Data Exposure Incident Highlights Need to Implement IT Strategic Plan Recommendations

Since this is the first TechTalk for the academic year, let me greet all new members of our community and welcome all returning faculty, students and staff. Miami is a great place to live, learn and work and there are exciting things happening in information technology across our university. Allow me to share a few clear successes that have occurred over the summer and at the beginning of fall semester:

- We have had the most successful fall move-in ever, facilitating our students’ smooth transition to residential living by supporting their technology needs efficiently and effectively.
- The spread of computer viruses and worms through the residence halls has been virtually eliminated.
- The new wireless network, myMiami portal and Blackboard course management system performed admirably as the pressure of the fall term start-up was applied.
- The PhD level research computing support staff members have been hired and are becoming engaged with our faculty.
- Continued classroom upgrades and enhanced support are receiving very strong positive review by new faculty who are arriving.
- Bringing up technology services in the new apartments in a two week window was a valiant and successful undertaking.
- Changes have begun related to IT cost management that will result in dollars saved in our units across the campuses.

Despite these positive outcomes, Miami has had an unfortunate data exposure incident discovered recently. An electronic report routinely provided by the registrar’s office through the online reporting environment was accidentally placed in a folder on a server operated by the school of business that was accessible from the World Wide Web. Because of this accident, personally identifiable information about Miami students enrolled in fall semester of 2002 may have been viewable by people outside the university for a period of time. The university deeply regrets that this accident occurred and has been aggressively attempting to demonstrate this concern over the past two weeks. There are several related facts that are important for everyone to understand:

- This was not a compromise of the university’s enterprise systems, security firewalls or user password system, all of which are performing as required.
- The subject web pages were not accessible through a published or discoverable web site name, and only became visible recently when the Google search engine discovered this site and added it to its index.
- We are not aware of any actual malfeasance or criminal activity that has occurred in this incident.
- The university has responded quickly to correct the situation, notifying those involved and going beyond the norm in terms of care and consideration for those adversely affected.
Data Exposure Incident Highlights Need to Implement IT Strategic Plan Recommendations

This incident occurred because of several contributing factors. I would like to share a strategic perspective of the incident, as compared to the operational facts you have heard up until now. We already have identified several improvement areas in our IT Strategic Plan (http://www.muohio.edu/itplan) adopted in 2004. We also have committed resources to initiatives to address these areas. Four of these targeted initiatives relate to this particular incident.

1. Our IT Strategic Plan clearly recognized the need for a strong decision support system to not only provide information easily, but at the same time, control unnecessary or unapproved distribution of this information. We are in the process of implementing this replacement environment.

2. Our IT Strategic Plan recognized the need for strengthening the reliability and availability of Blackboard as our strategic solution for the problem of faculty-student information exchange over the Internet. We have upgraded this system and now are encouraging our deans and faculty to complete the migration from older solutions to this preferred environment.

3. Our IT Strategic Plan recognized the need for the establishment of an Information Security Office, promulgation of policy, auditing of compliance and forensic investigation of violations. As of this spring, we have staffed to do most of these activities and now are expecting involvement and buy-in from units across the institution. Last February, our Information Security Officer proposed an aggressive security and privacy awareness program, and this will be a key component of our remediation of this incident.

4. In our IT Strategic Plan we clearly stated the need for more consistent, uniformly managed solutions that are less ad hoc and unpredictable. This incident has helped crystallize the need for this even more in many people's minds.

As a summarizing statement on this incident, I should point out that there are positive outcomes from such an unfortunate experience. As of this week, many on our campuses are now realizing the urgent need to move ahead more diligently on implementation of already stated objectives. So, in many ways, this situation may allow us to cooperatively accelerate removal of risk and otherwise enhance operations in ways that we already had recognized as possible.

I wish each of you a most productive year. As this year unfolds, please feel free to contact me with suggestions on how to make information and instructional technology more effective for our community.

J. Reid Christenberry
Vice President for Information Technology
306 Hoyt Hall
Miami University
Oxford, OH 45056
E-mail: vp-it@muohio.edu
Miami Notifying Students, Alumni of Privacy Breach

Miami University is notifying all students who attended Miami during the fall 2002 semester that a report containing their names, Social Security numbers and grades had been inadvertently placed in a file accessible through the Internet. (See full press release available at http://newsinfo.muohio.edu/news_archive.cfm)

Miami has established a Web page, www.muohio.edu/privacyhelp, with additional information. A toll-free number staffed by trained investigators experienced in dealing with privacy issues has also been put in place. Any students or alumni who may have been affected are encouraged to call 1-800-588-9839 from 8 a.m.-5 p.m. Central Time, Monday-Friday. Individuals who want to contact the university about the situation can use a special email address, privacyhelp@muohio.edu, or call Miami at (513) 529-0438.

