Minutes
Information Security Committee
Columbus State Community College

10/7/2013

Attendees: Robin Buser, Carol Thomas, Rob Clifford, David Wayne, Mary Reiter, Murray Holmes, Joe Gaines, Lori Thomas

Introductions were provided.

1. The purpose of the committee was reviewed. The procedure governing the committee work (Procedure No. 15-01 (M)) was reviewed and revised and the following change were suggested:
   - (1) Purpose of the Committee:

     The Information Security committee will also actively pursue audits of information systems and environments, and prove training and other educational activities to raise the campus community's awareness regarding protection of information and its resources.

     Change to:

     The Information Security committee will also be made aware of audits of information systems and environments, and will suggest training and other educational activities to raise the campus community's awareness regarding protection of information and its resources.

   - (2) The Information Security Committee Responsibilities
     The committee shall:

     (a) Investigate every security incident to ensure that policies, procedures, standards, practices, and other related topics or systems are updated or corrected to prevent repetitive incidents.

     Change to:

     (a) Review the investigation of every major security incident to ensure that policies, procedures, standards, and practices are updated or corrected to prevent repetitive incidents.

   - (4) Committee Meeting Frequency

     The committee shall meet twice a semester or more as needed to ensure all components of the Information Security Program are current.

     Change to:

     The committee shall meet once a semester or more as needed to ensure all components of the Information Security Program are current.

The procedure was written before there was a dedicated security department in IT. The committee no longer needs to be involved in audits or design training. The committee's current primary roles are to

review major incidents, to communicate to the wider college community, and to help with training the community in the importance of security awareness.

The proposed changes will be provided to the Technology Committee.

2. Current security status and prevention of attacks

- Rob Clifford reported that there are approximately 3 million attempts against our network per month. There have been no breaches in 5 years with only one virus outbreak.

- Student requests to unblock sites

  The college has extra security in place because of network printing. IT currently blocks over 400 sites, based on recommendations by MicroSoft, the FBI, and other companies as these web sites are known to contain and/or distribute malicious code. A site can be unblocked if there is a valid academic reason to unblock the site.

- Requests to restrict access to adult content

  Access to adult content is restricted by security software through the network. Some adult content needs to be available for valid academic reasons. Adult content includes sites that are considered pornographic and downloading pirated video or songs through the college network.

  One solution is to minimize the amount of network bandwidth used by such sites, make them available but extremely slow to load.

  If the site needs to be accessed for valid academic reasons, the appropriate faculty administrator can make a request to IT, and access to the requested site will be allowed for a particular user. This process is currently in place but there have been no requests. There is a need to communicate this process to the faculty.

3. Audit findings and recommendations

- Spring audit

  An audit of security was completed this past Spring as part of the financial audit. The audit included a review of project management documentation and of new systems.

  The college maintains a private network, and there is a cost associated with that maintenance.

4. Current issues

- Vulnerability – There is open access to wire ports without authentication. Technology exists to eliminate this vulnerability, but is intrusive to users, as it forces them to accept an agent on their laptops. The committee asked IT to investigate software requirements to see if the fix could be placed on student or administrative networks. If implementation occurs, communication to the users will be needed.

  IT proposed to the committee that we recommend:

  1. Single sign on for all CSCC computers
  2. A personal devise to install agents

Comment [RAC1]: This can come out as it's not related to the blocking of malicious web sites.

Comment [RAC2]: Added

The committee is considering this recommendation and asked Mary Reiter to discuss with the Technology Committee.

5. Next meeting

- The next meeting will be schedule in January 2014.
- Points of discussion:

  -- Expiration of student accounts after inactivity and how to return the accounts from being expired.

  -- Revisit recommendation for single sign on