Data Security Obligations for Businesses

Most nations have laws in place to ensure the protection of personal information shared online by their citizens, a uniform global code of conduct towards data security obligations for businesses is yet to be put in place.

WinEncrypt

WinEncrypt™

Data Security Obligations for Businesses - What You Ought To Know

The spate of identity thefts, data thefts and hacking over the past decade has fueled a spurt in the attempts of governments to protect the rights of their people. While most nations have laws in place to ensure the protection of personal information shared online by their citizens, a uniform global code of conduct towards data security obligations for businesses is yet to be put in place.

Today, most businesses rely on their web presence to grow. Central to the success of any business is undoubtedly the trust it engenders in its customers. And what can engender trust better than the assurance that any sensitive data collected online will be subjected to most stringent security measures. Does data security need to be merely a legal obligation for businesses when it is clear from past experience that companies who have gone the extra mile to ensure security have better client additions and retention?

Companies operating in the finance, outsourcing and healthcare sectors have been found to be most prone to data theft due to the sensitive nature of the information they gather. Personal information that is considered sensitive includes name, address, telephone number, social security number, account number, credit or debit card number, personal identification number or password, driver's license number, user name and password or account number and its password.

In the United States, all data gathered by financial companies fall under the jurisdiction of the Gramm-Leach-Bliley Financial Modernization Act of 1999, which not only lays down guidelines for security measures but also requires the data gathering organization to inform the customer about the purpose of the data and to notify customers of any breach in security. The healthcare sector is similarly protected by the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Work is still in progress in various states to enact data security legislation, with California having already enacted the SB-1386 legislation of 2002.

What needs to be done?

For any business, from a small scale organization to a large scale multinational corporation, data security obligations need to be translated into action points that can be implemented, such as:

- ✓ A customer privacy policy should be developed and customers informed of the same. The customer should be notified of any modification to the policy or the implementation of new regulations as soon as possible.
- ✓ Periodic review of actions concerning responsibilities regarding data security and analysis of the resulting effect on business activities. For this, the foremost step to be taken is to regularly observe legislative changes at state and federal level.
- ✓ Any kind of personal information that has been collected so far should be examined regularly by businesses. Moreover, data that is usually discarded after being considered irrelevant should be secured against theft.

- ✓ Laws enforcing the regulation of computer usage, tracking gadgets such as CCTV's, etc., should be implemented across the business. One such law has recently been passed by the Parliament in New South Wales, Australia.
- ✓ As per surveillance legislation, the data that is recorded by surveillance equipment has to be retained and proper documentation of the computer policies needs to be made and employees across the organization need to be informed regarding the same.
- ✓ All businesses should get insurance coverage providing for loss incurred as a result of breach of data security.
- ✓ As far as data mining and data warehousing are concerned, related security policies should be introduced and duly implemented.
- ✓ In order to safeguard data from being disclosed, legal duties should be enforced even by small businesses. Legal guidance should be sought from lawyers with experience in the field of data security.

Thus, data security obligations for businesses pertain not only to data gathered online but to physical records and storage of information of any kind by an organization. Ensuring data security today might be seen as an unnecessary expense not required by law. But the benefits in terms of the impact on prospective and existing clientele will be invaluable.