Update Your Desktop E-mail Application to Use SSL!

As of Spring 2005, Miami’s incoming e-mail server began supporting SSL connections. SSL (Secure Sockets Layer) is a protocol that creates a secure connection between two computers and encrypts the data exchanged between the computers. With SSL in place, information that is transmitted cannot be read, even if it is intercepted. SSL was put in place on Miami's incoming e-mail server so that the MUnet password would be encrypted when transmitted between the server and desktop e-mail applications (like Eudora, Outlook, Outlook Express, Mac OS X Mail, etc.)

In order to use SSL, you must adjust the settings in your desktop e-mail application. IT Services strongly recommends you take this step now. Detailed instructions on configuring Eudora and Outlook to use SSL can be found in the Knowledge Base - just search for “SSL”.

On February 1, 2006, Miami’s incoming e-mail server will begin denying connections from desktop e-mail applications that have not been configured to use SSL. Please adjust your desktop e-mail settings now to ensure that your ability to check e-mail is not disrupted.

Note: No action is required if you only check e-mail via myMiami, as myMiami uses a secure connection to transmit the MUnet password.
Alert! New Policy to Delete “Sent” E-mail Older than 30 Days

Due to a huge increase in the number of e-mail messages stored in myMiami “Sent” folders, a new deletion policy will go into effect on October 10, 2005. Email stored in the “Sent” e-mail folder that is more than thirty days old will be deleted. This will allow the university to recover over 660 gigabytes of e-mail storage space.

Most students, faculty and staff are not aware of the fact that when an e-mail message is composed in myMiami a copy is retained indefinitely in a “Sent” e-mail folder. Most of this “Sent” e-mail is not needed or wanted, but it is retained as long as the person is affiliated with Miami. The storage space consumed by this “Sent” e-mail is enormous.

The new deletion policy applies only to messages stored in an e-mail folder labeled “Sent” on Miami’s e-mail server. This primarily means messages sent from myMiami, but anyone who has a desktop e-mail application configured to use IMAP and has created a folder named "Sent" on Miami’s central e-mail server (po.muohio.edu) will be impacted.

Please note: If you are using a desktop e-mail application (like Eudora, Outlook, Mac OS X Mail, etc.), IT Services still recommends that you use myMiami to check and see if you have messages in the mail folder titled “Sent”. In most cases, you will not. Most desktop e-mail applications use a slightly different folder name (such as “Out”, “Sent Items”, “Sent Messages” etc.) when storing sent e-mail on the e-mail server. Those folders will not be affected, nor will any e-mail that is stored on a desktop. Looking at your folders in your desktop e-mail application may be misleading because some applications, like Mac OS X Mail, display the folder name as “Sent” when it is really stored as “Sent Messages” on the server.

IT Services encourages ALL e-mail users to go to myMiami and review their “Sent” e-mail folder before October 10 to determine what messages will be impacted by this policy. Any important messages in the “Sent” folder should be moved to another folder before October 10. Instructions on creating a “SavedSent” folder and moving messages to this folder in myMiami e-mail can be found in case #2445, Saving sent e-mail for more than 30 days, Miami Knowledge Base.

Please contact the IT Services Support Desk at 513-523-7900 or supportdesk@muohio.edu if you have any questions or concerns.

Checking your Sent e-mail folder in myMiami

1. Open a web browser and go to http://mymiami.muohio.edu.
2. In the Login area, enter your Miami UniqueID and MUnet password and click “Login”.
3. Under Tools in the top left corner, click “e-mail”.
4. Under Folders, click “Sent”.

Please note: the number next to Sent is misleading, it reflects the “unread” messages in the folder, not the total number of messages in the folder.

5. Move any messages you wish to retain to another folder, as outlined in the Miami Knowledge Base case #2445.
Making myMiami Yours

Over this past summer, IT Services enhanced both the myMiami portal and Blackboard. Changes were made in May and again in August that merged myMiami and Blackboard into one easy-to-use application with new functionality and many new, client customizable features.

