ITAC Minutes: October 27, 2011

8:30-10:00

Attendees:

Guest Attendees:
Allison Winslow, Dr. Marchbanks, Dr. Dandridge

Item 1: Approval of Minutes
Minutes from October 13, 2011 unanimously approved.

Item 2: New It Trends
- Willis Marti announced Google has revised contractual terms for agreement regarding Google apps for education. NIS is reviewing the application from a both a contractual and security standpoint. Other depts. within CIS are examining functionality of use. Possibly, could be a realistic option in FALL 2012
  (It was mentioned the University of Texas is already implementing Google Apps for education).
- Steve Conway, in Galveston, raised concern about non-emergency text messaging. It has been an issue on his campus that a number of students bypass email and only text. Steve has found a vendor that had a flat rate for product usage. An inquiry was presented regarding Cheryl Cato’s group looking into “Box-” No updates. Additionally it was stated Walt Magnusson was researching an option that charged a rate per message cost. Allison Oslund recommended that Steve get with Walt and Pierce to collaborate and combine investigative outcome of exploration; especially the question on cost.

Item 3 Announcements:
- Allison Winslow presented an update on Web accessibility review Tier 2KEP to begin November 1, 2011. She will be back in 2 weeks to outline more specifics.
- SAP requires all new and redesigned websites and web content be accessible to and useable by “all users.”
  - Standards used to define and evaluate web accessibility are outlined in TAC 206
  - Charley Clark is the University’s web accessibility coordinator, it is his responsibility to monitor adherence to that SAP
- IT Risk Management is providing technical support by scanning University’s websites using automated scanning tool “World Space Enterprise.”
Item 3 Announcements cont.:

- It Risk Management will perform baseline scans according to Charley’s plan, and rescan sites monthly, and report to Charley on a quarterly basis.
- **Definition: KPEP (Key Public Entry Points)** a webpage that is designed for the general public to access official information.
- **Tier 1 KPEPs**: Baseline scans to occur Sept 2011-these sites are designed for users with disabilities and provide information on health, safety and welfare
- **Tier 2 KPEPs**: Baseline scans to take place Nov 2011- Encompasses other sites that are not Tier 1
- Throughout 2012 It Risk Management will be completing the scans on all other sites that are not KPEPs

- Allison Winslow is asking for assistance from ITAC, to please inform webmasters, that IT Risk Management will be contacting them when a baseline scan is performed. Procedure outlined:
  - IT Risk Management will give webmaster a user account in “World Space.”
  - On their website, at completion of scan, IT risk management is requesting the webmaster to log in and view scan results; determine which are violations or which are false positives. (“World Space” scans can generate some false positives). The webmaster, if any accessibility violations or possible violations are flagged, may log in and approve occurrences manually or remediate violations. Allison emphasized the need for human determination by webmasters on how to proceed, and not to blindly accept findings.
  - Subsequently, webmasters are to continue the management process by logging in monthly to “World Space,” repeat procedures and remediate automatically or manually correct findings.
  - The goal is progress not perfection. All will not occur at once.
- Any technical questions can be directed to IT Risk Management: WebAccessibility@tamu.edu
- Any high level questions can be directed to Charley: WebAccessibility coordinator@tamu.edu

Willis Marti was asked has the law changed. He responded the Law outlines new language: “New or changed KPEPs.” Important to note the law used to only indicate KPEP, now it is applicable to all websites. Allison will speak more on that topic in two weeks.

Item 4: Password Subcommittee Report:

Henrick Schmiedche shared the Password and Subcommittee report:
(SubCommittee Members: Henrick Schmiedche, Jim Rossier, Rick Young, Bill Chollett, Jeff McCabe, Willis Marti)

Henrick presented the subcommittee’s charter, and elaborated on the first 3 deliverables.

