TTU IT Organization Changes

Promotion
Last fall, Mr. Darrell Bateman was promoted to the position of Assistant Vice President for Information Technology. He joins Dr. Katherine Austin, Assistant Vice President for IT, in assisting the CIO with the overseeing of the IT departments. Mr. Bateman, formerly the Managing Director of Technology Assessment, has 27 years of experience in Information Technology at Texas Tech University. Mr. Bateman was an integral part in the deployment of the first administrative network backbone at TTU (Token Ring). He has experience in mainframe computing, system support, technology assessment, and system programming. He has seen dramatic changes in technology over the years – punch cards to secure online transactions! In addition to his assessment role, he will oversee the operations of the Telecommunications Department and the High Performance Computing Center. Please join us in congratulating Mr. Bateman on his promotion!

Reorganization
Over the last few years, there has been a significant increase in TTU IT Division efforts to assist university departments with programming applications, PCI compliance (bank card transactions), and authentication in order to reduce the number of online vulnerable applications. In the last year, we have assisted with the repair of over 80 departmentally-managed online applications. We have created an organizational structure that more readily supports those growing customer needs. The new department (formally part of Technology Support), Application Development and Support, will design, program, and manage selected applications for TTU. This department will continue to assist TTU areas and units with protecting data using appropriate security mechanisms and will also assist in reviewing contracted vendor IT solutions for security compliance. Mr. Mike Simmons, Associate Managing Director, will lead the new department that will report to Dr. Katherine Austin, Assistant Vice President.

Microsoft Vista Availability

Over the last year, we have received numerous requests for the Microsoft Vista operating system. We have worked with Microsoft and have resolved the compatibility issues with software provided by the TTU IT Division under its site license agreements. After extensive testing and negotiation, the TTU IT Division released Microsoft Vista to the TTU community on Monday, January 21, 2008 for those faculty, staff, and students comfortable using the new operating system. Please note that we have released the software based on TTU community requests, but the TTU IT Division does not recommend migration at this time.

Two versions of Microsoft Vista are available:
- For faculty/staff campus users, Microsoft Vista Enterprise may be downloaded from the eRaider site to campus machines (http://eraider.ttu.edu). Please note, installing Vista Enterprise on a non-campus, personal machine violates the terms of the Microsoft Campus Agreement. The resulting failed activation attempts will cause the system to default to Reduced Functionality Mode (RFM).
- For students and faculty/staff work-at-home users, Microsoft Vista Ultimate may be purchased for $10 in the ATLC (west basement of the University library).

Microsoft Vista uses considerably more system resources than previous operating systems, so please make sure your system meets the minimum system requirements before upgrading. Faculty/staff campus users are strongly encouraged to consult with their local IT support providers before upgrading their computers (or ordering new computers) with Microsoft Vista. We also highly recommend that individuals considering this upgrade review our FAQs beforehand at http://www.depts.ttu.edu/helpcentral/vista.

This information is provided for those that are interested in upgrading to the Microsoft Vista operating system. There is no requirement for anyone to upgrade at this time. Windows XP Professional will continue to be supported by Microsoft and the IT Division of TTU.

Microsoft media purchases are available to TTU students, faculty, and staff according to the terms of the Microsoft Campus Agreement. As with all site licensed software, you must sign a license agreement and present identification at the time of purchase. Please note that purchases must be made with cash or check only—at this time we are unable to accept credit card payment.

If you have any questions regarding Vista, please visit the Vista Web site at http://www.depts.ttu.edu/helpcentral/vista. For other questions or for further information regarding Microsoft software sales, please contact IT Help Central at (806) 742-HELP (4357).
Managing Your Own Server: Important Things to Consider

Security breaches and “hacker” activity continues to escalate in the Internet world. As individuals become more aware, hackers shift their techniques and hone in on new vulnerabilities. Recently, hackers have begun to aggressively target servers, which translate into a burden on server administrators. After reviewing the activity that the TTU IT Security team thwarts on a weekly basis, we want to provide you some information that server administrators must be aware of:

- Server administrators must be extremely familiar and in compliance with the Server Hardening policy located at [http://www.infotech.ttu.edu/security/docs/server_hardening.php](http://www.infotech.ttu.edu/security/docs/server_hardening.php) (requires eRaider authentication);
- Server should be maintained by a trained professional;
- Server should be configured for optimum security;
- Server should be in an environment that minimizes downtime;
- Security settings should be routinely tested and monitored; and
- All servers should be registered with the Vulnerability Management System to receive weekly vulnerability scans (security@ttu.edu); critical and urgent issues should be resolved within seven (7) business days.