To help you become familiar with the new myMiami portal, each Tech Talk edition will spotlight a new feature or functionality. This issue features the new Miami Web Page Index, formerly known as Quick Links.

Miami Web Page Index (Quick Links)

The Miami Web Page Index (Quick Links) module appears on the “Login”, “My Tab” and “News and Events” pages. It offers several different ways of accessing Miami web pages.

Using the Miami Web Page Index

To find a particular Miami web page, simply click the appropriate letter from the Web Page Index list and scroll to locate the link. For example, if you want to find out information about the Recreational Sports Center, click “R” and scroll down until you find “Recreational Sports Center”. Click this link to open the Recreational Sports Center web site.
Making myMiami Yours (continued)

Customizing My Favorite Links

Removing a Link: e-mail

To remove a link, click the red next to the link. A confirmation box will display on the screen. Click “OK” and the link will be removed.

Adding a Link from the Miami Web Page Index: Recreational Sports Center

To add a link, you first must find it in the Web Page Index list. Once you locate it, click the green + next to the link. This will automatically display the My Favorite Links list with the new link added.

Adding a Link Not Found in the Miami Web Page Index:

To add a link that is not in the Miami Web Page Index, click Add a personal Favorite Link at the bottom of the module. A new form will display.

- For the Link name, type the name as you wish it to appear in My Favorite Links.
- For the URL, type the complete web address.
- For the Description, if desired, add a brief note that will display when you roll your cursor over the link.

When you have completed the form, click the “Add” button. The new link will now display in your My Favorite Links list. There will be a blue pencil icon next to the link that you can use if you wish to edit the link.

Add a personal Favorite Link
New Credit Card Payment Feature Available on Miami’s Pay Online service
By Karen McIntyre, Assistant to Bursar, Office of the Bursar

As of July, 2005, Miami University began accepting MasterCard, Discover, and American Express payments for tuition and fees through our secured web-based payment service. This service is provided through CASHNet, an Alameda, California, company that has provided Miami University’s cashiering system since 1999.

CASHNet will assess those paying via credit card a convenience fee of 2.9% for payments of up to $3000, and 2.3% for additional amounts in excess $3000. This convenience fee is required so that Miami will not have to pay merchant fees, which we expect would approach $1,000,000 annually, to provide credit card service to all students. Payments may also be made electronically by check, for which there is no additional convenience fee assessed.

Since early July, the Bursar’s office has received over $1.6 million in web credit card payments for 627 students, and over $7 million in electronic check payments for 1,747 students.

Paying Online . . .

Miami’s Pay Online service allows students, others authorized by students, or “guests” to make payments on a student’s Bursar account as well as deposit additional money into Diplomat, Attache, Passport Snack, and/or MUlaa accounts in any of the following ways:

1. Students can logon to BannerWeb, view their Student Account Summary, and click “Make a Payment”. For detailed instructions, visit the Miami Knowledge Base case #101900, Using BannerWeb for paying your Miami Bursar account or adding value to your MUlaa account.

2. Students may assign friends or family members an ID and password which will allow them to make a payment without giving them the ability to view non-financial personal student information. For detailed instructions, visit the Miami Knowledge Base case #102139, Authorizing others to make online payments to my Bursar account.

3. Others (“guests”) may make payments on behalf of students by accessing the payment link on the righthand side of Miami University Bursar’s Office home page at www.muohio.edu/Bursar. This will not reveal any personal information (including the student’s balance) to the payer.

Our department/division/office/organization wants to accept credit card payments over the web too!

The Bursar's office is embarking on a project that will allow other departments at Miami University to use CASHNet to process credit card and electronic payments via their web sites. If they don’t currently have a web site, the CASHNet Emarkets software helps create one using a shopping cart approach.

The CASHNet product provides a secure means to process electronic payments, meeting the rigorous payment card industry (PCI) standards.

More information about this project will be forthcoming in future editions of TechTalk.
MU Wireless Available Everywhere (Almost) on Miami’s Campuses!

As of Fall 2005, Miami’s students, faculty, and staff have access to Miami’s wireless data network, known as MU Wireless, in every building on all four of Miami’s campuses. Wireless coverage is also available in popular outdoor areas on the Oxford, Hamilton and Middletown campuses. Outdoor coverage maps can be found on the MU Wireless web site at www.muohio.edu/wireless.

Since MU Wireless went into full-scale “production” in early August, network monitoring equipment has shown that the wireless network gets a tremendous amount of steady use. For instance, on a recent Saturday morning at 7:00 am (not a peak network activity time!), the wireless network had several hundred active connections.

