laws requiring businesses to comply with specific security requirements, including encryption of personal information. The most notable states with regard to this new trend are Massachusetts and Nevada, both of which legally mandate some form of encryption with respect to personal information.

The Massachusetts law, which went into effect on May 1, 2009, states that all businesses that collect, store, or transmit personal data about Massachusetts residents must adopt a comprehensive written security program, conduct internal and external security reviews, and implement employee training programs. The regulations set out a checklist of minimum requirements for the security program and minimum technical requirements for computer systems that electronically store or transmit personal information. Further, they require businesses, to the extent technically reasonable, to encrypt records and files containing personal information that will travel across public networks or to be transmitted wirelessly. Encryption of personal information stored on laptops and other portable devices is all required.

The Nevada legislation that went into effect on October 8, 2008 mandates that “a business in this State shall not transfer any personal information of a customer through an electronic transmission other than facsimile to a person outside of the secure system of the business unless the business uses encryption to ensure the security of electronic transmission.” (Nev. Rev. Stat. 597.970)
Each of these states take a different approach to defining the geographic scope of these encryption laws. In general, the Massachusetts law is based on the residency of the individual associated with the personal information; the physical presence of the business or extent of business activities within the state does not matter. Nevada, however, focuses on where the organization is doing business, and therefore applies to any entity “doing business in the state.” The two laws also differ on when and where personal information must be encrypted.

Generally speaking, Nevada requires encryption while the personal information is in transmission outside of the secure system, while Massachusetts mandates encryption both during transmission (including wireless) and while stored on laptops and other portable devices.

While a handful of other states also have specific encryption requirements for certain types of information, such as social security numbers, there are many others that more generally dictate a “proactive” yet “reasonable” approach to implementing procedures and practices to secure data. These include Connecticut, California, Texas, and Rhode Island. Some others – for example Minnesota and Washington – have data security laws that, in addition to breach notice or establishing minimum standards for security, also impose legal liabilities to third parties, such as card issuing banks, who may incur costs arising out of a data breach.

As time marches on, we will see the enactment of more and more legislation (both state and federal) that is in favor of the consumer and against the entities handling their personal information. Whether we refer to these laws as “proactive,” “reactive,” or in some way “punitive,” they all pose significant compliance challenges to organizations. These challenges arise out of ambiguity in language, lack of uniformity between them, as well as coordination with third parties with whom such personal information is shared or exchanged in the course of doing business.

As with other legal compliance issues surrounding information security, organizations of all sizes must engage representatives from legal, IT, and risk management to form teams that will work collectively to analyze requirements, establish business policies and processes including infrastructure, and regularly review plans and implementations as the technology and legal environments continue to evolve. An enterprise risk management approach to data security and privacy is essential, and should also include network security and privacy insurance coverage to mitigate costs associated with data breaches when, not if, they happen.

* * * * *

“*You cannot prevent the birds of sorrow from flying over your head, but you can prevent them from building a nest in your hair.*”

– Chinese proverb

For more information, contact Helen Richards, 800-528-7730 • helen.richards@wellsfargo.com