Some Key Points Extracted from the IBM Report
"University of Tennessee Security Assessment Report – Version 2.2 – Final"
Dated: February 15, 2002

The following material has been quoted from the IBM Report. This report contains the following text in the footer of each page: "IBM and UT Knoxville Confidential". It is not known at this time whether President Fly has formally submitted a request to the State Attorney General to exempt this document from the Tennessee Open Records Law. Therefore, any requests from individuals who are not employees of The University of Tennessee for this document or the IBM Report should be forwarded to President Fly (efly@tennessee.edu).

(p. 2): "The impact of not responding to the most significant concerns of this security assessment exposes UT to some, of not all, of the following events: failed audits, loss of research funding, fines or more serious legal action for improper protection of sensitive or private data, information theft, fraud and disruption of systems."

(p. 2): "IBM strongly recommends that UT increase focus on security and privacy issues and implement tighter security policies by creating a position for an empowered security officer. Past security efforts at UT have been fragmented across departments, and roles and responsibilities have not been well defined nor effectively communicated. The University should appoint a Security Officer (much like the President of the United States named a Security Czar) to function as a dedicated security manager with full responsibility for all information security related activities across all departments of the University. UT must empower the Security Officer with a mandate by communicating to all departments that he/she defines and administers security issues with the full support of the President of the University."

(p. 13) "The *UT Knoxville Acceptable Use Practices* lists the rules and responsibilities for all users of UT IT resources, but is unclear who owns the document and whether or not users can be held accountable for the responsibilities outlined in the document."

(p. 14) "The general perception is that security policy and controls are not required because most information is subject to the Tennessee Open Records Act. During the interviews the IBM team attempted to educate people on the need to protect the information from unauthorized update or destruction. However, this perceived lack of a requirement to protect data seems to be part of the culture and requires policy and awareness at all levels of the University to address fully."

(p. 14) "The IT Security organization has a security plan detailing tasks that, if implemented, would improve the security of the University. The IBM team was not provided a security strategy document to support the tasks in the plan."

(p. 14) "There is a draft Incident Response Procedure developed by the IT Security organization but it has not been approved."

(p. 17) "Several people have knowledge of an IT Security organization but do not view it as having UT system-wide authority. Most people viewed the current IT Security organization as having a security focus for the network only, and not responsible for drafting security policy. The current IT Security manager is located organizationally in the OIT Infrastructure department which could contribute to the reason the security organization is viewed as having network security focus."

(p. 17) "Some managers in the University are strongly opposed to the system vulnerability scanning performed by the IT Security organization. They don't view the organization, as having authority to scan their department owned servers and some expressed a dislike to the actual people responsible for the scanning."

(p. 17) “There is cooperation between the computer investigators in the UT Police department and the IT Security organization. UT Police investigators indicated they have worked with the IT Security organization on several incidents.”

(p. 17) “The UT Police investigators have a good relationship with the Knoxville FBI Cyber-Terrorism agents. These are good relationships to establish and maintain.”

(p. 17) “The IT Security organization is planning to establish departmental security officers and possibly use the First Responders for this role. This would establish a point of contact in each department for information security.”

(p. 18) “There were no guidelines for security requirements that must be contained in third party contracts in any of the policies or standards reviewed.”

(p. 18) “There is no regular independent review of information security on the critical information systems.”

(p. 19) “The University must determine who within the organization has authority to authorize and conduct scanning of devices on the network. The result should be included in the Information Security Policy and must be communicated to the organization. There is a potential risk that scanning devices on a network could impact the availability of the system, therefore the actual scanning should be coordinated with the business owner and included in the University’s change management process.”

(p. 20) “Arrangements involving third party access to UT information systems should be based on a formal contract containing, or referring to, all the security requirements to ensure compliance with the University’s security policies and standards.”

(p. 20) “The cooperation and collaboration of OIT, business managers, and faculty is essential to implementing security at UT.”

(p. 26) “The computer and server rooms located in Stokely Management Center managed by OIT do not have a fire protection system. However, IBM understands there is a proposal to install a fire protection system.”

(p. 29) “System manuals and supporting documentation are non-existent for UT servers and databases. This was found to be the case in most all departments across the University.”