As with any new service, widespread use is revealing some areas for service improvements. IT Services is actively working to fine-tune the network based on client feedback. For instance, client reports helped IT Services identify that there was insufficient coverage in two residence halls (Elliot and Ogden). Additional wireless access points are being added to enhance the service in those buildings. A brief listing of known service issues and their resolution status can be viewed on the MU Wireless web site.

If you experience a problem with your wireless connection, please contact the IT Services Support Desk via phone at (513) 529-7900 while the problem is occurring.

A few hints about MU Wireless

- **Wireless is radio waves - so lots of things can interfere**
  A wireless connection problem can be caused by something as simple as a person standing in front of your computer in just the wrong spot. If you find your signal is weak or your connection drops, sometimes just turning your computer to face a different direction can fix the problem.

Microwaves, 2.4 GHz cordless phones, and unauthorized personal wireless access points can all interfere with your MU Wireless connection. If you are aware of any of these sources of interference, try to distance your computer from the source.

- **Moving between locations on campus with your laptop? You may need to reinitiate a wireless connection.** Please keep in mind that if you close your laptop while connected to wireless and move to another building, your laptop may not automatically reconnect to wireless when you re-open it in a new location.

- **Use VPN to secure your wireless traffic and get a full range of network services.** MU Wireless Lite lets you browse the web and use instant messenger; if you want to check e-mail using a desktop e-mail client (like Outlook or Outlook Express) or use other network services, add VPN. Check the Miami Knowledge Base for more information - just search for "MU Wireless Lite" or "VPN".
Between May and August 2005, Classroom Services upgraded the electronic presentation equipment in 38 classrooms to the Standard Technology level. The 38 classrooms were selected by the Classroom Enhancement Council and include 27 classrooms on the Oxford campus, 8 on the Middletown campus, and 3 on the Hamilton campus.

This summer’s upgrades bring the total number of standard technology classrooms on the Oxford campus to 90, the Hamilton campus to 12, and the Middletown campus to 21. A Standard Technology classroom includes a ceiling mounted data projector, resident computer, guest computer port with audio, DVD/VHS player, wall mounted speakers, a touch screen control panel, phone, and, in some select rooms, a document camera.

Instructors—Important Classroom Technology Support Updates

- To request classroom technology support, please call 9-7900 and press 9. Your call will be automatically directed to Classroom Services.
- Classroom Services is now open until 7:30 pm on Monday through Thursday to provide support to classrooms being used past 5:00 pm.

FY06 Operational Plan and Portfolio Rebalancing

IT Services recently finalized the FY06 Operational Plan. This plan was developed through the first IT Services’ project planning cycle that included a university-wide nomination process.

The process began with a solicitation to the Offices of the President, Vice Presidents and Deans requesting they identify and nominate academic and administrative business needs as potential information technology projects. This yielded a total of 148 requests.

After collecting the requests, IT Services’ personnel performed a fast-track process guided by client priorities to create project deliverables for each request and to estimate the IT resources required to produce the deliverables. Similar requests were combined into single projects, and those being worked on or already completed were removed.

As a result, 92 client nominations were converted into IT Services’ projects and placed on the FY06 Operational Planning Calendar. The Planning Calendar was approved by the IT Executive Council on August 17.

These 92 new projects have been added to 39 active projects, for a total of 131 managed projects in IT Services’ current portfolio. The portfolio is updated weekly, and can be accessed on the Project Office website at www.muohio.edu/projectoffice by using the link on the left titled "Project Hot List."
IT Services Wants to Hear from You!

This October, IT Services will be seeking feedback on the state of IT at Miami and we want to hear from you. As part of our annual IT Strategic Plan renewal, we will be conducting forums and an online survey to gather valuable feedback and your input is important to us. Your thoughts, questions and ideas will not only help us gauge the current state of IT, but will also be helpful in shaping the future direction of IT at Miami. The forum dates will be announced soon on the IT Strategic Plan website, in The Report and the Miami Student.

To learn more about the IT Strategic Plan, please visit: www.muohio.edu/itplan

Lights, Camera, Action!
“Loaner” Digital Camcorders now available from the Gaskill LTC

The Gaskill Learning Technologies Center (LTC) in 200 Gaskill Hall recently acquired four new Canon camcorders for student use. Currently enrolled students can borrow these digital video-cameras for up to 2 days. To use the camera, students must have a mini-DV tape which can be purchased from the Bookstore or off-campus.