While it is possible for today’s server software to be installed and operated on default, out-of-the-box settings, such operations may leave avenues of penetration open to hackers. Server administrators should:

- Disable or uninstall unnecessary services during the installation and configuration;
- Use strong passwords for local machine administrator and service accounts;
- Disable local machine guest accounts (Default in Windows 2003 and Redhat Linux);
- All Windows servers are required to be a member of the TTU domain;
- All servers (Windows, Linux, Macintosh, etc.) need to be included in the Server Vulnerability program by contacting the IT Division security team at security@ttu.edu;
- Customer access to web-based applications should require eRaider authentication; and
- Physical security of the server should be observed at all times. Only the server administrator or authorized personnel should have physical access to the server.

Those areas and units that manage their own server bear the institutional liability should a breach occur. As such, we suggest that you consider the server and units may want to consider leveraging these resources to reduce the security risk that you assume by hosting your own server. Note that TOSM has a myriad of services to include hosting the physical server, but allowing the area or unit to provide you some information that server administrators must be aware of:

- Immediately report the incident as outlined below:
  - For virus & worm infections, compromised systems, or improper use complaints contact the IT Security Team at security@ttu.edu or 742-0840.
  - To report an incident that may be a criminal act (data theft, fraud, etc.), the exposure of confidential information, or a threat to personal or homeland security, directly contact 1) the Information Security Officer, J Stalcup, at 742-8000 x7000 or J.Stalcup@ttu.edu, or 2) TTU Chief Information Officer, Sam Segran, at 742-5151.
- Perform appropriate remedial action in accordance with the ISO’s instructions and IT guidelines.

Serious incidents will require some investigation to assess the severity and whether further forensics are required. Please contact the security staff above before altering the computing system or attempting to “fix the problem.” Typically virus and worm infections can be cleaned up without further investigation and IT Help Central, 742-HELP (4357) or itherpcentral@ttu.edu, can provide assistance.

**Spring Semester Event Highlights**

The TTU IT Division has another busy semester full of educational opportunities for the TTU community. We invite you to attend the following events:

- **Dell Roadmap**
  - Dell will be reviewing their product roadmap and highlighting topics of interest to the TTU Community
  - March 11th
- **Microsoft Technical Briefing**

**Reporting an IT Security Incident**

While we all know that we should protect our workstations, laptops, servers, and applications by using safe computing practices, some of us may not be aware that should a security issue arise we should report it promptly to the appropriate security staff. Texas Tech University has procedures in place for reporting computer security incidents as outlined in the Incident Management Security Policy. To view the policy, visit [http://www.infotech.ttu.edu/security/docs/incident_management.php](http://www.infotech.ttu.edu/security/docs/incident_management.php).

There are a wide variety of data security incidents that must be reported which include, but are not limited to: virus, worm, and Trojan horse infections; unauthorized use of computer accounts and systems; complaints of improper use of Information Resources; data theft and fraud; and computer system compromises. Should you become aware of a data security issue, there are two fundamental things that should be done:

1. Immediately report the incident as outlined below:
   - For virus & worm infections, compromised systems, or improper use complaints contact the IT Security Team at security@ttu.edu or 742-0840.
   - To report an incident that may be a criminal act (data theft, fraud, etc.), the exposure of confidential information, or a threat to personal or homeland security, directly contact 1) the Information Security Officer, J Stalcup, at 742-8000 x7000 or J.Stalcup@ttu.edu, or 2) TTU Chief Information Officer, Sam Segran, at 742-5151.

2. Perform appropriate remedial action in accordance with the ISO's instructions and IT guidelines.

**Contributions by:** Katherine Austin, Ph.D., Darrell Bateman, Bryan Carson, Shannon Cepica, John Geesling, Darvin Jordan, Alvin Mills, Rick Ramon, J Stalcup, John Vandygriff, and Allen Young.

**Safe Computing Practices Committee:** Sam Segran, Katherine Austin, Ph.D., Darrell Bateman, Eric Burrell, J.D., Tony Castle, Shannon Cepica, Scott Hall, Alvin Mills, J Stalcup, Allen Young, and assistance from IT Division leadership and staff.

**IT Web Site:** [http://www.infotech.ttu.edu](http://www.infotech.ttu.edu)

**Texas Tech University Web Site:** [http://www.ttu.edu](http://www.ttu.edu)

**Computer-Based Training (CBT):** [http://cbt.ttu.edu](http://cbt.ttu.edu)

**Laws and Texas Tech Policies:** [http://www.its.ttu.edu/documentation/laws](http://www.its.ttu.edu/documentation/laws)