
Absent: Sue Achteneier, John Anderson, Greg Ashley, Melanie Bone, Michael Brewer, Sharon Burch, Mark Cherry, JoEllen Childers, Maria Cleghorne, Michael Dennis, Bert DeSimone, Shefali Dhar, Debbie Ellerson, Tammy Holman, Stuart Ivy, Rehan Khan, David Knox, Will Laney, Juan Machado, Tammy McGarity, Anthony McLeod, Jeff Pentz, Nathan Pettigrew, Jeremy Sanderlin, Cletus Stripling, Rayid Tartir, Jeff Teasley, Dale Wetzelberger, Dr. Barbara White, Chris Wilkins, and Chris Workman

Approval of Minutes: Minutes from the October 4, 2007 meeting were approved.

Welcome of Visitors:

Featured Speakers/Discussion:

Lynn Latimer: Compact Planning Update: Handout

EITS has taken all the comments we have received and grouped them based on our services which can be found in the UGA Fact Book. Then we have grouped all the comments based on topic area.

Different directors within EITS have been assigned to look at this initial pass of consolidated items and do several things: 1. Make sure the alignment with a given service is correct 2. To assess if the topic is correct and to determine if the comments are just feedback that we received versus something that could actually be a new project or initiative that we need to move forward on. This is the process that we are working on now.

My goal within the next few weeks is to have some internal meetings with EITS staff to gather their input as well. Then this information will be pushed out on the Compact Planning Website. This is an aggregated report where all of the comments will be out there and available to view and drill down on for further information. We have a list of everyone who attended the Compact Planning Sessions and they will be notified via email that the report has been posted.
One of our focuses is to make sure that everyone who submitted a comment(s) knows where it will get integrated, if it does get integrated, if it doesn’t, why. This is one of the pieces of information that we heard back during the sessions. Individuals wanting to know want happened to the input that they provided.

**Stan Gatewood and Sandi Glass**: UGA Role-based Security Accountability Model

Update: Handout

Security is an extremely important issue here at UGA (IT Security, Information Security, and Data Security).

UGA has had a number of security incidents over the years and one thing that stands out in just about every incident that we have responded to was the people issue.

We recognize from this that security cannot be handled just by the Office of the CIO and The Office of CISO. So what we proposed a while back is that we deputize individuals as security liaisons, and that everybody around campus has to understand that security is everybody’s responsibility. It is a shared-responsibility. The central office cannot do it all alone and now we have people listening to that fact and now we have action behind it.

**Vision Statement**

The **vision** for the University of Georgia is a campus environment where the protection of sensitive and critical data, and information technology resources, is a shared responsibility among administrators, faculty, staff, students, and IT professionals.

This responsibility will be addressed campus-wide by implementing information security **best practices** based on individual **role** and **level of accountability**, and will be supported through building increased awareness and participation in training and educational opportunities.

**Historical Perspective:**

2007 Senior VP Campus Memo- “Role/Accountability” Campus-wide Plan

Accountability for implementation of University security standards, policies, processes and procedures based on individual position and level of responsibility.


2006 President’s Retreat – “Securing UGA Sensitive Data: Current Status, Challenges and Future Directions” Atten: Issue #5 – Acceptance of shared responsibility for institutional data and information security campus-wide
2005 Campus Memo – “Securing Sensitive Data Initiative:” Phase I: UGA Auditor/CISO high risk Assessment (19 campus units) – Phase II; Inventory of all assets (i.e. servers, databases, personnel) through ASSETs Online software application. Version 1 (350 campus units)

In this security model every person has role in security. (From Awareness, Policy Making, Policy Enforcement, and Resource Allocation and to the Technology part where we actually work on the technology and have hands on of our systems and our data processes that we build. This model is base on best practice. A lot of research has been done and we had to approach it from three different roles: technology, process and people.

This is our first iteration, ITMF will be very important to this process because we are going to do a lot of training and awareness campaigns. Travis Ray and Stan will be developing a website that will be used as an online resource for you to get to presentations, training opportunities, podcasts etc. (www.ssdi.uga.edu)

On May 6, 2007 the Senior Vice Presidents sent out a memo to the campus indicating specific actions by campus entities: Stan will forward the memo to the group for part of the minutes.

The Chancellor will be holding each president accountable for the safety and security of the institutions. When it comes time for the annual performance review process each president will be required to show their security and accountability model for each one of their institutions. The president has arranged to have his annual training.

Other levels of Accountability and Responsibility in this model are: (Refer to Handout)

- Executive (Vice Presidents, Deans, Vice Provosts, Assoc. Provost, Dept./Unit/Division Heads)
- IT Leadership, Management and Unit Security Liaisons
- IT Administrators (Network, Systems, Database, Web Administrators and Programmers)
- UGA Community – Students, Faculty, and Staff (Focusing on Faculty and Staff for now. We will be working on how to roll out awareness education to the student in the very near future).

One of the things that was very exciting to see in this effort was a spreadsheet that has the role of the person and the training that is available for that role. There’s also a first look at what we considered at the beginning as required training. Most if not all of the training is available online through Elementk, or through Training and Development. The training material has been developed specifically to support this model.

We decided to look at the IT job roles because when Stan did the research with his team on what this should look like, the levels of accountability and the level of skills and
knowledge that you would apply to the work fit very well with our Assistant, Associate, Specialist, and Principles job classification levels.

