Security Sub-Committee Meeting
Meeting – April 2, 2009 / Notes Prepared April 13, 2009

Attendance:

Zeb Bowden - VBI
Al Cooper – Business & Management Systems
Dale Pokorski – College of Engineering
Rebecca Simon – VPAS IT Office
Sandy Power – Hokie Passport
Mary Dunker - SETI
Wayne Donald – IT Security Office

Wayne Donald opened the meeting by expressing an appreciation for those that sent comments and additions for the notes from the last meeting. He again made reference to the purpose/goal for this sub-committee (see below) and emphasized the importance of providing input as to the areas of concern from their perspective.

> Purpose / Goal – To provide advice and counsel that assists in guiding, supporting and communicating information technology security strategic aims at Virginia Tech. The goal is for the sub-committee to provide the Vice President, SETI and the IT Security Office an indication of areas where there is a need to give consideration for assistance and/or potential solutions to a security concern.

Those in attendance were again reminded of the security review service (free) by the Information Technology (IT) Security Office and if there is an interest at any level (department, college, etc.) please contact Brad Tilley or Randy Marchany.

The meeting was then opened to have those in attendance express areas where they have to most concern, and would like to see positioned as priorities for the IT offices involved.

1. **Awareness / Education –** there was a long discussion about the importance of awareness and education for the user community at Virginia Tech and there are probably areas that are not listed that need to be added after review by the sub-committee.

   I think in general terms the sub-committee feels that there are several methods that need to be investigated, and there is a broad range of education that needs to be made available (some education is important in the short-term but there also needs to be a long-term commitment).

   Wayne Donald indicated that his office is working with Human Resources, the Professional Development area (although the person they were working with has left the university), and beginning discussion with Learning Technologies on offering more opportunities for classes. The sub-committee felt some consideration should be given to the following:

- Review methods used currently for communicating with “technology” personnel and consider how they might be improved. The group brought up several listservs, some wikis, basic mail lists, and web sites that need to be evaluated as to purpose, clientele, and how they are used.

- Technical training/education included the following:
    - i. At least a quarterly 1-2 day workshop aimed at new system administrators that would provide information on their responsibilities and specifically what to do when administering systems at Virginia Tech. This was the #1 priority item
        1. A workshop should include the following general information:
            - a. A good layout of existing services, resources, systems and ideas on how to leverage them
            - b. Knowledge of who to contact and when (i.e., who is responsible for which areas, and whether or not it is appropriate to contact those people or 4Help)
            - c. An overview of IT and data-related policies, procedures and guidelines
            - d. IT audit and security practices at Virginia Tech
        2. Discuss with HR to see if they can assist in identifying such positions when they come on board – work with colleges/departments
    - ii. Continue to offer SANS training and consider other opportunities that might provide personnel with professional certification
    - iii. Look into a possible “internal Virginia Tech certification” program
    - iv. A “mentors” program within colleges/departments or even through the IT personnel could help with needed technical assistance/direction
        1. Central IT should look into opportunities to open communication channels and build relationships between new employees and central IT

- Awareness for general user community
    - i. Continue activities with faculty, staff, and students and look at ways to reach more individuals – for example, with the verification process that will be implemented in the near future
    - ii. Investigate new techniques that can be utilized by the ITSO to create awareness and assist users – ITSO staff is currently looking at online techniques to satisfy some compliance requirements
    - iii. There are several “groups” on campus that might be interested in working with security professionals to provide a “general” awareness – for example, the Fiscal Bunch for Lunch, Administrative Assistants, secretaries, etc.
    - iv. Look at feasibility of using some of the communication techniques that the technical personnel use for the more general user