*The following is an excerpt from the report* His report and his power point presentation were given to all present. Additionally, he will be send reports electronically to catalogue with the minutes. The deliverables are necessary to include in official minutes.
Password Subcommittee Deliverables:

1. A summary of password industry standards and best practices including how they have changed and where they seem to be headed. *(See Report)*

2. Summary answers to the five questions posed above including references to justify the answers. *(See Report)*

   A. Does the current Texas A&M password policy meet industry standards and TAC 202?  
   *The “best practices “ reflected in Texas A&M password policy is out of date and does not reflect the most recent research on the matter*

   B. Should the current password aging policy be changed? If so, how?  
   *Password aging is outdated and counterproductive and rarely does any good. It should only be used in very limited situations. Please see the “Conclusions,” section for further information.*

   C. Should password complexity rules be changed? If so, how?  
   *Strong passwords matter, but changing default passwords is even more important. Nonetheless, the research suggests that password complexity does not need to be as high or complex as previously thought. Please see the “Conclusions,” section for further information.*

   D. Should two factor authentication be used or encouraged?  
   *When appropriate/applicable it appears that two–factor authentication can greatly reduce password risk.*

   E. How should password security/authentication relate to the confidentiality/sensitivity of the information resource being assessed?  
   *Even though it may seem that the more sensitive” a resource, the more “secure“ the password should be, the complications introduced by having multiple level rules for different resources may negate the benefits of different password rules for different resource classifications. Furthermore, the DBIR reports that users are often unaware of the data on an information resource and compromised data is often not secured because it was not known to be present. As such, we recommend all password security policies be the same for all information resources.*

3. Any Additional questions and answers the subcommittee discovers are relevant to the question of passwords and authentication. *(See report)*

4. Not completed: Should the committee recommend a password policy update, a new draft SAP Information Resources-Password /Authentication (29.01.99M1.14) policy document that addresses the subcommittee’s finding. *Additionally, the report states, prior to drafting a new SAP the full ITAC committee would need to accept the conclusions from the report.*

Henrick's presentation was well received!

The only points raised to back current procedures: Changing passwords frequently could protect against the same password being used for multiple sites: Texas A&M, Facebook, Twitter, etc. If a password is compromised elsewhere; then, the practice of a mandatory reset procedure could catch and remedy that breach. Safeguarding an attack against a Texas A&M account.
4: Password Subcommittee Report cont.:

Further defined was the user’s need to understand the value of a password to protect info stored.

Question posed relevant to Government agency trends regarding passwords? Henrick responded: government agencies are incorporating both “ridiculous password complexities” and passwords that expire frequently.

Conversely industry trends for example, bank passwords, do not expire. The user provides extra authentication, more information to aide in risk mitigation procedures (questions that make sure they validate you are who you say you are)

Item 5: New Subcommittee for Business Continuity

Subcommittee for Business Continuity formed: Members include Steve Conway, Bill Chollett, John Norton, Jim Rosser, Stephen Balfour, outreach to CIS Business Continuity rep., Peter Walsh – Lori to arrange the first meeting. (Lori to verify names)

Item 6: Cloud Computing

Tabled discussion for next meeting, due to time constraint: Bill Chollett and Stephen Balfour will present at next meeting

Open Discussion:

Ron announced that the auditors had contacted Juan Garza, and reached out wanting to talk with him regarding his work with “Essential Elements.” Juan, Willis and the auditors met. The auditors stressed they were present not to “police”, but to “help.” Process will include soliciting feedback from the auditors regarding the report. The auditors stated they would never tell ITAC what to do, because in doing so, they would be auditing themselves. The auditors expressed an interest in participating in ITAC. To that end, it is a possibility they will attend ITAC meetings quarterly.

Henrick, as the IPC representative for ITAC, asked the committee for a response regarding the issue associated with releasing pictures of students, from their ID cards, for student activities. (IPC will be addressing that SAP). Henrick will pass along opinions to the IPC committee

It was stated that the practice of using student pictures is already in place in the classroom or advising setting. Pictures offered a valuable second form of authentication. Seemingly little push back; as long as safeguards are in place.

The concern was raised regarding establishing a data base which could possibly function as data source for abusers. Additionally, Willis Marti offered a response and a question: The main arena of concern is where there is currently not already face to face identification; for example: within the Employment, Admission and Scholarship units, could providing a picture offer a bias to an applicant?