GLOBAL LEGISLATION

The biggest concern about data security today is the lack of uniform legislation

WinEncrypt

GLOBAL LEGISLATION: CURRENT REGULATIONS ABOUT DATA SECURITY AROUND THE WORLD

The biggest concern about data security today is the lack of uniform legislation not only across the world but between the various states in the US. With more and more people choosing to conduct business online, online stores mushrooming across the world and information being exchanged every second of each day over the internet, the safety of data posted on any website is at the mercy of steps voluntarily taken by that site to ensure data security. Identity thefts are not only common, they are rampant. And data breaches are not limited to credit card information, data theft occurs at the websites of banks, schools, businesses, government agencies, hospital and health care organizations, online retail stores, etc.

Before talking about data security, it is important to understand that all large organizations, corporations and institutions are always in the process of gathering data. According to a survey of 47 countries conducted in 2007 by Privacy International and the Electronic Privacy Information Center, the United States ranks the lowest in data privacy and is the worst "endemic surveillance society." What is even worse is that data is not only collected for an organization's own use, information is swapped between organizations for their mutual benefit. But before we blame a particular organization, remember that businesses are also victims of hacking and data breaches.

One of the worst data breaches occurred in January 2007. Massachusetts-based TJX Companies found that its database had been hacked into and information stolen. The problem was that the security breaches had occurred between 2003 and the end of 2006, but the repeated break-ins were only discovered in 2007. The fact is that retailers continue to gather vast amounts of sensitive consumer data without any legal regulations being put in place to hold them accountable for the privacy and security of the data. What makes cyber crime easy is that most companies are unaware of how and where all this data is stored. This means that once data theft has occurred, the company might not discover the breach till it needs to access that specific bit of data.

But why should a company spend thousands of dollars ensuring data security when such expense is neither required by law nor enhances its business in any way? So, unless websites are held legally responsible for the data they collect, there is little incentive, apart from their own conscience, to invest in software and personnel to monitor the safety of information collected online.

Another area that has seen data breaches is the outsourced business segment. Outsourcing companies maintain both personal and transaction data, both of which are sensitive in nature. These companies, then, become prime victims of identity theft because transaction data usually includes credit card details, social security numbers and various other personal details. Inadequate security measures, poor data encryption or ineffectual monitoring of data sharing with partner companies and third parties can leave the data vulnerable to theft.

All this does not mean, however, that the United States is completely ignoring the problem of data security. Although there is no federal legislation in place, the finance and health sectors have put forth laws to protect data, as has the state of California.

1. **California legislation SB-1386 of 2002** requires any agency, business or individual that conducts business in the state and owns or licenses any form of "personal information" to disclose any breach of security to the resident of California whose unencrypted personal data is believed to have been breached. The bill mandates various measures and procedures with respect to data security, subject to other defined provisions.

2. **The Gramm-Leach-Bliley Financial Modernization Act of 1999** has put in place three privacy requirements – the Financial Privacy Rule, Safeguards Rule and pretexting provisions. The Act is aimed at protecting personal financial information provided by consumers to financial institutions. The Gramm-Leach-Bliley Act requires all financial institutions to notify consumers not only regarding what information is likely to be collected but also the use to which such information is to be put. The Act also requires financial institutions to develop a written security plan for all the information they intend to gather.

3. **The Health Insurance Portability and Accountability Act of 1996 (HIPAA)** includes a Privacy Rule, put in place by the U.S. Department of Health and Human Services. The Privacy Rule covers all personal health information, including any information about health status, provision of health care and payment for health care that can be linked to an individual. It also covers all information regarding a patient's medical records and payment history.

Various countries across the globe have already put in place a legislation to protect the rights of their citizens. The first and possibly most comprehensive attempt was made through the **Data Protection Act of 1998 by the U.K**. This Act covers all residents of the United Kingdom and all UK-based organizations.

According to the Data Protection Act, all personal information, including data that is not stored on a computerized system, is to be protected from abuse and secured from unauthorized access. The Act requires organizations collecting personal data to take appropriate technical and other measures to ensure the safety of data from unlawful access. The legislation also requires that data be protected during storage, transport, transition and update.

The major drawback of the Data Protection Act, however, is that it is known for its complexity. As a result, while many organizations seem unsure of exactly what the Act entails, others hide behind the Act and refuse to disclose even public information.

Data security legislation across various other nations includes:

1. **The EU Directive on Data Protection of 1998** – provides a framework for data security for all member nations. The legislation is aimed at protecting the rights of EU citizens with regard to the collection, use and storage of personal information. An organization that does business in one or more EU countries is obligated to abide by the minimum data protection stipulations of the data protection legislation of the country it operates in.

2. **The Privacy Amendment Act of 2000** – aims to bring **Australia** at par with international data security laws and to address concerns regarding data protection due to the growing online and ecommerce business sector. The Act monitors the handling of personal information by organizations operating in the country.

3. **The Personal Information Protections and Electronic Documents Act of Canada** – requires all organizations operating in the country to develop and implement a security policy for handling personal information. Security safeguards should include physical, technical and organizational measures to ensure data security.

4. **The Personal Information Protection Act of 2003** – provides guidelines for businesses for the handling of personal information of **Japan's** citizens, while outlining the fines and punishments for organizations that fail to comply with the legal requirements.

5. **Payment Card Industry Data Security Standard** – is a set of rules that ensures security of personal information submitted to payment brands, such as American Express, MasterCard, Discover, etc. The legislation ensures the security of customer account data on a global basis.

Various other countries, such as Argentina, Hong Kong, India and China, among others, have put national legislation in place to safeguard the interests of their citizens. The need of the hour, however, is for a uniform global legislation that establishes a standard code of conduct for all organizations that collect and use personal information. After all, with the advent of the Internet, the world is becoming little more than one large playground.