Security of Information Technology Resources at UT[1]

J. Douglas Birdwell
Research Council

February 25, 2002

Within the past week, ORIT received an assessment of UT security practices related to information technology, prepared by IBM under contract to UT. Both the report's contents, and initial ORIT actions in response to this report, cause me great concern. Current UT practices appear to be placing the research mission of the university at risk, and recent actions indicate that UT may be headed in the wrong direction. The following quote from the IBM report highlights the level of risk:

> (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."

and

> (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."

The problem is not just caused by poor funding, but also appears to be the result of poor leadership and a lack of education on security requirements and risks across the University community. Quoting from the IBM report:

> (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."

A committee is meeting this afternoon to discuss the finding within the IBM report; however, actions that appear to have already been taken lead me to believe that ORIT's intent is to "dodge the bullet" and cover up their deficiencies by placing blame on a very few individuals and reorganizing. For example, I have learned that Rod Meryweather, the campus' head of the ORIT security group, believes he is to be given an unsatisfactory review and demoted, and that blame for the shortcomings found by IBM is to be placed upon him. This is highly unfortunate, since Rod Meryweather is the person most responsible for the improvements in University IT security and security awareness over the past year.

[1] **The quoted material is from the IBM Report titled "University of Tennessee Security Assessment Report Version 2.2 – Final," dated February 15, 2002. 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).**

A trend appears to be repeating itself that occurred with the previous security officer, Sandy Goldstone, who was hired into a position that reported at a high level in the administration. When Sandy chose to leave the University, the position was re-classified within the network infrastructure group, effectively demoting the security officer's function and limiting his power to positively influence IT security from his first day on the job. An example of this is the evolution – or lack thereof – of policies related to IT security. Although Rod Meryweather has drafted several statements that could form the basis for security policies, to my knowledge none have been approved by the head of ORIT, Dwayne McCay. The University's Acceptable Use Practices document, which was authored by Sandy Goldstone in cooperation with the Research Council, has never been promoted to or spawned a similar policy statement.

The University's lack of commitment to adequate security of information technology resources has been evident to me for a long time. I have been reminded of the problems over the past several months as I have watched the deployment of SAP/IRIS. On January 25, 2002 I met with Sylvia Davis and Neal Wormsley. In this meeting, it was strongly implied that SAP/IRIS posed no security risks and had never been compromised. In my follow-up e-mail, which is in a separate handout, I documented Rod Meryweather's August 13, 2001 and September 21, 2001 postings to the UT INFOSEC campus mailing list that five SAP systems had been identified as being infected by the Code Red II worm, and that one system had been infected by the Nimda worm. The only certain method of recovering a system infected with Code Red II is to reformat the disk drives and reinstall everything, recovering data from backups made before the date of infection. My understanding is this has never been done. The IBM report is very explicit about the status of the IRIS system:

> (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."

And:

> (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."

Among IBM's recommendations that affect IRIS are:

> (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) "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."

Concerning network monitoring and pro-active security management, IBM states:

> (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. 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. 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."

Following these incidents, it is my understanding that, rather than implement a pro-active procedure to identify SAP systems that have been compromised and implement procedures to ensure that these systems maintained up-to-date security patches, Rod Meryweather was instructed not to perform worm detection scans of these systems in the future. Therefore, today, it appears possible that our University does not know whether its financial accounting system is infected by a worm or not.

Rod Meryweather has also been instrumental in procuring and configuring firewalls to establish protected enclaves within the University's network to form a barrier between the Internet and sensitive resources. Yet, the management within ORIT is attempting to place the blame for the current state of affairs, which is more likely to be a consequence of indifferent or hostile attitudes toward IT security and inadequate personnel and financial resources, on Rod Meryweather.

Rod Meryweather's case does not appear to be the only case involving ORIT personnel that may have been demoted or asked to leave in order to shift blame, or, at least, to make certain that people who are not "team players" and do not unquestioningly accept ORIT policies are marginalized or removed from their positions. The person who was primarily responsible for the implementation of DHCP services on campus has told me she has only a limited time remaining at the University. This, in spite of the fact that the University already has a severe shortage of people skilled in DHCP services, and continues to experience problems with DHCP services to the campus.

IBM recommends that a Security Officer, or "Czar", be appointed:

> (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."

It is interesting to note that this is essentially what the University had in Sandy Goldstone's position, which was intentionally weakened before Rod Meryweather joined the University.

There is a lot more material in the IBM report, which runs for 56 pages. A small amount of the material is inaccurate or inappropriate for an academic institution, but much of the information that the report contains reveals and corroborates what several faculty members have known or suspected for a long time. At present, there appears to be an effort within ORIT to suppress the findings of the report.

When we made a formal request to Dewitt Latimer for a copy of the report, he replied by e-mail, stating: "The final draft is being reviewed by the steering committee on Monday and will be approved and turned over to Dr. McCay and President Fly shortly thereafter. I'm sure Dr. McCay, after consulting with his peers, will decide on an appropriate and expedited schedule for it's [sic] release into the University community."

The report's title page states "University of Tennessee Security Assessment Report Version 2.2 – Final", and is dated February 15, 2002. On page 10, the report provides an assessment schedule, citing a "draft review by UT" from 2/04/02 through 2/08/02, with "final report delivery" in the date range 2/11/02 through 2/15/02, and, the last item, "final presentation" as "TBD (after 2/15/02)". My assessment is that today's meeting may have much more to do with damage control than with review of a "draft".

Based upon the information in the report and from other sources, I believe the Research Council has an obligation to discuss the potential impact of our vulnerabilities on our research community and determine whether the Research Council should make formal recommendations to the Faculty Senate and UT administration regarding remedies.

If we decide to discuss recommendations, I believe the following remedies should be placed on the table for discussion.

1. A fundamental problem appears to be the relative sizes and the potentially conflicting goals of the Research and the Information Technology missions of the Office of Research and Information Technologies. Should we recommend that ORIT be split into two organizations that focus entirely upon each mission?

2. I believe information security, or, more generally, information assurance, responsibilities should be centered much higher within our organizational structure. I suspect that we are seeing, in part, the consequences of conflicts between the current information security office and other entities within and external to ORIT. Should we recommend that the position of Information Security Officer be (re-)established, and to whom should that person report?

3. The buck always stops at the top. In this case, it appears that Dwayne McCay has not effectively managed and protected the information technology assets of the University. Should we recommend that a formal, and independent, investigation be convened, with the possible outcome of replacement of Dr. McCay? Given the appearance of a mindset within ORIT to protect itself (or its management) at the expense of University vulnerabilities, should other investigations be conducted?

4. It appears that one of the University's largest single vulnerabilities is within the Budget & Finance organization and involves the protection of IRIS and possibly other databases. A problem with the existing organizational structure is the equal status of Budget & Finance and

ORIT. How is it possible to enforce compliance with IT security requirements and requests to monitor or tests these systems?

It is not the Research Council's mission to tell the University administration how it should be organized. However, we have an obvious stake in any expectation that the University administration provide adequate security of information resources. At present, it is clear that security is not adequate, and that the consequences could severely hamper faculty members' efforts to attract and perform research within the University. This can in turn have a severe impact upon hiring and retention of quality faculty. Therefore, I believe the Research Council must provide input, through the Faculty Senate, that documents its expectations.