Chapter 80
The Need for a National Data Breach Notification Law

Kirk Y. Williams
Walden University, USA

ABSTRACT

Individuals, groups, organizations, companies, and foreign government agencies that threaten the National Security of other countries, not only threaten their National Security but also threaten the security of state agencies, and the security of the individuals, groups, organizations, academic institutions that are consumers of those companies. Therefore, a National Data Breach Notification Law that would inform consumers once unwanted intrusions in the form of a cyber-attack occurs that results in the disclosure of their personal and financial information is needed. In the requests for a National Data Breach Notification Law suggestions have been made on what the law should include, and how the information should be reported to the public and to the individuals affected by the cyber-attack. This chapter explores how a National Data Breach Notification Law should be produced that would require uniformity across all states with guidelines that relate to the compliance of the law as it can affect individuals, organizations, academic institutions, companies, and governmental agencies.

INTRODUCTION

Individuals, groups, organizations, academic institutions, companies, and governmental agencies have all instilled a sense of security within our daily lives based on our reliance and use of secured forms of technology. With this reliance on secured forms of technology and communication networks, technology users – consumers – have begun to delude themselves into thinking that companies have levels of security and safety that exists within their secured and trusted networks that can defend itself from all forms of cyber intrusions. In their daily lives, consumers rely on those secured and trusted networked systems to access private information on secure Internet sites, and to conduct various forms of business in a safe and secure manner; therefore, that access must be global to complete the tasks at hand, and secured to not allow for communication interception by third parties. However with the reliance on technology, communication networks, and the access that users desire and require, consumers also make themselves

DOI: 10.4018/978-1-5225-5634-3.ch080

dependent on the security that is in place for each system that they access, only consumers never tend to think about how they leave themselves open to intruders who may also access those same secured networks. When intruders enter into these systems with unauthorized access, this leads to a security breach and can lead to a data loss or a data leak.

Each new security breach that leads to a data loss or a data leak can result in more companies being hacked and causes more consumer information to be released to the public. Each attack on a company not only compromises the security of the company, but also reduces the trust of the public in the individuals, organizations, academic institutions, companies, and governmental agencies that are in the business of providing security and protection to consumers that supposedly have safeguards in place to protect consumers and their information. When these safeguards fail, it leaves consumers wondering: *What where the safeguards that companies were using to protect the consumer(s) and their data/private information?* However, additional worries have increased with regard to protecting data from security breaches, and consumers have begun to ask: *Should more be done to safeguard consumer information? What additional items should be considered with regard to the state and federal laws and the reporting of security breaches, data loss, and data breaches*?

Although these are the typical questions that one would ask after a security breach that results in data loss occurs, it should be the forethought on everyone's mind when establishing public and private policies that govern data loss as a result of a security breach. Over the last five years, numerous individuals, organizations, academic institutions, companies, and members within the governmental agencies have called for a change in the reporting and openness of information that resulted in data loss, the reporting of security breaches that resulted in data loss. With these requests these individuals, organizations, academic institutions, companies, and members within the governmental agencies have requested reporting in the form of laws and policies to be established on the state and federal level to govern the reporting of the information and notification of the data breaches that resulted in a data loss. With these requests, these individuals, organizations, academic institutions, and companies feel that the US government should consider constructing and implementing federal policies that govern security breaches that result in a data loss. In their formation of such policies, it has been suggested that federal agencies consult with state officials on the laws that each state has in place, determine what the states would like to achieve with their laws, evaluate what they are doing to enforce the law, and review how the state established reporting from organizations, academic institutions, companies, and government agencies that have been breached.

Currently each individual state have some laws in places that comprise a patch work of laws that focus on data breaches, but each state is not consistent and the laws in place are not effective across the entire United States. Therefore the objective of this chapter is to inform others where they can find information on which states have policies and laws at the local and state level that pertains to notifications and security breaches, suggest how such policies can be enforced, suggest what can be done on the federal level in the way of developing a National Data Breach Notification Law, and discuss areas of the Data Security and Breach Notification Act of 2015.

THE NEED FOR A NATIONAL DATA BREACH NOTIFICATION LAW

With each new cyber-attack, security breach, data leak, or data loss, constantly evolving, different and inconsistent responses are reported to the consumer as described in blogs, media reports, and company