Security Sub-Committee Meeting
Notes – March 4, 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
Nicolas Pachis – IT Security Office

1. Introduction
    a. Brief history of the Security Sub-Committee
    b. Introduction of members (as there are three new members)
    c. Purpose of the Security Sub-Committee
    d. Organization of IT Security Office,
    e. Organization of SETI

2. 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.

Wayne Donald reviewed some of the activities of the IT Security Office and highlighted some areas that are a concern to management.

1. Security Reviews (a service provided by the IT Security Office)
    a. What they are: college/departmental scans for potential vulnerabilities, evaluations of computer and physical security, search for data disclosure issues
    b. Why do them: to ensure a secure environment, prepare for audits, potential or reported problems, special requests, compliance issues

2. Sensitive Information Initiative (as directed by VP's office and BOV)
    a. Discussed University Policy 7105 and associated procedures and standards
    b. Verification form/process sent by VP to certain individuals (very limited) was discussed at some detail
        i. Concern over March 2009 deadline/date – Wayne Donald indicated that will not be a reasonable date as there is a need for awareness from the top down to departments, and a better understanding of expectations

        ii. Concern over “ease of use” for average user, i.e. Find SSN or equivalent – may need more instructions on “basic” verification
        iii. The need for “easier” tools to be available to assist the user community
        iv. This sub-committee can comment and on the final verification form and the proposed process

3. Scanning Tools / Encryption Tools
    a. Identity Finder, Find_SSN
    b. Email Scanning – how available, good product?
    c. Rights Management System – Encryption and sensitive date monitoring

One reason for the Security Sub-Committee is to identity key areas where the institution might provide resources to help improve the environment at Virginia Tech, and help protect the user community from the many technology risks that exist. The initial list the sub-committee arrived at contained over 20 areas so some effort was used to place as many as possible in somewhat broader categories. The sub-committee decided on 5 categories with another category that can be listed to focus on new technologies and their impact on the security environment.

Categories – Areas of Security

1. Awareness / Education – one of the most important things for colleges/departments in this difficult budget time is to provide training for their technical support personnel. There was some discussion on how it's important to be able to identify those responsible for systems' security and that we currently lack a good identification process for those people now.

    - In response to the concern above, how might we identify those who need to know about policy, security, or recommended systems changes? Review the current listservs, mail lists, and other methods that are maintained to communicate support personnel
    - Look at feasibility of creating a technical portal or maybe a wiki that could be used to facilitate communications with technical support personnel

    - Technical training/education
        i. SANS Training / Certifications
        ii. A possible “internal VT certification” program
        iii. Basic training for new system administrators (with certification) – actually consider as part of their orientation
        iv. Central location (web) for information for administrators
    - Awareness for general user community
        i. A process is currently being implemented that would require all users to sign a verification statement to ensure they are secure and properly using sensitive data
        ii. Continue activities with faculty, staff, and students

    iii. Investigate new techniques that can be utilized by the ITSO to create awareness and assist users

  - Look at feasibility of creating a technical portal or maybe a wiki that could be used to facilitate communications with technical support personnel

2. Secure Enterprises – the type of “enterprises” one might consider in this area is administrative applications, research projects, instructional technologies, departmental systems and so on.
   - Ensure that existing policies/procedures are up-to-date and consider new ones that may be needed to provide direction
   - Incorporate requirements for secure systems into the university procurement process and ensure they are understood prior to a purchase -- for example, version updates, encryption, data handling, and so on
   - 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. Consider providing examples of assessments and recovery plans to give areas some guidance and assist in writing better plans
   - Conforming to standards – industry, State, and even federal

3. Access Security – part of the actually “secure enterprises” is to ensure who is accessing what and if that is the correct activity. Areas to be consider in looking at this are:
   - Perhaps a broad term for this area might be “identity management.” Managing user identities in a large, complex environment like Virginia Tech is very important in ensuring a secure environment
     - i. Review areas within the university that are involved in some aspect of identity management and determine how they might better work together
     - ii. The Identity Management Services (IMS) group within the IT organization has a mission to improve this area and needs to work cooperatively with other areas within the institution
   - 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
   - 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

4. Data Issues -- with an increased emphasis on data exposures and the use of sensitive data within an organization, there needs to be some guidelines and tools for users in doing their day-to-day business activities.
    - It is important that Virginia Tech have an up-to-date way to classify data that can help in defining ownership, sensitivity, access, and so on.
    - Confidentiality issues are something that needs to be understood by the data custodians as well as those that might be accessing (and using) the data
    - Data loss prevention (DLP) needs to be emphasized and can include a number of topics – (several mentioned earlier) for example, access “management”, encryption, data handling, data classification (which as define above is an area by itself), and so on
    - Procedures need to be in place as to what one needs to do when they experience a data exposure (especially if it involves sensitive data), and who takes the lead in ensuring all procedures are followed
    - Obviously there are compliance issues that are define below

5. Compliance Issues – a need to consider Virginia Tech specific, as well as state and federal compliance, and possible special needs (such as in the research areas). Some examples provided were:
    - Provide easier access for users to be able to determine what applies to whom, and how it applies – perhaps some type of cross reference for regulations
    - Review Virginia Tech policies/procedures/guidelines to determine how they are used and what might be obsolete or needs to be updated – what may need to be added
    - Ensure that procurement procedures at the university take into consideration the compliance issues and that some (if not all) responsibility is placed on the vendor
    - From above, understand what is sensitive, how it needs to be protected, and what assurance is required before moving forward with any planning, development, implementation, or use at Virginia Tech

Rather than list another category, the following area has been included as something that can be considered by this sub-committee for possible discussion. We see different/new technologies/directions being introduced into our environment on a frequent basis, and it is important to have some understanding of how they might impact individual units and if there is any specific requirement to prepare the user community.

- Technologies/Directions --
    - Cloud computing
    - Virtualization
    - Password resets
    - Data “growth” is making it increasingly difficult to provide sufficient backup
        - "Offsite hosting" - amazon, rackspace, etc. are becoming increasingly competitive so eventually so will departments have to tackle the question of continuing to keep data/systems local or moving them to a large service provider.