(p. 29) “Change control procedures are not well documented, and vary across the different departments of the University. Most all of the interviewees expressed concern with the lack of a change control process. Several areas cited the migration to DHCP as an example of a change that could have benefited from a documented change control process.”

(p. 29) “There is little to no concern about segregation of duties within OIT and the various departments that were interviewed (for example between application developers and persons with access to production data regarding students).”

(p. 29) “System auditing is either not being performed or only performed at a minimal basis, and audit log reviews are performed on a reactionary basis. Most interviewees understood the need to have system auditing enabled on the servers and stated that they planned to do so in the future.”

(p. 29-30) “Network scanners are used to test server security in a proactive manner by the OIT Security Organization. Some departments and managers expressed concern that they were not notified of the scans until after the fact. The scans were perceived to have caused system disruptions for hours during prime production periods. Very strong reactions were expressed to IBM multiple times during the interviews.”

(p. 30) “Sensitive data such as student records and financial aid information is sent across the network in clear text format without encryption. Some users mistakenly believed compression was a form of encryption. This allows for the possibility that the data could be intercepted and read by unauthorized users. If this data were to be compromised and posted on an internal or external web site, the University could face legal action or at the least, a loss of confidence from students and faculty.”

(p. 30) “The UT network is an open design that allows unauthorized users to gain access via computer labs or public accessible library computers. There is no distinction between a trusted or untrusted zone of control. Systems that house critical or personal data are on the same segments as the servers intended for publicly accessible data.”

(p. 30) “The First Responder Program was found to be viewed very favorably by the departments interviewed who were aware of the program. Unfortunately, some departments pointed out that through attrition or lack of communication, the program had lost its effectiveness. These interviewees supported this program being revived; stating that benefit to the University could be gained if it was extended.”

(p. 30) “The University does not have a Windows domain structure implemented for the campus network. During the interviews, several areas cited problems with server names that are not unique. A campus domain structure would ensure unique server names.”

(p. 30) “The research areas interviewed identified a need for a VPN solution between research labs, but indicated that none had been provided by OIT. Some research grants require the University to protect the sensitivity of the information. Penalties can include paying back the research grant and suspension of all Federal grants.”

(p. 31) “The router configurations are not backed up and there is no document recovery procedure for the routers. The IBM team understands there are plans to update the scripts that create backups. In the event of a router hardware failure, the University could potentially lose critical router information or spend hours reconfiguring a router.”

(p. 31) “Network-based intrusion detection systems should be utilized to detect denial of service attempts and network hacks, both from external and internal sources. The network-based systems would complement the host-based intrusion detection systems such as Tripwire and Snort, which are already being used on some servers within the University.”

(p. 31) “Sensitive data such as student records and financial aid information should be encrypted when transferred from one system to another. There should be trusted zones of control and all data that passes through un-trusted zones should be encrypted. This would prevent sensitive data from being read by unauthorized users.”

(p. 31) “Network change control procedures should be documented. These should be treated as formal documents and closely monitored by OIT.”

(p. 32) “The OIT network group should provide point-to-pint VPN solution for research areas at the University.”

(p. 33) “Controls are not implemented to protect the University network from external or internal attacks and misuse. There is a concern from interviewees that there should be a firewall to protect the University network from the Internet, or at least to protect critical systems such as IRIS from unauthorized users and attacks.”

(p. 33) “The network security controls for IRIS appear to be inadequate to protect user access from on campus and off campus locations. It is IBM’s understanding that the SAP client is providing no encryption of the authentication process or the transfer of data between the SAP client and the SAP server. Users are accessing IRIS from remote and home locations on PCs with no personal firewalls. A personal firewall would protect the PC as well as prevent hackers or viruses from gaining access to the IRIS system.

Otherwise, a hacker could electronically install a tool like BackOriffice onto a remote user's PC without the user's knowledge, and when the valid user accesses the University network or IRIS, the hacker would then gain access to the University's system as well through the valid user's connection."

(p. 33) "The OS/390 and VMS systems are running TCP/IP services with no firewall. With these TCP/IP services enabled, an unauthorized user could gain access to these systems and alter or destroy valid data."

