INFORMATION TECHNOLOGY COMMITTEE MEETING
February 11, 2010
2:00 pm -3:30 pm
Washington Street Campus, SSC 277

Minutes

Members Present: Lee M. Colaw, Lynn Thornton, Robert Austin, Claudie Biggers, Ed Nolte and Kim Davis

Members Absent: Gina Garrett, Delton Moore and Dan Ferguson

Guest: none

I. Action Items
   a. Approval of the Minutes – December 3, 2009 - Motion was made by Kim to approve minutes as written, Bob seconded the motion. Minutes approved.

II. CIO Report
   a. General update (Lee)

   1. Rogue DHCP Challenge - we have been experiencing what we call a “rogue DHCP” attack. A rogue DHCP attack is a fairly simple attack that causes a denial of service by not allowing legitimate computers to obtain DHCP addresses in order to access network resources. Let me explain what is happening during a rogue DHCP attack. It begins when a DHCP server that is not under control of Information Technology Services (ITS) is connected to the network by an unknowing user (usually a computer infected by some type of malware or virus) or a user intentionally wanting to interfere with the normal network operations. Historically in the former case, that of an infected computer is the most common occurrence at a college or a university. As users connect to the network; both the rogue and legal DHCP servers will offer them an IP address. If the information provided by the rogue DHCP server differs from the legal IP address, then users receiving IP addresses from the rogue DHCP may experience access problems to obtain network resources, such as access to the Internet.

   Please note this denial of service will only apply to computers trying to acquire an IP address during the time period when both a rogue and legal DHCP servers are broadcasting. Most of the College computers were already on the network and that is why in the previous paragraph I said this problem is not a systemic issue across the entire network. Only a minority of the computers trying to acquire IP addresses during the time period in which the rogue and legal DHCP servers were jointly broadcasting were affected. This problem primarily occurred last Tuesday and Thursday beginning around 9:30 am and then it would gradually subside till around 1:00 pm, with normal operations resuming about 2:30 pm. We experienced a similar problem during the fall semester on Mondays, Wednesdays and Fridays; but it was resolved in the November timeframe and did not reappear again until last week.
The intermittency of this denial of service attack makes it a little more challenging in identifying the source of the problem. Last week the networking staff traced the problem to the Byrd Business building, room 216 in the CIS area where a whole lab was unable to connect to the network. It was found that a large amount of malware had been inadvertently loaded on these computers while preparing for the spring semester. The appropriate parties are cleaning up these systems and the probability is moderate this will resolve the current rogue DHCP issues. It must be stated that a rogue DHCP denial of service attack cannot be truly prevented, especially in an open college environment. However there are ways to make a DHCP based network a little more resistant to attack and we’ll continue to strategically implement those solutions that do not restrict the flexibility of the faculty and students.

You may be wondering what a user can do to ensure the integrity of the network to prevent rogue DHCP attacks and other viruses, Trojans, and anomalies from occurring. The answer is the user has everything to do with preventing an unauthorized attack. In a sterile world where we did not allow the use of the Internet, or the use of CD/DVD drives, or memory sticks we could reduce the chances of an attack to less than 10%. However that is not the world in which we live. In today’s world we provide an open environment allowing the exchange of information from more sources than we can count. Users should perform daily maintenance to ensure their computers are up to date with the latest operating system patches, application software patches, antivirus updates, and never open email from someone you do not know. User performed daily maintenance is the number one way to combat anomalies on the College network. If a user has trouble logging into the network they should simply turn their computer off, and then turn it back on. This operation may have to be repeated a few times, but more times than not the user will receive a legal DHCP address and get connected to the network.

While these service interruptions last week may seem widespread to those affected, they are generally not that extensive. The College community as a whole continued to work without incident last week so I would ask that intermittent network outages be viewed in their proper perspective.

A LAN/WAN engineer (third tier support) will be on site to trace and help with the problem.

Question was asked if this is a growing pain in opening up the system to the world. Mr. Colaw Responded by saying yes and no, yes because we’re opening it up we could close it down to where no flash drives would be allowed, but it is also an indication that we are running behind on technology security. Every campus has some issue to address.

2. Surveillance Security cameras-- there has not been a guidelines agreement established on the care and maintenance of the surveillance cameras. No policy is in place yet, but the some guidelines have been established:

1) The Emergency Manager will be responsible for and have access to all Amarillo College security camera systems except the one located in the Art Museum.
2) The Emergency Manager will monitor the systems on a daily basis to determine if the systems are operational. If systems are not operational a work request will be sent to the Help Desk. The Director of Administrative Services/HR to be the designated backup for the Emergency Manager.
3) ITS will be responsible for maintenance of systems which includes all cost associate with such maintenance. If work is to be performed at a Branch Campus location, the Branch Campus will be charged for all maintenance and repairs.
4) The Emergency Manager will obtain a list of users from the areas which the systems cover in order to restrict use of systems and to establish new network id's and passwords.
5) The Emergency Manager will have the responsibility and ability to view past “footage” in the event of an incident which warrants such review.

