TechTarget Security Media
SearchSecurity.com SearchSecurity.co.UK SearchSecurity.in SearchFinancialSecurity.com SearchMidmarketSecurity.com
SearchSecurityChannel.com INFORMATION SECURITY DECISIONS FINANCIAL INFORMATION SECURITY DECISIONS INFORMATION SECURITY

SearchSecurity.com
E-Guide

DATA Act protection: Effects of a federal breach notification law

The Data Accountability and Trust Act, should it become law, would mandate new breach notification requirements. What does this mean for enterprises? This article will look at the new reporting requirements and examine when and how your organization will have to report a breach to the FTC and what new steps you'll have to institute to comply.

TechTarget
Where Serious Technology Buyers Decide

SearchSecurity.com
E-Guide

DATA Act protection: Effects of a federal breach notification law

Table of Contents

DATA Act protection: Effects of a federal breach notification law

Resources from CDW Corporation

DATA Act protection: Effects of a federal breach notification law

By Richard Mackey, Contributor

As of this publication, a federal personal data protection bill, called the Data Accountability and Trust Act (DATA), has passed in the House of Representatives and is awaiting Senate approval. Designed to protect personally identifiable information (PII) from misuse, the DATA Act, if passed, would be similar to many existing state identity data breach notification laws requiring organizations that are entrusted with PII to report breaches promptly once they are discovered.

The business benefit of the proposed federal breach notification law is that it would supersede the 48 existing state and territory laws that vary in their definitions of personal information, specify different notification methods and differ in their requirements for preventive and detective controls.

Another difference is enforcement. The federal law would be regulated and enforced primarily by the Federal Trade Commission (FTC) rather than the state attorneys general. This is important in two ways: The law applies only to organizations that fall under the jurisdiction of the FTC, and it centralizes the rulemaking, regulation, and, to some degree, enforcement. The FTC's jurisdiction limits the applicability of breach laws because the FTC does not regulate banks, common carriers, federal credit unions or savings and loans. And, while the DATA Act is supposed to supersede state laws, it's hard to say whether the state laws will still be in effect for organizations such as these that fall outside the jurisdiction of the FTC. It is interesting to note that the bill does not remove states from the equation altogether. The bill specifically reserves states' rights to bring civil suits and impose penalties on organizations that do not comply with the requirements of the act.

The mechanics of notification under DATA

Under DATA Act protection, when a breach occurs, the party responsible for the breach needs to notify affected parties in a manner similar to those required by existing state laws. One major -- and simplifying -- difference is that, instead of performing the notifications according to the requirements of each state whose residents' information was compromised, the organization notifies the victims and regulators according to the rules established by the FTC.

The mechanics of notification under the DATA Act are as follows:

1. The "owner or possessor" of the personal data (i.e., the organization suffering the breach) needs to notify the individuals whose data was breached and the FTC within 60 days of discovery of the breach.
2. The notification must include a description of the personal information that was breached, a toll-free telephone number for information about the breach, an offer to provide free credit reports or credit monitoring service for two years to individuals affected by the breach, contact information for the major credit reporting agencies, and contact information for the FTC. In this case, it would be wise for organizations to err on the side of caution and notify all individuals whose data may have been breached, not just those whose information was provably breached.
3. Notification of individuals can take multiple forms. The organization can send written notice to all those affected. Alternatively, if the organization possesses email contact information for the victims and the affected parties have consented to receive official correspondence electronically, it may notify via email.
4. If the organization possesses fewer than 1,000 records and does not have sufficient contact information for all parties, or the cost of notification is excessive (as defined by the FTC after the bill is passed), it must display a notice prominently on its website, provide a notice in print and broadcast media in areas where victims reside, and notify affected parties by email (where contact information is available).
5. If the number of accounts breached exceeds 5,000, the organization must report the breach to the three national credit reporting agencies.
6. Service providers that discover a breach must report to the organization consuming the service. The organization with a relationship with the victims must perform the

notification. For example, if a merchant contracts a service provider to process credit cards, and the processor has a breach, the processor must report to the merchant, and the merchant must notify the cardholders.

