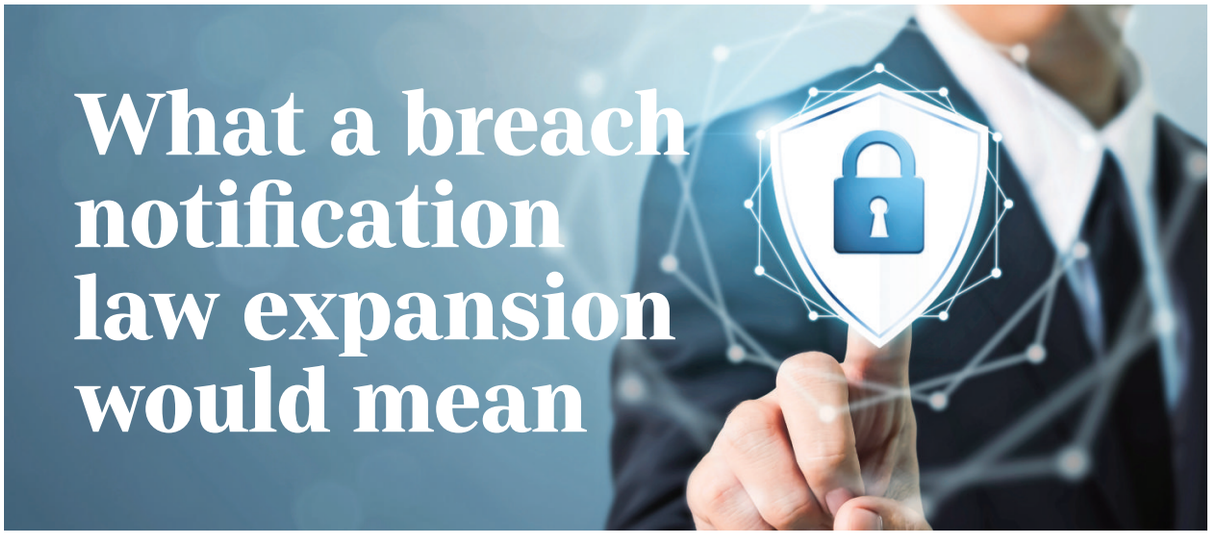
Eliza Scott
escott@wmbac.com

What a breach notification law expansion would mean



GETTY IMAGES/ISTOCKPHOTO

The Tennessee legislature is considering a bill that would update the Tennessee Identity Theft Deterrence Act of 1999 (the "Act"), which functions as Tennessee's breach notification law. The basic structure of the breach notification provisions remains the same. Information holders are required to notify Tennessee residents whose Personal Information has been acquired by an unauthorized party. As defined in the proposed bill, an information holder is a person who owns, licenses, or maintains the computerized Personal Information of a Tennessee resident.

Other updates include:

- Expansion of the definition of Personal Information;
- A requirement that information holders implement and maintain, what is in essence, a reasonable computer security policy;
- A requirement that information holders cooperate with owners and licensees in the event of a breach;
- A reduction in the number of affected Tennessee residents needed to trigger notification of the Attorney General from 1000 to 500;
- A requirement that information holders give notice of compromised email account credentials via alternate means; and
- Clarification regarding the timing of notification.

Personal Information is currently defined as first name or first initial and last name in combination with social security number, driver license number or certain financial account information. The new definition of Personal Information would include the following information types, simplified for the sake of brevity: government issued identification numbers, passport number, email account login credentials, medical information, health insurance information and biometric data.

The original bill proposed removal of the safe harbor for information holders who are subject to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and included express provision for civil actions against information holders who violate the statute. These two changes are notably absent in the recent senate version. It is striking that Tennessee would propose such a removal, perhaps indicating the potential for greater involvement in cyber/information privacy law at the state level.

However, what excites me most as a former computer security professional is the proposed requirement that information holders have, what is in essence a computer security policy. This is referenced in the bill as "reasonable procedures and practices ... to prevent unauthorized acquisition, use, modification, disclosure, or destruction of personal information." Such a requirement would serve as a signal to information holders that it is time to get serious about technical and legal risk assessments and protective measures.

To my mind, the implementation of a state-level requirement that information holders must have a computer security policy would also signal Tennessee's irreversible passage toward the creation of a healthy body of state-level cyber/information privacy law. Such body of law would be a long-awaited and much anticipated acknowledgement of our current reality, namely, that we live our lives not only in the physical world, but also in the cyber world.

C. Eliza Scott is a former computer programmer and security professional, licensed to practice law in Tennessee. She is currently employed with Woolf, McClane, Bright, Allen & Carpenter, PLLC. This column is provided through the Knoxville Bar Association, your trusted source for lawyer referrals. The KBA is a nonprofit corporation that offers community service programs such as the Lawyer Referral & Information Service, speakers' bureau and public education programs.