA/TA Orientation Sessions.

5. Mitigated renewal problems with dual digital certificates.

6. Implemented Sourcefire RNA, a state of the art commercial intrusion detection system, to replace the existing freeware system.

7. Managed the response and investigation of a University exposure of sensitive information.

8. Evaluated software to improve the ability to enforce security policy university-wide in order to reduce vulnerabilities due to inconsistent adherence to best practices.

9. Implemented a pilot project for encryption of confidential information on laptops, workstations and file servers to be rolled out to campus in response to UT System Security Bulletin #1.

10. Created an Information Security Coordinator group in response to the UT System-wide Action Plan to improve communication about information security initiatives to campus.

11. Implemented project to remediate storage and use of SSNs on campus computers and applications as required by UTS 165.

12. Assumed responsibility for the door access system to address audit findings.

13. Began PeopleSoft training for implementing security on the Student System, as well as began to address security issues inherent with moving into a remote, shared data center.

7.8 Top 3 Program / Unit Challenges:

Extremely high workload, staff are under constant stress and management evaluation of priorities.

New regulations to implement.

Extension of central control over departmental practices and assets.

7.9 Detailed Resources Needed to Improve and Fulfill Mission: Additional resources will be neeed in Information Security to handle PeopleSoft security based on UTA estimates of FTE requirements. Additional resources will be needed to address the additional responsibilities encompassed by the door access system and the implementation of a new system and an increase in the number of buildings to be covered.