To help students understand how to use the camcorders, a short, easy-to-understand overview titled Using the Canon Digital Camcorders was developed by students in a upper-level technical writing class. This overview complements the full Canon instruction manual which is loaned out with the camera.

Once taping is complete, students can return to the Gaskill LTC to use iMovie on the Macintosh computers in the Multimedia area to edit and enhance their movies. Again, a new, student-developed set of instructions is available to help students quickly learn to use iMovie.

To check out a digital camcorder . . .

Visit the Consultant’s Desk in the Gaskill LTC, 200 Gaskill Hall with your Miami ID card. You will be asked to complete a form verifying your student status and acknowledging receipt of the equipment.

Laptops & iPods: the Fine Arts Mobile Community

By Brad Myers, Computer Services Coordinator, School of Fine Arts

Over 3 years ago, student-owned laptops & iPods invaded Architecture & Interior Design and the mobile community never looked back! Was it innovation at its best? Almost! The program was actually adopted to compensate for diminishing equipment budgets...crunches we’ve all had to deal with.

Drop in to any studio and you’ll find students scattered, typing or designing away on a laptop, sharing or collecting information through wireless connectivity and tapping to the latest tunes playing on an iPod.

Mobility has given faculty a freedom with teaching structure. The students get the benefit of a personalized and portable learning environment that doesn’t change when they return to their dorm or apartment. And, the department is able to focus on more specialized, high-end computer clusters.

Issue Number 13 September 29, 2005
Laptops & iPods: the Fine Arts Mobile Community (continued)

How do you implement such a program? Requiring a specific computer is a difficult proposal. Some students will already have computers purchased a year ago. We anticipated this and decided to strongly recommend packages instead. The Miami Bookstore, Apple and IBM were key in working with us to market bundles and passing savings on to students well under Miami’s institutional pricing. I was nervous the first year, wondering how parents would embrace such a program. I was surprised and pleased to discover most parents were relieved to know what to purchase for their kids.

The program has been so successful that the School of Fine Arts has adopted a laptop requirement in the other departments of Art, Music and Theatre. Ok…that’s great! However, with well-equipped students the faculty was feeling a little underpowered to say the least! Not to worry! Our technology-savvy Dean, José Bowen worked with me to create a Technology Jumpstart Program that seeded $50,000 in the form of 21 laptops and 42 iPods to faculty.

There was a catch. Faculty had to submit…in 40 words or less…how they would use the technology given them. It wasn’t truly competitive, but what we did learn was ‘how’ faculty intended to use technology in the classroom. Overall, it’s been a win-win situation for everyone. For more detail, you can contact me, Brad Myers, at myersbw@muohio.edu.
E-mail Tip: Using Spam Scoring to Filter Junk E-mail

Miami’s incoming e-mail server uses a spam scoring system that provides the option of configuring e-mail applications (myMiami, Outlook, Eudora, etc.) to filter e-mail identified as spam, so it is not delivered to the in box.

What is Spam Scoring?
Each message is reviewed, using multiple tests, to determine if it is spam. Messages that appear to be spam receive a spam score; the spam score is placed in an "X Spam Score Message Header". The higher the spam score number, the greater the likelihood that the e-mail is spam. If the X-Spam Score is one or above, the spam score, along with the number of asterisks representing that score, will be present (see example below). If the X-Spam Score is lower than one, the e-mail is considered less likely to be spam and then only the words "X-Scanned-By: MIMEDefang 2.42" will be present.

Example of an X Spam Score Header:
X-Sender: samplejq@po.muohio.edu
Date: Tue, 26 Oct 2004 09:20:31 -0400
To: samplejq@muohio.edu
From: John Sample <samplejq@muohio.edu>
Subject: Test Junk Mail message
X-Spam-Score: (****) 4.021
X-Scanned-By: MIMEDefang 2.45

Testing to date has shown that any e-mail flagged with a score of one or above is very likely to be spam. Please note that spam scores are assigned by the system and cannot be altered.

Will Spam e-mail be delivered to me?
You will receive ALL messages addressed to you, regardless of spam score. You make the decision as to whether and how you wish to manage e-mail flagged as spam. This approach prevents the mishandling of messages incorrectly identified as spam and leaves the control of what happens to spam messages to you.