Lynn commented on some older systems that need replacement. Rusty Cornelius will budget for new updated systems.
Ed suggested contacting John Keel from the Panhandle Regional Planning Commission. Mr. Colaw will follow up on contacting John.

3. Update on School Messenger Emergency Notification System - School Messenger offers delivering emergency alert services through voice, SMS text and email messaging. We have the system where it’s currently building the database. The new website will be www.actx.edu/acalerts where you could go in and add your new contact information. An email will be sent out when someone changes their contact information to HR and Registrars office. It will not be go automatically in the Datatel system. The ITC will be the testing group before going out to the AC public.

4. Computer Replacement Status - There should be enough TRTF funds for the upcoming annual computer replacement. The goal of TRTF is to keep the technology budget protected.

III. Discussion/Information Items

a. Common UserID and Password – discussion form ATC; faculty identified the need for a common username and password system. A common AC Net ID is needed that is good anywhere on campus. This includes students, faculty and staff. The goal to have a common AC Net ID to log in into the system in service by summer 2010. Special accounts will also be covered with the common interface. With this interface everyone will be able to maintain their own profile, will allow self-service wireless registration of wireless devices; no wireless access form will be necessary. This is not the same as the single-sign-on (SSO) environment, but it emulates an SSO environment.

b. Appropriate Use Policy for Information Resources – Mr. Colaw brought forward the recommendation to rescind the Email Policy and the Data Access and Information Security (DAIS) policies. Some issues concerning online gaming were discussed, and the committee was asked to review the wording and make recommendations for change. A vote may be proposed at the next meeting.

c. Development of a Faculty Technology Grant Initiative – discussion tabled, after Mr. Colaw talked to CTL, no need to continue.

d. Student Email – MyAC is not being used 100% by students and faculty. Many faculty are still using student’s private email addresses to contact them, instead of using the MyAC account. Mr. Colaw discussed the possibility to move students email system to Gmail. Gmail Google Docs will enable students and faculty to share documents online, at any time and from any location. It will easily integrate with our current system, while keeping our schools domain safe and secure. Collaboration tools, calendar, etc. The use of Gmail could also limit the College’s liability. A directory would have to be maintained with all the students email addresses. This would also work with the proposed emergency notification system, and the common user ID and password system. The future of the portal is in question; as it does not seem to represent the culture at AC, and it has not and continues not to meet the needs of the college. Discussions on this topic will continue.

e. Strategic and Budget Planning (Lee) – Coming into the budget planning timeframe, ITS is attempting to budget out for at least 5 in years advance in order to stabilize the technology budget. One item discussed in January was the list of reviewing what computers are supported and not supported. Mr. Colaw would like to bring the technology budget to ITC to look at and discuss what is being used for and where is going.

f. ACT (Kim Davis) – No report

g. ATC (Dan Ferguson) – Claudia reported that there are still issues on student taking online classes not knowing how to navigate through Angel. Claudia will submit some question from students to Mr. Colaw.
IV. New Business –

a. Questions and Concerns
   1. With students email changing to Gmail, will a query be built to attach to student records and does an email blast to everyone? Yes, you will be able to sort by departments, students, staff and faculty.
   2. When will staff and faculty get more email space? Goal is by this summer.

Next Meeting – February 25, 2010, SSC 277

Membership

1. Chair: Dean of ITS/CIO – Lee M. Colaw
2. Faculty Senate President or Representative – Claudie Biggers
3. Administrators Association Chair or Representative – David Ziegler
4. Classified Employees Council Chair or Representative – Gina Garrett
5. Continuing Education Representative – Kim Davis
6. Finance and Administrative Services Representative – Lynn Thornton
7. Enrollment Management Division Representative – Robert Austin
8. Assessment Development Division Representative – Delton Moore
9. VP Council Representative or Instructional Division Chair Representative – Ed Nolte
10. Faculty Member At-Large – Appointed by VP/Dean of Instruction – Dan Ferguson
11. Recording Secretary: Rose Dukes, Executive Assistant

CHARTER

The Information Technology Council (ITC) is charged with:

- Review technology related policies, processes, and procedures recommended by the subcommittees and or sub-teams.
- Presentation of pertinent issues and recommendations (such as new policies) to the President’s Cabinet for consideration and review.
- Review and oversee the Information Technology strategic plan.
- Oversight of Technology related committees in terms of charter, representation, and focus.
- Coordination and communication of pertinent information regarding technology based needs, goals, and activities with the representative areas of the AC community.
- Discuss and prioritize IT initiatives and ensure alignment of IT initiatives with the institutional Strategic Plan.