UMD Data Breach Update

February 25, 2014

Dear University of Maryland community:

Today marks one week since the date our University suffered a sophisticated cyber-attack. Again, I apologize to each and every one of you for this data breach. I want to update you on what we are doing to protect -- as best as we possibly can -- the personal, research, and financial data you have entrusted to us.

State and federal law enforcement agencies, the U.S. Secret Service, consultants from the MITRE Corporation, and our own campus IT security personnel are working together to find out how the attackers penetrated our multiple layers of security. This forensic analysis will enable us to defend against this type of attack in the future. It will also provide clues as to who were the attackers.

I have ordered an extension of credit protection services from one year to a full five years of coverage. This extended protection will be available at no cost to every person affected by this breach. To register, please call Experian at 1-866-274-3891. If you have already signed-up for the initial one-year protection, you will be automatically upgraded to five years so you do not need to call again. Please note that call volume may be high, and we appreciate your patience. All coverage is retroactive to the date of the breach.

Effective immediately, I am launching a comprehensive, top-to-bottom investigation of all computing and information systems. This includes central systems operated by the University and local systems operated by individual administrative and academic units. This investigation has three missions.

First, we will scan every database to find out where sensitive personal information might be located. Then, we will either purge it or protect it more fully in that database, as appropriate. There are thousands of databases throughout the campus, many created years ago when the environment for cyber threats was different.

Second, we will do penetration tests of the security defenses of our central and local information systems to identify and seal any possible technological gaps through which cyber criminals could get in to search for any information. These probes will be performed on an ongoing basis.

Third, we will review the appropriate balance between centralized (University-operated) versus decentralized (unit-operated) IT systems. There must be policy changes to accompany technical fixes. We understand the needs of individual units to control their own servers and databases. We must also ensure that safeguards at central and local levels are equally robust and tightly coordinated. Our University’s entire cybersecurity system is only as strong as its weakest link.

To execute this threefold mission, I am forming the President’s Task Force on Cybersecurity. It will be led by Professor Ann Wylie, who formerly held the positions of Provost, Vice President for Administration, and Chief of Staff to the President.
The Task Force will have experts from our campus, including from our Maryland Cybersecurity Center. They will be supported by a leading cybersecurity company with advanced hacking capabilities in order to expose potential vulnerabilities in our systems.

I have charged the Task Force to complete its investigation and submit its recommendations to me within 90 days. It will have the full support of my office and the resources it needs to complete its task. I will take all necessary actions based on the Task Force's recommendations and the results of the forensic analysis now underway.

Professor Wylie will also serve as interim Vice President for Information Technology, effective March 1. Our current vice president, Brian Voss, previously announced his retirement as of March 31. They will work together for a seamless transition. A national search for a permanent Vice President and Chief Information Officer is underway.

There is no impregnable barrier against every fiendishly skillful cyber-attack. Every day, there are thousands of probes of our defenses that we spot and thwart. We are not alone. In the past couple of years, some 20 large universities across the country have also reported major data breaches.

There is an arms race between hackers playing offense and universities playing defense. In 2012, we doubled our IT security staff and doubled our annual investments in cybersecurity. We will continue to make the necessary investments.

In today's digital world, each of us must take reasonable steps to ensure our own information security. Therefore, the University will present a series of identity theft seminars to all our students, faculty, staff, and alumni. The seminars -- which will also be recorded and later made available online -- will feature experts on how to safeguard your sensitive information.

Additional updates will be posted on www.umd.edu/datasecurity.

Because of the actions we are taking, I pledge to you that the University of Maryland will be even stronger, bigger, and better in the unremitting and global fight against cyber-crime.

Sincerely,

Wallace D. Loh
President, University of Maryland