How do I use the Spam score to manage spam?
To manage spam messages, you will need to create a filter in your e-mail application based on the X-Spam-Score header. The filter can be configured to move messages to a different mailbox (strongly recommended) or to delete messages. For more information on how to set up a filter in your e-mail application, please refer to the Knowledge Base cases on creating Spam e-mail filters.

IT Services strongly recommends that you create a mailbox named "Spam30" and filter messages to that mailbox. We recommend you periodically check that mailbox to see if any messages have been misidentified as spam. Please keep in mind that, if you have your e-mail application set up to use IMAP instead of POP, the messages filtered to the Spam30 mailbox will be deleted 30 days after their receipt.

Outlook Express note: Outlook Express cannot filter messages based on a message header. Those using Outlook Express should upgrade to the Outlook e-mail application provided as part of the Microsoft Office Suite.

What is the difference between POP and IMAP?

**POP:** If your e-mail application is configured to use POP, messages sent to you are stored on Miami’s e-mail server until you connect and retrieve them*. When you check your e-mail, your messages are downloaded to your computer and, based on the options configured in your e-mail application, removed from the mail server. With POP, you will need to delete the spam messages that have been downloaded to your computer manually, after they are filtered to the Spam mailbox.

**IMAP:** If you have your e-mail application configured to use Internet Message Access Protocol (IMAP), your incoming e-mail remains on Miami’s e-mail server until you delete it*. You can read and manage your e-mail from different locations. Your In, Out, Sent, and Trash mailboxes, plus any mailboxes you create, are visible to you no matter what computer you use to access your mail account. If you are filtering spam e-mail, IT Services recommends that you create a mail folder for Spam e-mail named "Spam30". IT Services will delete any message over 30 days old from your Spam30 mail folder. This is a convenient way to further manage spam messages you may receive.

IT Services recommends that those who use Eudora as their e-mail application use the POP protocol, as Eudora’s handling of IMAP is not optimal at this time. Those who use Outlook may use either POP or IMAP.

*NOTE: Please check your e-mail at least once every 30 days. To protect the storage capacity of Miami's e-mail server, all e-mail that goes unchecked for longer than 30 days will be deleted. You do not have to read each individual message, you simply have to check your e-mail at least once every 30 days using any e-mail client (myMiami, Eudora, Outlook, etc.).
Update on Peer-to-Peer File Sharing

Miami implemented a ban on Peer-to-Peer (P2P) file sharing applications in spring of 2004, due to the virus activity on ports used by P2P applications. When the ban was lifted for 30 days in fall of 2004, the university was deluged with ‘copyright infringement’ notices from RIAA and other copyright holders. Miami reinstituted the ban on P2P so that staff time could be spent on service improvements, not on reacting to potential law suits.

In addition to the virus activity on these ports and the legal issues that individual students face when they traffic in copyrighted music and movies, there is the issue of intellectual property and how universities balance the desire for an open network with respect for those who own intellectual property.

Miami will be reviewing this ban during the current academic year and strategizing on all aspects of this issue: protection of university interests; benign uses of some P2P services (primarily, application updates); intellectual property rights; rights of the individual.

Please watch future issues of TechTalk for updates on this topic. Updates will also be published in the Miami Knowledge Base case # 50899, P2P file sharing at Miami, as they become available.

I need tunes! Legal online music sources

There are many legal sources of music on the web. Check out www.musicunited.org* to view one popularly referenced listing - or do an Internet search for “legal music”.

* Information obtained at this site is not endorsed by Miami University, nor does the site express the opinions of Miami University. The information noted here is meant to provide a starting point for finding resources and information and should be fully evaluated by the consumer before use.
Information Security Series: Are You Harboring a Bot?

A bot (short for robot) is a program that is placed on a computer without the knowledge of the computer owner and is used by a hacker to launch attacks on other computers. For instance, on June 16, 2004, a large network of botnets attacked several major web sites (Google, Yahoo, Microsoft and Apple Computer) by blocking access to their sites.

Bots can also be used to send spam and install keystroke logging software that captures passwords, credit card numbers, financial records and other private information about the victim.

Protect your system from becoming a bot!

To reduce your risk, use a personal firewall on your machine (like the Windows XP Service Pack 2 firewall), keep your anti-virus software updated with the latest virus definitions and keep your operating system up-to-date with the current fixes and patches. Please check the “Protecting Your Computer” section in the Knowledge Base for more information on all these topics.

More about bots and botnets . . .

