CARSON CITY, NEVADA, May 29th, 2009 - In the 2009 Session of the Nevada Legislature, a landmark bill (SB 227) was passed which affects the way electronic data is transmitted and stored. SB 227 will replace the current Nevada Encryption Law, NRS 597.970. This report will provide an overview of the law, and how to apply it.

The Nevada Data Encryption Law creates a payoff for good data security practices. The law grants a shield from litigation, when basic data security standards have been met or exceeded by businesses, government agencies and other entities. The state of Nevada has acknowledged a set of “best practices” for protecting Personally Identifiable Information, when that information is being transmitted over the internet. The standards also apply to data on devices like small “thumb drives,” portable hard drives, CDs, DVDs, Smartphones, iPods, and other devices that can transport data.

What some examples of security standards will offer me protection from litigation?
  • Payment Card Industry Digital Security Standard (“PCI”)
  • Encryption, and the proper storage of encryption keys, as approved by The National Institute for Standards and Technology (“NIST”).

What kinds of data are subject to the standards?
  • Credit Card Data
  • Bank Account or ATM Account Information
  • Social Security Numbers
  • Driver's License Numbers

Who is affected by this law?
  • Any entity, private or public, that collects, stores, or moves Personally Identifiable Information (“PII”)
  • Entities that accept credit cards
Entities that collect store or move other PII. Examples typically include payroll data, health insurance data, workers comp data, car or equipment rental data, gaming properties, pawn shop and payday loan data, and other entities.

Every business that collects credit card data is already mandated to follow good data security through PCI. Full compliance with PCI can provide businesses and government agencies safe harbor if their only PII is credit card data. Information about PCI compliance can be found at http://pcisecuritycouncil.org.

What questions should we be asking?
- Do we have data flow diagrams that map out where our PII is?
- Do we have systems in place to detect and encrypt PII?
- Do employees have unmonitored access to social networks like Facebook, Twitter, LinkedIn, MySpace, Gmail, Yahoo Chat, web chat, etc.?
- Do we have systems in place to automatically encrypt PII if it goes out via email, the web, chat, social networks, or via thumb drives? For example: Does the human resources have access to email, the web, and thumb drives on the same network that has access to payroll and health insurance data?

This doesn’t have to be difficult
Many organizations that consider themselves “safe” have systems that were not built with this level of security in mind. In many cases, taking existing secure systems and adding the ability to determine when PII data moves, and encrypting that data when it moves onto removable media, or online, will shield a business from liability under the statute.

Fortunately, there is software that can be deployed to automate the processes. Some of this software is very low cost or free. The key is to have knowledgeable assistance in making sure these tools are deployed correctly so the PII is properly protected.

The information provided here is an overview only of the new law. With so many data threats, and with the alarming rise in identity theft, every business and government agency in Nevada must assess their own data, the risks associated with a breach, and take appropriate action to mitigate risk. This new law provides a “carrot and stick” approach to data security and privacy, and gives the flexibility to allow decision makers to get the balance right.

About the Author: Ira Victor is a partner at Data Clone Labs, Nevada’s data security and digital forensics firm. He is a noted speaker, certified specialist on data security and compliance, and expert witness in civil and criminal matters before the courts. Ira Victor is President of InfraGard Sierra Nevada. InfraGard is a program of the FBI to facilitate information between the private sector and law enforcement to protect the Nation’s Critical Infrastructure. InfraGard has nearly 25,000 members nation-wide. You can find Ira’s contact info at IraVictor.net (not .com).

Copyright 2009, PTI