DATA, like some state laws, allows organizations to avoid notification if there is no reasonable risk of identity theft, fraud or unlawful conduct. The bill includes an example of such a scenario, describing data that was transmitted to unauthorized parties, but was unusable, unreadable or indecipherable. In other regulations (e.g., the HITECH enhancements to HIPAA), exposure is only considered a breach if the data was "unencrypted," or both the ciphertext and the key were compromised. To be conservative, accidentally sharing identity data with the wrong trusted partner would still be considered a breach.

The story isn't over

There are several significant concerns regarding the proposed DATA Act that still need to be taken into account. First, the DATA bill did not pass Congress last year and it is still tenuous as to whether it will pass this year. Currently, there are competing bills in Congress that attempt to fill the same need.

From another angle, such a law may limit the ability of the states attorneys general to protect their citizens, particularly if the final version of the federal bill is less strict than the state laws it would supersede. Finally, if the bill becomes law, the FTC will establish regulations that describe the controls and processes in detail that companies must follow. We will not know the whole story until all this is complete.

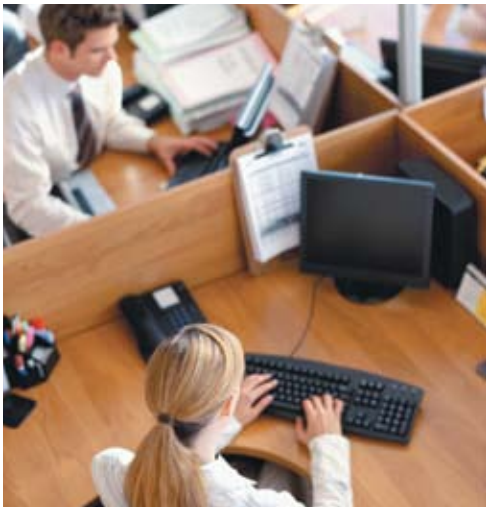
Conclusion

If made into law, the DATA Act would help to alleviate the complexity of compliance with state identity protection laws by making the process of notification more manageable and less expensive. Unfortunately, as the bill has yet to pass in Congress, the eventual contents of the bill, the effect FTC regulation will have on its enforcement, and the reaction the states will have to a single federal law that supersedes states' laws are uncertain. But, whatever

the outcome, understanding the possible implications of a federal data protection law can help you prepare your enterprise for compliance if and when the time comes.

About the author:

Richard Mackey has advised leading Wall Street firms on security architecture, VPNs, enterprise wide authentication, and intrusion detection. Prior to joining the consultancy SystemExperts, he was the director of collaborative development for The Open Group. Mackey is an original member of the DCE Request for Technology technical evaluation team and was responsible for the architecture of the Distributed Computing Environment Releases 1.1 and 1.2. Mackey has been a frequent speaker at major conferences and has taught tutorials on developing secure distributed applications.



Waging an endless war against security threats? We can help you prepare for battle.

Security threats like viruses, worms and hackers are toxic to your infrastructure. Fighting them off can burn through your time, and your budget. Not to worry. At CDW, we have your back. We have the people, products and plan to help keep your systems and sensitive data safe. Our security specialists can assess your infrastructure as well as design and implement a solution tailored to your needs. We know the latest threats and are well-versed in combating them. It's why we're the best allies in the business.

For free Symantec trialware, how-to videos or more information, visit CDW.com/protectionsuite

Symantec + CDW

Symantec and CDW. Partners and problem-solvers.

Resources from CDW Corporation

Are You Getting the Best Security for Your Money?

Getting from Point A to Point DLP

About CDW Corporation

CDW's business model focuses on small- and medium-sized businesses with 97 percent of sales derived from commercial accounts. CDW has built strong relationships within the technology sector and we are a leading direct source for Cisco, HP, IBM, Intel, Microsoft, Sony, Toshiba, and other top name brands. Our success is due to our exceptional coworkers, who are the most important element of CDW's business strategy. To foster our coworkers' success, CDW has designed a rewarding and challenging work place, recognized as one of the best companies to work for in America.