The Implementation of Higher Education Web Classes; Technological Issues, Concerns and Potential Problems

by Jerry Plummer, Vicky Langston and Tommy Meadows
Austin Peay State University

What Exactly *Are* Higher education Web Classes?

In higher education, Internet based course offerings are a hot current topic. What are these classes, and what do they mean to higher education?

Much like e-commerce, web-based learning involves the Internet and interactiveness between the web site and the student (consumer). The professor often places the lessons and usually tests on the selected web site for students. Group discussions are usually allowed between students and the professor, much like chat rooms. This interactiveness allows for a more realistic, class-like environment. As in e-commerce (where customer order requests are logged into the database for further processing), requests or responses from the student are logged into the class database for grading, interpretation, or professor response.

Web-based higher education classes are expanding in number, although to a lesser degree than e-commerce from the private (for-profit) sector, probably due to lack of profit motive on the part of higher education. Drexel University, for example, recently announced the first 'Techo-MBA' program where all classes are taught online.[1] Several major universities are considering offering Internet degrees, and many universities and colleges are experimenting with offering selected types of courses currently.

What are (if any) areas of concern for higher education in this burgeoning 'market'? Is everything an opportunity, or should we continuously look at this new 'gift' of technology prior to becoming involved? What items are of concern to higher education, and what are the possible outcomes, both positive and negative?

This paper will explore areas of potential concern to higher education in the arena of Internet based course offerings from a technological standpoint, and attempt to offer a basic set of conclusions that will require further research.

Technological Areas of Concern

From a computer hardware standpoint, it is clear that security measures must be present in order to reduce the possibility of hacking or intruder intervention to the course. These intruders, or 'hackers', in essence, spend time 'surfing' on the Web attempting (often successfully) to enter a site and its server (the computer housing the site data-in this case, for the proposed higher education course offering) for a variety of purposes.

One such group, Defcon,[2] is known internationally for successful endeavors of this nature, mostly on e-commerce sites as well as government sites. Many remember when President Clinton's site was hacked to send Internet visitors to a well known pornographic site, rather than the President's actual site. Another hacker group, Cult of the Dead Cow,[3] has members that are suspected of hacking the D.A.R.E. site, as well as Amazon.com and/or E-Bay. There are many 'shadow groups' of hackers worldwide who successfully enter sites without anyone knowing. Accurate data on the number of hacked sites does not exist currently.

Interestingly, many hackers are late high school to early college age--a fact that should not be missed in the academic community regarding existent and/or proposed Web courses. The hackers are generally not interested in damage, simply that they can 'get in and out', although there are hackers who write code for viruses with the intent of causing damage to the server contents. Recent viruses that attack email comes to mind. It can be seen that the hacker interests could also involve acquisition of test data, test grades, and passing university classes.

Unfortunately, many universities are ill-equipped to combat hackers or intruders of a similar nature. Most large

---

[1] Nashville Tennessean, February 10, 2000; 'Online MBA Program Offered.'

[2] Nashville Tennessean, March 12, 2000, 'What's In A Name.'

[3] Nashville Tenness,2000, Ibid.

e-commerce firms, such as E-Bay,[4] employ several high-paid technicians simply to monitor and reroute attempted intrusions. Many universities simply do not have the required funds available for this purpose. This leads to the implementation of hardware services, such as 'firewalls'[5]--to try to close the door to the site/server from intruder attacks, or hacking.

So, the next concern, from a hardware standpoint as well as course content, relates to the 'housing' of the database for the class. A good Web class is dynamic, or interactive, allowing for the student to access the class information from the site, as well as return data to the site. This includes tests for the class, since essay testing is not applicable for classes. The interactive database must be fully protected in order to reduce or dismiss any possibility of the test answers (for example) being accessed by the student.

Most of the available Web classes are packaged and sold by firms like Blackboard,[6] WebCT[7] , Ecollege[8] or UniversityAccess[9]. These are 'canned' packages, allowing for some modification by the professor, but still (generally speaking) pre-built to an existing 'standard', traditionally developed concurrently by the Course Manufacturer along with an established member of the academic community. This is similar in some ways to the selection of a particular text for a course, but the text can be added to at will. Modification of some of these canned programs is tenuous, and tends to limit the professor's freedom in class topics and usage.

Course manufacturers are (generally speaking) not members of higher education, but for-profit members of the private sector. Clearly, the opportunity for profits is tremendous, and in a competitively arrayed market system profit becomes the primary motive. The implications to higher education here are obvious and should not be swept aside in the euphoria to join the groundswell for Internet courses.

Potential Solutions and Questions

One recent approach to 'fixing' the above hardware issues or concerns has been by the course manufacturers (Blackboard, WebCT, eCollege or UniversityAccess, for example) to maintain the course on *its* server and proxy the course to students by the distribution of passwords to students, thereby reducing the universities liabilities from a hardware protection standpoint. Professor involvement is by the same means of passwords, both for course modification and student progress analysis.

The university is (possibly; theoretically) absolved of all computer-related issues, since the manufacturer maintains the entire site on its own server for all courses and all members of higher education using the courses. (This would be transparent to the students, who would still access their higher education site, and then be transported via an 'alias' to the manufacturer site.)

As with many things in life, the simple answer often provides a new group of questions. Questions now arising include the following:

* who is the 'school', the manufacturer or the university?
* who is responsible if the site is hacked?
* what does the university do about grades if the test data is 'out there'?
* what happens if the professor wants to change course content beyond the scope of the manufacturer's desires?

---

[4] Nashville Tennessean, February 11, 2000, 'Web Sites Race To Bolster Defenses.'

[5] Http://www.zeuros.co.uk/firewall

[6] http://www.blackboard.com

[7] http://www.realeducation.com

[8] http://www.webct.com

[9] Http://www.universityaccess.com

* does the university receive any renumeration for course modifications or enhancements?

* does the university stand a chance of losing its individuality if it uses canned manufacturer courses

* are there market 'niches' for Universities, and what is to stop smaller schools from losing enrollment to larger 'name' schools?

Although it is true that answering any or all of these questions is beyond the scope of this paper and is a topic for further research, we can still arrive at three general conclusions:

(1) The area of ownership of the course should be closely inspected by higher education prior to any type of binding commitment.

(2) The placement of the course from a hardware standpoint relates to two major areas:

(a) Security considerations must be a top requirement

(b) Higher education should require full access to the site, wherever it is placed, and retain the ability to change or modify the class in accordance with university or professor requests.

(3) Higher education must retain its own individuality in the course content, rather than have a generation of 'cookie-cutter' degrees, based on Course Manufacturer's (potential) desire to increase profits due to the synergistic concept of developing one course and having it used by all universities and colleges.

These three points and sub-points all appear to be candidates for 'major risk' to higher education if not clearly considered prior to course acceptance and implementation or with any type of agreement with course manufacturers.

Closing Remarks

In the area of combining higher education courses with the new technology of the Internet, it is clearly true that tremendous potential is evident and that higher education should become involved. However, as with many 'new' things, one should consider both the positive and the negative prior to implementation of the course to the Internet.

This paper is *not* written to attempt to state that the Internet class offerings should not be considered, nor to state that higher education and course manufacturers should not consider a partnership. Possible synergy is clearly possible and certainly should be pursued by members of the higher education community.

The paper simply states that there are possible negative connotations that could be involved, and prior to implementation, all areas should be considered in order to ensure that the learning process is cognitive and in line with existent higher education standards and procedures. Further research will be done by the authors in these areas to delineate further areas of opportunities and concerns.