Bots are installed by an attacker using worms or viruses that place a backdoor component on the machine. The bot runs silently in the background, letting an attacker send commands to the vulnerable system. The owner of the machine has no idea this is being done. Bots take advantage of vulnerabilities that are often found in software programs and operating systems. Mass-mailing worms, found in e-mail attachments, can carry a bot. Most bots use Internet Relay Chat (IRC) or peer-to-peer (P2P) to communicate with and receive commands from hackers.

Botnets (short for bot network) are formed when a collection of computers have been compromised by software specifically designed to create a network of systems for attack purposes. Botnets can be used for mass spam mailings and for installing key logging software that can capture passwords, credit card numbers, financial records and other private information about the victim. The latest statistics show that botnets send nearly 70% of spam today. Bots and botnets are increasing in number and are becoming more sophisticated.
I Wish I Knew: Student Voices of Experience

Who knows best what students need to know about technology to survive and thrive? Students, of course! During spring 2005, IT Services asked students what technology advice they felt would be most valuable to other students. We received lots of great responses which we'll be sharing in this new feature column in the student edition of TechTalk.

Whether you're an incoming freshman or well on your way through your college career, we bet you'll pick up some valuable tips.

Have some advice you'd like to share? Please send it to techtalk@muohio.edu.

This issue's technology tips . . .

Tip 1: BACK UP, BACK UP, BACK UP!

By far, the number one thing students said they learned the hard way was to back up their files!

"Two weeks before finals my hard drive crashed, and I hadn't backed anything up. I lost everything on my computer - pictures, songs, word documents, projects, everything. I wish I had known how important it is to back all my important documents up on CDs or something."

L.W., Sophomore, Public Administration

There are lots of storage options for backing up:

- Universal Disk Space - 100 MB of personal storage space on Miami's centrally maintained file servers
- CDs/DVDs (if your computer has a CD or DVD writer)
- USB memory drive

More detailed tips on backing up can be found in the Knowledge Base - just search for "backing up".

Tip 2: Be very, very wary of IM links and e-mail attachments

Many students indicated they quickly came to regret opening e-mail attachments or clicking on links in IM messages, even in messages from people they knew.

"Not every e-mail sent to you is safe; never open ANY e-mail that was sent to you by an unfamiliar address. Additionally, if you use AOL instant messenger, never click on any links sent to you by people that you don't know, or sometimes by people that you do know - there are a LOT of evil little viruses out there that will sneak their way onto your computer. Never open anything that looks fishy."

R.S., Senior, English

"Be sure of every link that you receive in an e-mail or on instant messenger before you go to it it could be a virus! Also beware of viruses that are disguised under seemingly okay names: "pics!" "flowers", or "hey, check this out!" type things, it often means disaster for your computer, as well as everyone on your address or buddy list."

J.S., Junior, Journalism

Remember, it's easy to fake "From" e-mail addresses, so even if a message is from someone you know don't open the attachment unless you are expecting it!
Hardware Repair Service Brought In-house

In March 2005, IT Services began performing hardware repair services for university-owned computers. Bringing the hardware repair operation in-house has doubled the resources for this service while lowering the cost to the University.

Upon bringing hardware repair in-house, IT Services - Support Services hired two stellar hardware technicians with decades of experience fixing personal computers and printers. These technicians are able to coordinate the service for any computer or printer owned by the University.

IT Services has agreements with Apple, Dell, IBM/Lenovo, and the HP printer division that allow these technicians to directly service machines under warranty from these vendors. The agreements provide access to higher level vendor support, when needed, as well as labor reimbursement for many types of repairs. Warranty repairs are provided at no cost. Service for out-of-warranty repairs, however, necessitate a $20 service fee, plus the cost of any parts and shipping. While Miami’s hardware technicians can coordinate warranty repairs for products from other vendors, service is slower, as the technicians cannot perform the repairs directly. IT Services is exploring the creation of service agreements with other vendors as demand dictates.

The current agreements extend to personally owned equipment made by Apple, Dell, IBM/Lenovo, and HP (printers only). As long as the product is under warranty, IT Services can repair the product at no cost to the owner. At the current time, repairs for personally owned computers and printers that are out-of-warranty cannot be conducted, although IT Services is working to supply this service this academic year.

Hardware repair services are scheduled through the IT Services Support Desk. If you have a computer or printer that requires hardware repair, please contact the IT Services Support Desk at supportdesk@muohio.edu or 513-529-7900.