How to Prevent a Breach of Your Cloud-Hosted Data

February 27, 2017
By: Alex Beall

While most cloud service providers meet data security standards, associations still need to ensure those standards are kept and their data is protected. Taking preventative steps can mitigate the risk of a cloud-based data breach.

The idea of hosting data with a third-party cloud service provider isn't a new concept for associations. Many use these services for data storage or management, either relying on the cloud as their entire data center or choosing a hybrid model that treats the cloud as an extension of their internal data center.

"Many associations are moving their AMS's, regulated data, and sensitive data to the cloud because these cloud service provider vendors are being able to offer compliant and secure infrastructures hosted within the cloud," says David Kim, senior vice president, information security, of governance risk and compliance services at ITPG, Inc.

The decision to switch to cloud-based storage largely depends on the related hardware, software, and operational costs. In fact, IT spending on cloud services is expected to reach $216 billion in 2020, with more than $1 trillion in IT spending being affected by the shift to cloud services, according to **tech research firm Gartner, Inc.**

> **Ask, 'Am I prepared to transfer that risk and the risks or vulnerabilities associated with regulatory compliance, security, and privacy to a third-party vendor?**
>
> **—David Kim, ITPG, Inc.**

But switching to the cloud can leave data vulnerable in new ways, something associations need to be aware of and take steps to address. Because the fact is if something goes wrong, it's the association and its members who bear the worst consequences.

Before choosing a cloud provider, Kim recommends that association leaders ask, "Am I prepared to transfer that risk and the risks or vulnerabilities associated with regulatory compliance, security, and privacy to a third-party vendor?" And if they decide to make the switch, Kim recommends taking precautions to protect members' information, knowing that the association no longer has direct control over the security of its data.

Vetting the vendor. During the vendor-selection process, risk mitigation involves assessing a potential provider by running a cloud security assessment. Associations should compare the provider to a baseline set of security standards, like **Shared Assessments** or **Cloud Security Alliance**. They should also determine if the provider has gone through an internal certification and attestation process, further demonstrating it meets certain industry standards. "You, as an association, want to look for a cloud-security vendor that is already regulatory compliant, that is already addressing security and privacy," Kim says.

Signing the contract. A vague contract could leave weak points in an association's security defenses. Once an association chooses a vendor, it must lay out a master services agreement that will help mitigate that risk. The contract should determine how the association and the company will each handle the data, such as if the data will be encrypted and who is responsible for that process. And in the event of a cyberattack, the agreement should outline who is liable and who will cover the resulting cost—a decision that goes hand-in-hand with the association's breach response plan.

Transferring and storing data. During the transfer of data to a cloud storage system, information could be uniquely vulnerable to security risks. If the data is too large to upload, a physical transfer will be required. The association will need to bring the data directly to the provider's storage center. If the location is farther away, the data will need to be sent by mail, in which case the data should be encrypted and closely tracked to prevent theft.

Another risk arises if the association decides to use a public cloud, a situation in which private information is stored in the same piece of hardware as other cloud tenants' data. In such cases, a flaw in one of the other client's applications could also put the association's data at risk. For a higher cost, associations can use a private cloud, meaning the data would be held in its own storage unit.

Maintaining security. Risk mitigation shouldn't end once the association vets a provider, signs the contract, and stores its data. Kim recommends that associations perform annual security risk assessments and penetration tests, as well as ongoing vulnerability assessment scanning, to ensure their provider maintains security compliance.

"[T]hose are still your IT assets, and those are still an extension of your IT infrastructure," he says. "So that is the only way to maintain and continuously look at where your security baseline is, even if you're using an external cloud service provider."

After all, while the cloud hosts the data, the responsibility to protect association members still rests with you.