Cybersecurity is a growing concern at the state level, and cybersecurity breaches are costing state governments large sums of unbudgeted money to fix and accommodate.

Like many who file state income tax returns electronically, I received official notice on December 22 from a state government that my Social Security number, tax identification number, payment information, bank accounts, and credit cards may have been exposed due to a security breach that took place three months earlier and was not discovered until a month afterward. In this particular case, which involves the state’s department of revenue, the potential breach of stored information goes back more than 10 years and involves millions of state income tax filers—both businesses and individuals.

In addition to hiring outside forensic experts, putting new policies and procedures into practice, and installing new technology, this state government is paying an outside security firm for one year of credit monitoring and fraud resolution services for each tax payer who may have been violated (and who chooses to register for the offered services). This is just one example from our increasingly cyber-connected world, but it serves to illustrate how cybersecurity has become a new problem for individuals and businesses to worry about and for state governments to deal with on a comprehensive, cross-functional, statewide basis.

The National Association of State Chief Information Officers (NASCIO) continues to identify cybersecurity as a critical concern for state governments. The recently released “2012 Deloitte-NASCIO Cybersecurity Study” notes that cybersecurity does not fail gracefully. CIOs and chief information security officers (CISOs) must worry that if they don’t get security right and systems are breached, the state’s cybersecurity program may be perceived as ineffective and the state’s citizens may suffer direct harm.

Cybersecurity threats to state government—like threats to all sectors—are growing in sophistication and frequency. A new breed of cybercriminal and hacktivist is emerging with a narrowed focus on monetary gain or on making political statements. According to a recent Rapid7 report on the “Data Breaches in the Government Sector,” government agencies have lost more than 94 million citizen records since 2009. Remarkably, the average cost per lost or breached record is $194, according to the Ponemon Institute’s 2011 Cost of Data Breach Study.

From the Deloitte-NASCIO Study, 92 percent of state officials feel that cybersecurity is very important for the state, yet only 24 percent of CISOs are very confident that they can protect state assets against external threats. Further, 70 percent of state CISOs have reported a breach, but only 32 percent feel that their staff has the required cybersecurity competency. Most noteworthy is that the increasing need for cybersecurity education and training is repeatedly identified in all sectors of government, business, and society.

Within state government, security breaches may be far more costly than cybersecurity programs, especially when considering the cost of regaining lost citizen trust. At the heart of an effective state cybersecurity program are properly educated and trained cybersecurity professionals. I am pleased that UMUC continues to work to meet this need through its cybersecurity degree programs and by producing trained cybersecurity professionals to meet growing workforce demands.