Source: Smiley Pete Publishing

Safely storing confidential customer data in the cloud

by Will Montague and Todd Gieseler

December 08, 2010

Lexington, KY - Two major legal and technological changes that have taken place in the past several years are now colliding. First, with the rise of social networking and other trends, governments at every level are passing tougher laws that protect the privacy and security of personal data. Second, the decreasing costs of computer storage and bandwidth make it feasible for the first time for businesses of all sizes to outsource storage of their customers' personal and financial data to the "cloud."

These two changes — a patchwork of new privacy and data security laws and the rapid rise of cloud computing — mean that businesses face different data storage risks. Businesses therefore should understand, both from a legal and technological perspective, how to use cloud computing safely to store personal data about their customers.

Some privacy and data security laws have been in place for years. For instance, HIPAA regulates the privacy and security of medical information, the Graham-Leach-Bliley Act controls how financial institutions must safeguard customer data, and the European Union's privacy directives regulate how personal data of European citizens — now the customers of most any internet-based business — may be treated.

Quickly rising, however, is the number of states that require disclosure to their citizens when the security of an out-of-state business's customer database is compromised. These instances — not limited simply to situations where a computer criminal has hacked into the database — are usually very expensive to remedy and create public relations disasters for consumer-facing businesses.

Similarly, the FTC is currently in the process of rolling out its Red Flag Rule: federal regulations requiring all sorts of businesses that maintain credit accounts for their customers to maintain policies and procedures to protect against identity theft. While the FTC says the Red Flag Rule "picks up where data security leaves off," the rule is yet another patch in the patchwork of privacy and personal data regulation applicable to so many businesses.

Even private industry is imposing its own new data security requirements. The Payment Card Industry Data Security Standard (PCI DSS) sets specific data security requirements for businesses that accept credit card information from customers. If you don't comply, you risk losing your ability to take payment from your customer by credit card.

Under most or all of these laws, even though a business outsources its data storage to a third-party service provider, it does not surrender its legal responsibility to securely store the data. According to some laws, the controls of the service provider effectively become the controls of the business. Other laws specifically state that, when outsourcing data storage, businesses must take reasonable steps to select a provider that will comply with the requirements applicable to the business itself.

In other words, it's not enough simply to outsource data storage to a cloud provider with a good reputation. Special attention is necessary to ensure that the service provider's practices match or exceed those that would be used if the data storage was not outsourced.

When contracting for storage in the cloud, a business should ensure that its agreement with the service provider requires a level of data security at least as strong as its own. As always, the devil will be in the details, so a business should push for concrete details in the agreement about how the storage provider will handle things like infrastructure security, compliance reporting, security auditing, and data storage and access metho-dologies.

Infrastructure security is crucial when storing data in the cloud. At an absolute minimum, security devices such as firewalls and intrusion prevention systems should be utilized, and workable security controls and reporting systems should be in place.

Organizations should also ensure that the service provider maintains appropriate physical security measures. The service

provider should always store the customer's data in a secured, isolated environment with strict controls over internal and external access to the data. Limited personnel should maintain access to the data, and all physical access should be logged.

Logical data access should be limited and documented. Technologies such as firewall rules and access control lists should be utilized. The logical segmentation of data should also be used in order to limit data access to only authorized users and systems.

A business should likewise validate that its data will be encrypted when being accessed from the cloud. The data should be stored and backed up in an encrypted format, and accessed via encrypted sessions utilizing technology standards such as Secure Socket Layer (SSL) and Internet Protocol Security (IPSec) Virtual Private Network (VPN).

Unfortunately, this article covers just the tip of the iceberg when it comes to safely and securely storing data in the cloud. A business that starts by addressing these few items, however, can at least feel comfortable that it's on the right path.

Will Montague is a partner in Dinsmore & Shohl's Lexington office and can be reached at (859) 425-1057 or by email at will.montague@dinslaw.com.

Todd Gieseler is a Consulting System Engineer with NetGain Technologies and can be reached at (502) 212-4737 or by email at tgieseler@netgainit.com.