Official White Paper

Security in the Cloud November, 2011

Cloud computing looms ever larger—from consumers accessing music and video via iCloud and Microsoft 7 to the federal government requiring agencies to develop cloud-based solutions with the aim of trimming the deficit by consolidating data centers. As more people rely on their smart phones and tablets for Internet access, the mobile cloud is taking shape; IBM estimates that *1 trillion* devices, many of them mobile, will be connected to the Internet by 2013. According to the website CloudTech, worldwide cloud adoption is growing at an annual clip of 17 percent, and half of the business organizations it polled have implemented some form of cloud computing.

The question for credit unions, then, becomes not whether to consider moving to the cloud, but how to take advantage of the economies, efficiencies, and opportunities it offers while simultaneously and continuously ensuring the security of data hosted in the cloud. As credit unions evaluate outsourcing critical applications, including lending and imaging packages, e-mail, virtual desktop, home banking, and core data systems, they must ensure that the vendors they select meet or exceed their own security standards. Security can often be enhanced by moving to a cloud-based solution, provided that the vendor providing cloud services understands the unique requirements of credit unions.

As a CUSO committed to serving credit union's business continuity and technology needs, Ongoing Operations (OGO) employs a broad set of policies, technologies, and controls to protect the data, applications, and associated infrastructure of client credit unions within the structure of the cloud computing environment and in compliance with NCUA's information security requirements. This white paper presents a brief overview of key considerations in assessing the security of cloud solutions.

Evaluating Potential Vendors Offering Cloud-Based Solutions

In its *IT Examinations Handbook,* the Federal Financial Institutions Examination Council (FFIEC) cites the risks credit unions must manage in outsourcing technology services, cloud-based or otherwise, including the potential for financial losses, data breaches, damage to reputation and competitive standing, regulatory action, and costly lawsuits. Toward that end, here are a few of the questions credit unions must address in the vendor selection process:

- How does the vendor's security model compare with that of your credit union?
- What type of service level agreement (SLA) would be acceptable for your credit union and members for this application? How does the SLA proposed by the vendor compared with internal downtime the credit union currently experiences?

- Is the vendor familiar with credit unions and the multiple third party connections they require (e.g., Federal Reserve, core processor, online banking vendors, debit and credit card processors)?
- Is the vendor familiar with the security requirements for credit unions required by the NCUA and spelled out in the *FFIEC IT Examinations Handbook*?
- Do the vendor's financial records and history suggest long-term viability? This is a critical consideration if your credit union plans to shift from an internal infrastructure to cloud-based solutions.
- How would staff levels be affected internally? What other initiatives could the credit union move forward if the data center functions were outsourced?
- What impact, if any, might this solution and vendor relationship have on member service?

A more comprehensive list of sample questions is provided in the Credit Union Information Security Questionnaire for your reference.

Security at OGO Data Centers

Ongoing Operations maintains a highly controlled environment, certified to meet SAS 70 standards and currently undergoing an independent audit required for the new standards of SSAE 16. Certain OGO facilities have also been structured to comply with the PCI Data Security Standard. Here are a few examples of how OGO meets or surpasses the standards for secure operations:

Physical security

- Secure access cards for all facilities, broken down by zones
- Cameras, front- and rear-facing at each door
- Secure code employing multi-authentication
- Additional security measures as needed for specific clients

Environmental safeguards

- Fire detection and suppression
- Climate and temperature
- Uninterruptible power supply (UPS); backup power supply from diesel generators

Employee policies

- Background checks for employees and client representatives

Backup and redundancy

- Cloud-based solutions hosted at multiple geographically diverse locations, with real-time data replication and backup

Account Level and Network Security in the Cloud

Ongoing Operations' approach to account level security in the cloud meets similarly exacting standards. A physical desktop can be accessed via one password, or multifactor authentication may be applied, with additional authentication requirements when trying to launch core systems or other critical applications. The virtual desktop can be structured in the same way.

One advantage of using virtual desktops in the area of security is that a user's access to all applications can be shut down much more quickly than when managing individual applications. For example, if an employee is terminated, one click in our management console will prevent him or her from accessing anything through the virtual desktop and any additional components in the network. Virtual desktops also imply that remote employees (at branch offices or home ofices) to mot retain local copies of company data. Since the data on the virtual desktop actually resides in one of Ongoing Operations secure datacenters there is no risk of it being compromised if a laptop or desktop is lost or stolen.

VPN certificates and RSA keys are other options for multifactor authentication. In addition, OGO can structure its network interface to isolate client credit unions' data. Our platform is robust and flexible enough to facilitate the varying levels of security required by individual credit unions with diverse application requirements.

OGO's network security complies with NCUA requirements for security domains; perimeter protections, including firewalls, malicious code prevention, outbound filtering, and security monitoring; appropriate application access controls; and remote access controls, including wireless, VPN, modem, and Internet-based controls.

Conclusion

The European Network and Information Security Agency (ENISA) notes in a recent report that "the cloud's economies of scale and flexibility are both a friend and a foe from a security point of view. The massive concentrations of resources and data present a more attractive target to attackers, but cloud-based defences can be more robust, scalable and cost-effective." As credit unions come to rely increasingly on cloud-based solutions, they must be able to count on the technology services providers with whom they partner to be as committed as they are to identify and address emerging security concerns. As the FFIEC handbook cautions:

> Security is an ongoing process, whereby the condition of a financial institution's controls is just one indicator of its overall security posture. Other indicators include the ability of the institution to continually assess its posture and react appropriately in the face of rapidly changing threats, technologies, and business conditions. A financial institution establishes and maintains truly effective information security when it continuously integrates process, people, and technology to mitigate risk … Financial institutions protect their information by instituting a security process that identifies risks, forms a strategy to manage the risks, implements the strategy, tests the implementation, and monitors the environment to control the risks.

Nowhere is this approach to information security more vital than in the migration to cloud services. It is possible for your credit union to secure the cloud provided that:

- Your vendor evaluation and selection process effectively assesses the track record and continued commitment of technology services providers in the area of security;
- You thoroughly vet their financial health and stability and long-term viability;
- You require redundancy and examine the business continuity plans of hosted solutions; and

- You ensure that prospective partners in the cloud understand the requirements of the financial services industry in general and credit unions in particular.

To learn more about Ongoing Operations' cloud-based solutions, please contact us at info@ongoingoperations.com or 877-552-7892.