(p. 33-34) "There are inconsistent processes and no documentation for the requests and granting of system access by the IT staff, developers and vendors. Most accounts are created via email request or a phone call with little or no verification that the requester is who they say they are. System access is based on a request not a need, there is no process for de-registering accounts and users do not have to sign a letter stating they understand rules or policies."

(p. 34) "There are no known security management procedures requiring systems to have auditing turned on or the periodic review of audit logs."

(p. 34) "The University does not have guidelines for securing Microsoft NT or the numerous types of UNIX that are used as the operating systems for email, databases, applications and web servers. This has led to inconsistent security levels on these server platforms, making them susceptible to compromise."

(p. 34) "Some interviewees brought up concerns with the security of the current use of wireless technology. They felt that an unauthorized user could easily use the wireless network as an access point into the University network. There has not been an internal or external security review to identify the security vulnerabilities of the wireless network."

(p. 34) "Telnet and FTP are currently being used to access servers and network devices. The use of these plain-text services could result in the capturing of user ids and passwords by sniffers or various other tools used by unauthorized users and attackers to compromise the system or disrupt services."

(p. 35) "The Knoxville campus has revenue of $80 to $90 million annually in research grants and awards. Some of the research performed at the University is highly sensitive. Penalties for disclosing the information can include paying back the grant and suspension of all Federal grants."

(p. 35) "A combination of the above reported system access weaknesses pose a significant risk of unauthorized access to and / or unauthorized use of various systems and data residing within the UT wide area network. An example of a serious unauthorized compromise would be if an attacker gained access to the university routers or web servers and used them for Denial of Service attacks. If these attacks were successful in the outage of, for example the web services of a financial institution during normal business hours, the university could be held responsible for the lost revenue of that institution and its clients."

(p. 35) "At a minimum, the University should identify the business critical systems and the information that is required by law to be protected, and then apply the necessary controls to protect those systems and information. Protection of the networks should be provided by firewalls, which are more effective than the current filter lists used on the University's routers."

(p. 35) "UT should develop and implement a security hardening procedure for the Microsoft NT operating system as well as for the various types of UNIX in use. A process to regularly test and apply all approved security patches to the operating system is also required to protect the applications on these servers from on-going security vulnerabilities."

(p. 35) "The University should perform an application security assessment of the IRIS application that includes attempts to penetrate the application and the operating systems deployed for the IRIS application. The application security assessment should include a review of the application architecture and the processes to implement and maintain the application."

(p. 36) “In order to test the access controls currently in place, there should be a penetration test or ethical hack performed against the critical systems such as IRIS or the Student Information System.”

(p. 36) “A secure method of remote access should be implemented for accessing the University network. The use of VPN tunneling or some other form of encrypted communications should be explored and utilized. This would reduce the risk of unauthorized users gaining access to the network from the Internet.”

(p. 37) “The University should perform a security assessment on the current wireless network that includes attempts to penetrate the network. Wireless is a fairly new and evolving technology and should be monitored for unauthorized use.”

(p. 37) “Secure shell (SSH) and secure copy (SCP) should be used instead of Telnet and FTP. SSH and SCP are much more secure due to their encryption capabilities and would greatly reduce the risk of administrative user ids and passwords being captured by unauthorized users.”

(p. 37) “Network-based intrusion detection systems or some type of network monitoring systems should be implemented to detect unauthorized or malicious activity in the University dormitories.”

(p. 37) “The OIT and Security organizations should work with the research areas of the University to ensure adequate IT and security services are provided to protect sensitive research information.”

(p. 38) “Members of the faculty indicated that they were not consulting [sic] for user requirements for the IRIS/SAP implementation. This oversight has resulted in the accounting system not meeting the needs of the faculty. It was reported that a user could circumvent the workflow process and write checks without proper approval. Billing was also reported as a major problem.”

(p. 40) “There is no formal disaster recovery or business continuity plan, disaster recovery site or validation testing for the client / server systems or applications. This is especially of great concern with the IRIS system. During interviews, it was stated that work on a disaster recovery plan would begin after the start of the New Year. All client / server systems should have a valid disaster recover plan, especially the IRIS system.”