

Council on Libraries and Information Technology  
November 16, 2007

Minutes

Present: Daniel Avorgbedor, Karen Bruns, Fritz Graf, Mike Hemmelgarn, Meri Meredith, Kenneth Pearlman, Greg Smith, Les Tannenbaum, Mike Veres

Absent: Theodore Bauer, Joseph Branin, Roy Joshua, Kathleen Wallace

Guests: Cathy Bindewald, Celeste Feather, Bob Kalal, Charles Morrow-Jones, Eric Schnell, Chris Zacher

Topic: Cybersecurity

Charles Morrow-Jones repeated a presentation given to the University Senate on November 8 on the topic of “What You Should Know About Cybersecurity.” He first gave a chronology of data breaches in higher education and stated that the OSU experience generally compares to the national profile.

OSU has had one hacking situation, but mostly thefts of portable devices. There are three categories of OSU data – public, limited access, and restricted (can be used for identity theft, often constrained by law). The relevant legislation is FERPA and the Ohio Revised Code 1347, or Ohio House Bill 104. Ohio law requires notification of individuals whose information has been exposed. If the names of individuals cannot be pinned down, then a broad OSU web site notification is necessary.

The OSU Policy on Institutional Data for Restricted Data states that data must be encrypted if on a portable device, removed from university property, or electronically transmitted (including email). Restricted data sent to an outside contractor must be handled under the same restrictions that OSU maintains (such as the company that handles OSU W-2 tax forms). Restricted data cannot be placed on personal equipment. Known or suspected disclosures must be reported immediately.

Standards define requirements that protect the devices and networks. Policies control how restricted data are handled. One suggested workaround is to provide employees with university-owned encrypted thumb drives on which to store restricted data. OSU has a Minimum Computer Security Standard posted on the OIT web site.

Discussion after the presentation focused on the following concerns:

1. Educate community about limits on the use of personal devices for university business.

2. How do we disseminate this information successfully?
3. Financial concerns at \$25 per identity stolen
4. University reputation
5. Increase educational sessions about physical laptop security; need more classes to be held at the Digital Union

The OIT Security group is available for personal presentations, interested in providing additional educational opportunities.

A student representative suggested that an expansion of storage limits on email accounts might encourage students to stay with OSU email. Committee members can help by spreading the word personally, and make sure that the monthly security reports from the Colleges surface and receive attention. Individuals should consider personal identity theft protection, and perhaps academic insurance. If members hear misinformation, please raise the issue and let OIT know.