Faculty Information Technology Advisory Committee (FITAC)

FITAC Annual Report
February 8, 2013

Anselmo Lastra, Chair (lastra@unc.edu)
Suzanne Cadwell, Timothy Carey, Ryan Madanick, Laurie Maffly-Kipp,
Michael McNeil, James Porto, Marc Serre, David Thissen, Barbara Wildemuth
Members with term that ended AY 2012: Laurie Cochenour, Carlton Moore
From ITS: Larry Conrad, Chris Kielt, Ramon Padilla, and Stan Wadell

The charge of the FITAC is the following.

> The committee represents to the chancellor and the University community the concerns of faculty and others with regard to information technology. The committee's functions include:
>
> 1. considering issues pertaining to the use of information technology in teaching and learning, research, and other professional activities in the University; and
> 2. advising University officers and offices of administration on faculty needs and interests relating to information technology.

The committee has met three times since the last report.

At one meeting, we focused on the new data-stewardship report and on support for faculty. The report is available on

http://sils.unc.edu/sites/default/files/general/research/UNC_Research_Data_Stewardship_Report.pdf

Cloud support is one area that could use attention. ITS has a plan for faculty and staff secure cloud disk storage, but funding has not been available.

At a meeting in Fall of 2012, we discussed a proposal to install a firewall. A document from Larry Conrad and Stan Wadell is attached as an appendix. This topic is still under discussion with various groups.

In January of 2013, the committee discussed the proposal from ITS to lengthen the password expiration period, perhaps to as long as one year. To make passwords more secure, this would be coupled with a more stringent policy on the composition of passwords including a longer minimum length. Not surprisingly, the committee was very positive about this change since we had in the past discussed research results showing that frequent changes do not make for more secure passwords [1]. The ITS security team hope to roll this out in 6-8 months, but first need to make software changes and obtain approvals.

The password changes will likely come at the same time as new wireless networks are deployed to more of the campus. ITS encourages early adopters to use UNC-Secure.

Additionally, the committee members expressed their best wishes to Larry Conrad in his new job at the University of California, Berkeley.

A topic for future discussion is the effect of FERPA on faculty productivity. For example, are faculty members allowed to keep this semester's class grades on a laptop? We decided to invite university counsel and the Registrar to a future meeting on the topic. The goal is to publish guidelines.

[1] Yinqian Zhang, Fabian Monrose and M.K. Reiter. *The Security of Modern Password Expiration: An Algorithmic Framework and Empirical Analysis*. In Proceedings of ACM Conference on Computer and Communication Security, Chicago, 2010. See http://cs.unc.edu/~fabian/papers/PasswordExpire.pdf.

The FITAC web page is

http://faccoun.unc.edu/committees-2/appointed-committees/faculty-information-technology-advisory-committee/

or the shortcut

http://go.unc.edu/fitac

You can also use the following QR code.

Attachment:
Information Security Strategy/Philosophy
at UNC Chapel Hill — September 18, 2012

Information Security Strategy/Philosophy
At UNC Chapel Hill — September 18, 2012

Network/Computer Security is a never ending challenge to keep University and personal information and resources safe from those who would do us harm or utilize them for their own purposes. Over the course of the last 10 years, Internet rogues/villains have become increasingly more and more sophisticated in their methods of attack. They're smart, creative, capable, motivated, relentless, automated and 24/7.

Most large organizations have made significant investment in tools and put policies and processes in place to attempt to thwart these attacks…and we have done the same. However, Higher Education institutions, including Carolina, have been slow to adopt a major philosophical shift in the way computer environments are structured that is the norm for most corporate and governmental organizations: restructuring their networks and network practices to make it more difficult for troublemakers to get in to do their work while, at the same time, making networks easier to manage.

The reason for this reluctance stems from a long tradition of academic sharing, openness and transparency. These are admirable goals that we should not lose sight of, yet we must face the realities of today, where a completely open network is an invitation to those who would steal our data, identities and ideas and misappropriate our resources. We must also acknowledge that – as the world and technology has changed around us – our institution (like other major research universities), with our high bandwidth connectivity and 60,000 networked devices, is a literal bounty of information and resources that are highly prized. We're a veritable "destination resort" for the worldwide criminal and hacker communities. From a student's information to a researcher's life's work to the identities of our community members to our intellectual property, our University is a gold mine of information.

Because of these present realities, it's time to take a fresh look at the network design and practices that are part and parcel of our information security philosophy to see if we can find a more secure balance that enables us to continue to be agile and effective as a campus, yet create a safer computing environment. In the coming weeks, ITS will be dialoging with campus partners to examine fundamental changes in our information security strategy; specifically in the following areas:

A) Adding network border protection (equipment and controls) at the points where we connect to the Internet to create an environment in which the default condition is secure ("lock down" access) and individuals and units must thoughtfully and purposefully place data/information in non/less secure locations ("open up" access). This is the exact opposite of our present environment where access is generally open and we lock-down access as an exception.

B) Make secure storage and presentation environments available to the campus. We need to provide options for the campus community to place data in secure locations that are centrally managed.

C) Review and re-work our access and identity management practices. Particularly what privileges does possessing an ONYEN provide; also addressing the need to automatically de-provision access as people's roles change or as they leave the University.

D) Adopt and implement a data classification and location strategy – Data Loss Protection. We need tools to help us detect sensitive data wherever they reside and take action on the data once located.

E) Implement an annual information security awareness/training program to remind members of the Carolina community that each of us has a role to play in ensuring the University is adequately protected.

Each of these strategies would be a significant proactive change in how we have been approaching information security here at UNC Chapel Hill. Engaging in these efforts will strengthen our security posture and reduce our vulnerabilities while at the same time making it easier for campus users to maintain security compliance. However, significant work will be required by the Carolina IT community to implement these changes and greater investment in information security will be required. While vigilance is always necessary, once implemented, these changes in the campus information security strategy will reduce the security burden on users by making information security more of a "default" condition for Carolina.

Larry Conrad	Stan Waddell
VC for IT and CIO	Exec. Director and Information Security Officer