Taking Aim at Data Breaches and Cyberattacks

BY PAM GREENBERG

A little more than a decade ago, a security breach that released the personal information of almost 145,000 people to a criminal enterprise created a rush in state legislatures to enact security breach disclosure laws. That early breach seems almost insignificant when compared to the recent Equifax data breach, which exposed the social security numbers and other sensitive personal information of nearly 146 million Americans.

Forty-eight states, Washington, D.C., and the territories now have laws requiring that security breaches be disclosed to consumers. Many state lawmakers, however, continue to ask what they can do to protect citizens from security breaches.

State Action

Expanding breach notification laws. States are addressing data breaches in a variety of ways. Some are continuing to amend laws that notify people when their information has been breached. Trends in breach legislation include expanding definitions of “personal information” in cases of a breach (for example, health or medical information, biometric data, or usernames and passwords). States also are setting a time frame (usually 30, 45 or 90 days) within which consumers must be notified of a breach.

Requiring adequate security measures. An increasing number of states, however, are starting to turn their attention toward the security practices

Did You Know?

• Financial, health-care and public-sector organizations accounted for more than half of the breaches in a 2017 Verizon report on data breaches.
• The No. 1 leading cause of data breaches worldwide is employee error, according to the Privacy Rights Clearinghouse.
• Most cyberattacks begin with a user clicking on a phishing (fraudulent) email, says threat management company PhishMe, and an average of 4,000 ransomware attacks occurred per day in 2016, according to the FBI.
Increasingly, state lawmakers are looking at the security practices of their own state agencies. At least 19 states require, by statute, that state government agencies have in place specific policies or measures to ensure the security of the data they hold. Of businesses and government. At least 13 states have laws requiring businesses that own, license or maintain personal information about a state resident to implement and maintain security procedures and practices. While most of these states require only that “reasonable” security practices be followed, some requirements are more detailed and prescriptive. For example, regulations in Massachusetts require that a comprehensive information security program—which, among other things, must encrypt personal information—be developed, implemented and maintained. Other state and federal laws address the security of health care data, financial or credit information, social security numbers or other specific types of data collected or maintained by businesses.

State and federal government agencies hold vast amounts of data about citizens, and too many have suffered breaches. Increasingly, state lawmakers are looking at the security practices of their own state agencies. At least 19 states require, by statute, that state government agencies have in place specific policies or measures to ensure the security of the data they hold.

Many of these state laws provide for a statewide, comprehensive approach to security and security oversight. Most require agencies to implement and maintain reasonable security procedures and practices to protect sensitive information from unauthorized access, destruction, use, modification or disclosure. Some laws also require training, periodic security audits or assessments, development of standards and guidelines, and other provisions.

Centralizing cybersecurity oversight in government. States also are creating chief information security officer (CISO) positions to establish, oversee and facilitate statewide security management programs. At least eight states—Arizona, Colorado, Florida, Kentucky, Massachusetts, Ohio, Utah and Washington—require, by statute, a statewide executive branch CISO position or positions in state government. Other states have created CISO positions through executive orders or agency actions. According to a December 2016 Deloitte-NASCIO Cybersecurity Study, respondents from 49 states reported having an enterprise-level CISO position, which has become more consistent in terms of responsibilities and span of oversight.

Expanding and enhancing computer crime laws and penalties. All 50 states have computer crime laws that deal with criminal offenses committed using a computer. However, with new and growing threats like ransomware—a virus that blocks computer access until a ransom is paid—some states are targeting specific types of attacks to close loopholes in the law and make prosecution easier: These include ransomware and computer extortion, denial of service attacks, phishing (fraudulent emails) and spyware (software that collects people’s personal information without their knowledge).

State lawmakers also are looking at increasing penalties for cybercrimes. For example, last year, Washington enacted a comprehensive computer crime law that includes enhanced penalties for cybercrimes, and in 2017, Texas enacted a series of cybersecurity and computer crime bills. The new laws establish certain cybersecurity requirements for all state agencies in Texas, create a cybersecurity council, and require studies and reports related to cybersecurity threats and responses. Texas law also now expressly criminalizes denial of service attacks, ransomware and intentional deceptive data alteration.

Federal Action

Computer crimes are covered under the federal Computer Fraud and Abuse Act (CFAAA, 18 U.S.C. sec. 1030). Under the act, several penalties exist for unauthorized access of government computers. Private computers connected to the internet are protected in several situations: 1) if financial information is accessed, 2) if the intent of access is to defraud or 3) if the access causes damages in excess of $5,000. The Cybersecurity Information Sharing Act of 2015 (CISA) encourages businesses, state, tribal and local governments, and the federal government to share cybersecurity threat information. The Controlling the Assault of Non-Solicited Pornography And Marketing (CAN-SPAM) Act of 2003 prohibits fraudulent and deceptive emails.

Numerous security breach and cybersecurity bills have been introduced in the current 115th Congress.