We made an assumption at the beginning of the process that an Assistant System Administrator, Assistant Network Administrator, and Assistant Application Developer should not be solely accountable for protecting sensitive data. They should not be the one that designs the system to take care of all of this. That does not mean that an Assistant might not be working on a system with sensitive data but that they would be under the supervision of a more senior system administrator.

So while there will be skills and training for everyone on campus including the Assistants, when you start looking at the levels of required skills and training you will see a lot of focus on the Associate, Specialist and Principal Levels. This is all going to be out there. Career path information for example from Associate to Specialist will be out there to look at.

The assumption was made and voiced to the Provost that an Assistant should not be handling their own sensitive data. There are several options: Get the person reclassified, get the person trained, or use EITS or some other opportunity to host the sensitive data.

The Role-based /Accountability Model is based on the relationship between two people: The supervisor and the supervisee. Resources, planning, and monitoring the success of training and skill acquisition are built into the performance evaluation process.

Implementation Timeline: The first phase of communication and training will begin in October/November 2007.

Awareness, training, and education materials already exist on campus and many are free-of-charge.

SANS will be coming back to campus. It will be the same price. Training should begin sometime after Feb/March of 2008. We will be sending out a survey to this group and other groups to see what type of training we want here from SANS. The funding is coming from the University System of Georgia so therefore we will again open training up to all 35 institutions and public libraries.

**Hunt: Review Charter, Discuss ITMF’s Future: Handout**

**ITMF Charter**

Two sections of the charter that seem to be relevant to describe who we are and what we are supposed to be doing are:

Section 1.2: Charter

- Serve as Advisors to CIO (ITAC), CISO, & EITS
- Lead and Advocate
- Facilitate Collaboration and Communication
- Promote and Adopt Efficient Practices
- Integrate Local and Central Services
- Provide Input on Standards and Policy

Section: IV: Duties

- Make IT responsive, effective and innovative.
- Increase the efficiency of IT operations
- Integrate IT services across campus
- Align IT with UGA Strategic Goals
- Shape IT Policy and Standards
- Identify Common Priorities
- Facilitate Collaboration among Units
- Propose and Prioritize Projects of Broad Interest

Brad’s challenge to the group is to reflect on the items listed above and really think about what these things mean to us and more specifically, how are we going to live up to a charter that we crafted and put in place.

There are specific areas that we can point to and say “yes” we are doing these things. Is that enough? Are there other things ITMF should be doing? What activities do we need to initiate? What ideas do you have? This is where Brad would like feedback from the group.

Brad and Carol met with Dr. White recently and talked about things that are going on in her world and to find out what she wants from ITMF.

Dr. White’s message is that:

- She wants ITMF to be an influence on campus. There’s a great opportunity with the collective roles that we play to really drive things on campus. She wants ITMF to be proactive about that. She takes the committee’s rolls as an advisor to the CIO very seriously. She wants to hear from us about the issues we see on campus.

- Occasionally, she may ask us to do something specific, but she prefers that we bring the issues to her.

Dr. White, Brad, and Carol will try to meet on a monthly basis.

ITMF also plays a roll in advising the CISO Office and EITS. CISO attachment is the Security Committee but no real solid mention that this is the role of the Security Committee. No specific role in advising EITS other than informal conversations.
**Reports from Committees:**

*Security Committee*: The security committee is a standing committee with an identified membership. No chair has been identified for the committee. The committee just needs to get itself started. Matt has meet with Stan a few times on behalf of the committee just to try to keep the conversation going. The committee has looked at the Privacy Policy and have taken a first best try at it and sent it to Stan to look at.

*By-laws Committee*: Christine Miller, Chair. Very few changes were made to the charter. A motion was drafted in a meeting that accepted the recommendations. One change that occurred was the change in the “membership” section of the charter.

**Unfinished Business:**

Any current or former chair of a sub-committee should send Brad the name of the committee along with the name of the members.

Also, if you are a former sub-committee that falls under unfinished business please recognize that and raise the issue with the group. We will collect the information and add it to the vision statements so we can decide where we want to spend our time and efforts.

**New Business:**

Brad made a request on Sohayl behalf for ITMF representation on the CESS Review Process Committee. If you would like to volunteer for the committee, please email Brad .

Chris Adcock is looking for a collaborative employee development and training effort within ITMF.

**Summary of Action Items:**

- Set an agenda item for the next meeting for a collection of units to volunteer to share what they are doing on security awareness campaigns.
- The group needs to identify an accountability training team and volunteers.
- The security accountability topic will be placed on the next agenda(s).
- Brad will ask Sohayl to send the objectives of the CESS committee out to the ITMF group.
- The chairs are to report the committee, the membership, and any unfinished business.
- Individuals interested in collaborating on employee development and training and areas of common interest are to contact Chris Adcock. Chris will report back to the group.

**Future Discussion Items:**
Take one meeting a year and make it a full day event. Take some very meaty issues and take the time to discuss them. We will have a committee to organize it, pick the topics and invite senior leadership to come present at the meeting. Perhaps at the next meeting we can talk about formalizing it as a proposal.

Possible Committee: Integrate local and central services. Would be a great group to lead, advocate, disseminate, and study. It could also be an all day session.

**Meeting Adjourned**