UNIVERSITY OF MARYLAND AT COLLEGE PARK
DEPARTMENT OF PSYCHOLOGY
College Park, Maryland 20742-4411
(301) 405-5924

June 12, 2014

To:

Dr. Wallace D. Loh, President of the University of Maryland;
Dr. Mary Ann Rankin, Senior Vice President and Provost;
Dr. Ben Bederson, Associate Provost SVPAAP-Sr VP Academic Affairs;
Dr. John R. Townshend, Dean of BSOS;
Dr. Jack Blanchard, Chair of Psychology;
Dr. Ann Wylie, Special Assistant to the President IT-Information Technology;
Mr. Gerry Sneeringer, IT Security Officer;
Mr. Dan Navarro, Director BSOS-Dean-Office of Academic Computing Services;
Dr. Jonathan Katz, Professor of Computer Science;
Mr. Robert Maxwell, Manager IT-Security & Policy; and
The Faculty Senate:

From:

Dr. Kent L. Norman, Associate Professor, Department of Psychology, Affiliate of the College of Information Studies, and the Human-Computer Interaction Lab

I am writing this letter as an official complaint against the actions of Dr. Jonathan Katz, professor and director of the CMNS-Institute for Advanced Computer Studies, Mr. Robert Maxwell, Manager of IT-Security & Policy, and an unnamed undergraduate enrolled in CMSC 498N: Cybersecurity: Secure Maryland, during the Spring 2014 semester.

I received an email (Exhibit 1) from my Department Chair, Jack Blanchard on May 7, 2014, informing me: “Given the Maryland data breach, [the] campus is assessing various websites for vulnerabilities. As noted below and in the attached report, the web application that you use of PSYC445 is problematic. As Dan Navarro indicates below,

you will need to stop using the HyperCourseware application as soon as possible and move to Canvas."

Upon reading the attached report (Exhibit 2), I found that it originated from an undergraduate project in CMSC 498N, dated April 7, 2014.

To be honest, I was shocked and appalled! I was shocked that it took a full month to notify me and appalled that an undergraduate student had cyber-attacked my server (cognitron.umd.edu) and published sensitive student grade information. These are two clear violations of the University of Maryland Policy on the Acceptable Use of Information Technology Resources (Exhibit 3). (http://www.it.umd.edu/security/Nethics/Policy/aup.html).

In response, I sent an email dated May 12th (Exhibit 4) to the Chair of my Department and cc'd to Wayne McIntosh, the Dean of BSOS, Dan Navarro, Ann Wylie, UMB CIO, Gerry Sneeringer, and Ben Bederson. In this email, I expressed my outrage at having my server attacked and student information copied. My initial suspicion was that it was one of the current computer science students enrolled in Psyc 444: Cyberpsychology, the course attacked, and also enrolled for the Fall 2014 Semester in Psyc 445: The Psychology of Video Games, mentioned in the report. Finally, I briefly explained my rationale for using HyperCourseware™ and reasons for not moving to Canvas.

As suggested, I met with my Chair, Jack Blanchard on May 9th, and briefly discussed the "Vulnerability Report" and my position regarding it. We decided that it would be good to meet with Dan Navarro and others to discuss the situation.

During the weekend, I removed all web pages on cognitron.umd.edu that gave login instructions for my courses and changed the passwords from 4-digit to 12 alphanumeric characters. I emailed my 36 students and teaching assistant about the breach and much to their consternation, sent them each the new password.

On May 14th, I met with Mr. Dan Navarro, Dr. Wayne McIntosh, Dr. Jack Blanchard, Mr. Gerry Sneeringer, Mr. Robert Maxwell, and Dr. Johnathan Katz (via speakerphone). Exhibit 5 is my proposed agenda for the meeting.

To begin the meeting, I gave a brief background of HyperCourseware; how it was conceived during my sabbatical at the University of Cambridge, England, in 1990 and how it was based on principles of hypermedia and educational metaphors (See Exhibit 6 for a 1994 article on the principles of HyperCourseware). It was originally implemented in the AT&T Teaching Theater using stackware on the LAN and then transitioned to the Web in 1996 using a WebStar™ server at the domain cognitron.umd.edu and is currently on an Apple OS-X server. HyperCourseware is a complete electronic educational environment with a hyperlinked syllabus, notes, readings, discussions, polling, quizzes, exams, grades, project spaces, and a wiki. Evolving of over the years, it will celebrate its 25th anniversary next year.

