ABA Insurance Services
Serving banks for 25 years.

Safe Talk®
Loss Control Bulletin

SPECIAL REPORT

Use The Cloud With Caution

Many banks and other businesses are turning to "the cloud" for their IT resources, particularly when it comes to obtaining software and data storage. The primary benefit of using the cloud is a lower IT cost structure, but using cloud-based software also can speed decision making and help a bank improve its overall risk management practices. The influential marketing blog, marketresearch.com, published a report claiming cloud computing will be a $25 billion enterprise by 2013.

It is very likely that you are using certain software or data storage solutions without even realizing they are part of the cloud. Before we examine the insurance ramifications of using cloud technology, a brief introduction to the concept is in order.

The cloud may appear to be relatively new but it has been around a since the inception of the Internet. Only recently (since it has crept into our daily business and personal lives) has it been termed "the cloud." In essence, using the cloud is simply "renting or borrowing" Internet or Web-based software and storage from a third-party vendor. Today, banks often use cloud-based software to process and manage their loan application, approval and tracking processes. Banks also commonly use the cloud for remote data storage and data management.

In general, most insurance underwriters take a holistic view of a bank's electronic risk and do not focus specifically on the cloud. For this reason, insurance applications do not ask about the cloud, and cloud computing is not defined in any commonly available insurance policies. While coverage determinations depend on the specific facts and circumstances of individual claims, those arising out of cloud-based activities should be analyzed in the same manner as those arising out of other electronic activities.

As a best practice, we recommend that you review your coverage for all electronic activity. A comprehensive insurance program with broad-form electronic coverage is a must in today's rapidly changing environment. A properly structured program includes coverage for lawsuits against the bank and its officers and employees, as well as protection against first-party losses incurred when a bank is legally liable for a customer's loss. Beware of electronic policies that are written on a named-peril basis. They are significantly more restrictive than broad-form policies.

Proper insurance, however, is only part of the equation. As with any technology, there are steps that can be taken to mitigate your potential exposure when a problem arises.

- **Be sure to talk with your vendor regarding their data security measures**. In your customer's eyes, you are responsible for adequately safeguarding their personal and confidential information, regardless of where it is ultimately housed. Encryption is a key security measure in the protection of data, especially as it moves electronically from your network to the cloud. Also, login credential verification should be increased (i.e. more "personal" security questions asked of the logger) when there are attempts to access the cloud from IP addresses other than those of your bank's own standard IP addresses.
- **Access to cloud-based services should be password-protected and restricted only to employees with user IDs and passwords**. Security measures in place for the cloud should not be any different than those in place for your in-house network or servers. Be sure that your internal and malware policies are up-to-date and in place regarding Web site access, use of external storage media (i.e. thumb drives) and .exe files. These can create opportunities for perpetrators to get login credentials and gain access to your cloud systems. It may not be foolproof, but it does lend an additional wall of security against hackers. And to minimize your bank's vulnerability from security issues, access should be blocked immediately when an employee or contractor is terminated or leaves.
- **Also, be aware of where your data is actually stored**. Even though your bank and your cloud vendor's offices are located on U.S. soil, it doesn't mean your data is housed here. Your bank could be vulnerable to claims if the data is physically housed in a foreign country with lax security measures. There may also be regulatory and compliance concerns if data is stored on servers outside of the country.
- **Finally, ask your vendor about their procedures for preventing and combating viral intrusions to their primary and back-up servers**. The insurance industry continues to see losses resulting from these types of breaches.

Banks are using the cloud more frequently. The technology creates cost savings and other efficiencies, and the use of cloud-based computing can be completely transparent to your customers. For these reasons, cloud technology is enticing to banks of all sizes. With a properly structured insurance program and sound risk management practices, using the cloud should not present any material problems to your bank.