- There is a lot of security information on the Virginia Tech web, but it is scattered and sometimes difficult to locate

        i. Look into using the security web site (http://security.vt.edu) and the computing site (http://computing.vt.edu) for providing more information, tools, and references for areas of concern.
        ii. Sub-committee members were encouraged to view the contents of these two sites and offer any additions and improvements. For example, the security site has a link for System Administrators but input would be appreciated
        iii. Consider a KnowledgeBase (KB) article that would enhance getting necessary security information to those supporting the colleges/departments without their need to pull all the information together themselves.
        iv. Maybe a System Administrators' Quick Guide (this might be a part of the link on the security site for System Administrators)
        v. How should others, such as Records Management, user groups, professional development, Controller (who has several compliance issues) be involved to improve awareness and education

2. **Access Security** – under this area the major concern is finding a way to resolve system access once an individual leaves a department or the institution. Therefore, the main concern from the section below is the de-provisioning process
    - There is a need to consider how individual users are provisioned to access certain data and how they are de-provisioned (the latter being an area that needs improvements)
        i. It is important those providing access to understand user credentials
        ii. What does it mean to "provision" and "de-provision"
        iii. What happens (or needs to happen) when there is a "hostile exit" of a user
        iv. How are identities such as PID, email, etc. used / how should they be used
    - The point was made that Banner seems to work like a charm for de-provisioning so that should be considered – even providing Identity Management Services (IMS) with a list of employees who have left the university. Ways to take advantage of this type process needs to be considered in other areas.
    - There also needs to be a discussion with appropriate department on how PIDs and Hokies accounts that have been disabled can be re-enabled. Individuals that leave the university may have a legitimate reason to be "re-connected" to certain services, and it may need to be done quickly.
        i. The issue of W-2's for employees who have left the institution could be flagged to be U.S. mailed to those former employees, yet there may be a professor that needs immediate access to Scholar
    - Part of the access security area that needs to be consider is actual physical access – considered in the sense that technology that might be used for system access could very well be incorporated in actual access for facilities

3. **Secure Enterprises** – the main concern under this area was to look at what is happening with the areas below and how it there might be some repetition in certain areas.

- To be able to recover an “operating environment” in case of a disaster (or even stoppage of operations) prepare and update a Continuity of Operations Plan (COOP) – Risk Assessment (RA) – Disaster Recovery Plan (DRP)
    i. The current COOP and RA efforts are being discussed to see if they can be incorporated into one effort
    ii. There needs to be some conversations with Emergency Management to better coordinate what is being asked of departments
    iii. The IT Security Office is currently looking at developing a Data Analysis tool that would help in these areas as well as in searching for and protecting sensitive data
    iv. Consider providing examples of risk assessments and disaster recovery plans to give areas some guidance and assist in writing better plans
- Conforming to standards – industry, State, and even federal

These were the three areas that the sub-committee expressed the most concern for the colleges/departments. There are obviously other areas that we need to keep in mind as they are included in the daily tasks that not only SETI and the IT Security Office encounter but often at the college/department also.

- One area that several expressed concern about is the sensitive data issue. Although that formal process is still being developed, many departments are beginning to look at ways to either eliminate the sensitive data or properly protect it. Although there is some information on the security web site, there certainly needs to be a communication plan and an implementation plan shared with the user community. The IT Security Office continues to look at tools that might be used (in addition to what we have) and is available to work with areas to develop a plan for compliance.
- There are discussions about new technologies (for example, cloud computing) and there is a need to share information with users so they have some expectation on the impact it could have in their areas (good and bad impacts). It is also important to understand what might be potential security issues.
- The growth of data at all levels obviously brings concerns about sufficient backup. Will the new technologies help with that or does a department need to consider some type of offsite hosting?
- There is a need for the certificates issued by Virginia Tech to be recognized externally as many departments are still purchasing Thawte certificates to avoid having to instruct users to download the Virginia Tech certificate chain. Mary reported that there is funding and a plan to issue an RFP to invite vendors to propose solutions to externally sign the Virginia Tech Root certificate. The external signing will extend the trust of the Virginia Tech issued certificates outside the university. The external signing authority will be one that is automatically trusted by the most commonly used browsers.

Once these notes are approved by the sub-committee they will be shared with the VP for Information Technology and other appropriate areas within the IT organization.

Prepared: April 13, 2009