We then learned from Mr. Maxwell that students in CMSC 498N had routinely assessed the vulnerability of websites at umd.edu, with the exception of Testudo and ARES, but

that prior to an actual attack, owners of the websites were informed and gave permission for the attack to proceed. Robert Maxwell, assured the committee that they had had no problems prior to this one and that all sensitive materials that were downloaded were encrypted.

I was not told what other sites were assessed and attacked or why I was not informed prior to the attack of my site. I was not told why the report was sent to Dr. Ann Wylie and not directly to me. Nor was I told why the "Vulnerability Report" with confidential student information was made public. The document, Exhibit 2, has no watermark that indicates that it is private and confidential. We were not shown the course syllabus or the specifics of the vulnerability assignment. However, we did find out that the students were not FERPA certified.

I was assured from Gerry Sneeringer that the student I had suspected was not enrolled in CMSC 498N. He also assured me that none of the other Computer Science majors this semester (Spring 2014) and Fall 2013 were in my classes. Unfortunately, this does not preclude Computer Science friends and classmates.

Finally, I reiterated my feeling that I had been personally attacked and that rather than shore up the security of cognitron.umd.edu, I was being bullied into decommissioning HyperCourseware and shifting to ELMS (Canvas). I noted that the majority of Computer Science faculty do not use Canvas and that a number of faculty have serious complaints about Canvas. Moreover, there is no assurance that in a few years Canvas will not be replaced by yet another ELMS. The history of ELMS on campus reveals about a six year life expectancy (WebCT 1999, Blackboard 2006, Canvas 2012); whereas, I have consistently used HyperCourseware for almost 25 years.

Gerry Sneeringer offered to provide a more technical evaluation of the security of cognitron.umd.edu and I agreed to that offer; however, I would think that University resources might be better spent on higher profile targets than mine.

Ultimately, nothing was really resolved at the meeting. I am not aware of any actions taken to change the situation and to protect the faculty and students against such attacks in the future. All I know is that I had a class of very irritated students following the breach and the remedial measures that I had to take to further protect their information. I have not traced the student involved from the login information (Exhibit 7), but Mr. Sneeringer knows who he or she is.

In principle, I view this attack as no different than a thug hacking the 4-digit security pin for my office alarm, entering my office, pilfering through my file cabinets looking for student grades, copying one student's grades, and showing them to his gang leader and fellow gang members to prove that he had done it. Then when the authorities find out about it, rather than recommend that I increase the security of my office, they want to move me to a new building!

While I can appreciate efforts to make Maryland secure in light of major cyber security breaches earlier this year, in my case, I feel more insecure in light of the methods being used in CMSC 498N, namely, entrusting it to undergraduate students with no credentials

rather to professional contractors. Moreover, completion of the assignment by students in the class requires them to violate the University of Maryland Policy on the Acceptable Use of Information Technology Resources and FERPA.

Thank you for your consideration of this matter. I hope that the University will take the appropriate steps to hold those individuals involved accountable for their actions, and to prevent such attacks from happening in the future. I have lost valuable research time cleaning up the mess created by this class assignment and the student who completed it. While the identity of the computer science student is being protected, I feel unprotected and threatened by future attacks by faculty and students within the University.

Knowing that the faculty perpetrator of this attack, namely, Dr. Katz is also the current director of the Maryland Cybersecurity Center calls into question the ethics and the practices of the Center.

The University of Maryland has always supported and encouraged innovation in teaching and learning. A large part of this involves the use of computer and Web technology. HyperCourseware is my platform for research and teaching, exploring new ways to interact with the students and the materials, constantly changing and experimenting with new ideas and feedback from the students each semester. Consequently, I hope that the University will continue to support innovative teaching technologies at the University of Maryland rather than attempting to decommission them.