OVERCOMING THE FEAR OF CLOUD

Results from the 2012 Cloud Computing Security Survey

by Jenny Mangelsdorf

Despite cloud's stratospheric adoption rates among businesses, governments and personal users, lingering doubts about data security remain. Information Security Media Group's 2012 Cloud Computing Security Survey found security concerns are still top-of-mind for users considering cloud adoption.

The CSC-sponsored survey examines cloud security concerns, as well as how risks are being addressed through policy, technology and vendor management. The survey queried senior leaders who are involved with cloud computing decision making in their organizations and help determine their organizations' IT and/or IT security budgets.

The survey found that nearly one-third of respondents' organizations haven't used any cloud architecture, citing worries about data protection as their "greatest reservation," followed by "enforcement of security policies" and "data loss."

"Data protection is a particularly important concern," says Sam Visner, vice president and general manager, cybersecurity.

"Organizations need to ensure that their cybersecurity policies and protections cover information assurance — particularly as they seek to unlock the value of information and big data and use it to make high-value decisions regarding customer strategy, public policy and national security. The survey shows we still have some way to go to allay these types of cybersecurity concerns."

Almost three-fourths of the respondents reported that security concerns prevent them from adopting many cloud services. Of the services they currently or will shortly use, application hosting tied email/messaging at the top of the list, both at 34%, with data storage following at 29%, collaboration software at 25% and application development/testing at 23%.

Popular Offerings

What cloud services does your organization have or will shortly deploy? (top five answers listed)

Vendors, trust and risk

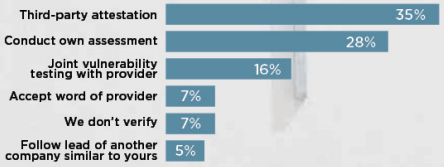
Tied to cloud security are issues such as cloud vendors' trustworthiness, risk, ultimate responsibility and the cloud's effect on the bottom line. More than two-thirds of the survey's respondents expect cloud computing will save their organizations money. When asked about the benefits of cloud computing, respondents ranked cost savings at the top, followed by better scalability and improved flexibility as second and third, respectively.

Even though survey respondents believe in the cloud's benefits, approximately 40% of respondents' organizations had allocated just 10% or less of their IT budgets on public, community and hybrid clouds. Nearly 40% hadn't budgeted for these types of clouds at all.

When organizations use the cloud, they believe that trust is key to adoption. More than 85% stated that external certification of a cloud provider is crucial. To reduce risk, 66% of respondents used a third-party organization to "certify or attest a cloud provider's security," whereas only 7% reported not verifying provider security in any way.

Checking Out Cloud Providers

What are the primary ways your organization verifies the security your cloud provider offers? (top six answers listed)



"Information technology professionals in general, and CIOs in particular, need to be informed about the controls necessary to protect their operations and the providers' approach to meeting those controls," says Visner. "Those contemplating the acquisition of cloud services should look carefully at how security certification or attestation is being performed, and who is performing it."

For U.S. federal government respondents, 57% said they use third-party providers to vet cloud providers' security. That will change as a new U.S. initiative called the Federal Risk and Authorization Management Program becomes operational this year. Under the initiative, the government will require agencies to use third-party assessment organizations to independently verify and validate that cloud providers meet security requirements.

While 79% of respondents stated that security is a "high priority" when evaluating a cloud provider, only 41% believe they have adequate policies and procedures to enable safe and secure cloud use. Just 50% of respondents also stated that internal audit reviews provide appropriate feedback to improve cloud security. Two reasons respondents cited for this low confidence in internal audits is a lack of education and sophistication in many cloud initiatives.

To enhance confidence, NASA's Jet Propulsion Laboratory (JPL), an early cloud adopter, has created a Cloud Computing Commodity Board, whose members span JPL, from departments such as finance and acquisitions to individuals such as the scientists and researchers who will be using the cloud.

"We don't put everything in one cloud because different clouds are good at different things," says Tom Soderstrom, JPL chief technology officer/IT, in the survey report. "So far we have data in 10 different clouds, and we let the users dictate which one is the stronger."

Ultimate responsibility

Regardless of how well vetted a cloud provider's security may be, respondents show different views on who ultimately has responsibility for security.

"Whether you put [your data] in the cloud or in the trunk of your car, it's your responsibility," says Françoise Gilbert, IT Law Group managing director, in the survey report. "It may be even more responsibility than before because there are situations where the cloud provider does not have a clue about the data that you have ... because that's not their business."

Just more than half of the respondents agree with Gilbert, with 38% handing responsibility to the IT or IT security organization, and 14% giving it to the business side/data owner. However, 48% of respondents give responsibility for ensuring security of cloud resources to the cloud provider.

The Guardians

Who's responsible for ensuring security of cloud resources?

"One of the things people thought [was], 'Maybe we could get out from under some of this risk if we move things to the cloud,'" says David Matthews, City of Seattle deputy chief information security officer, in the survey report. "We just have to assume that we've got, if anything, maybe more risk, or a different kind anyway."

As enterprise computing continues to move to the cloud, ultimately security will be the IT security professional's responsibility, the survey reports. However, the survey adds, in taking that responsibility, professionals should partner with their organization's IT and business groups as well as the cloud provider. ■

JENNY MANGELSDORF is a writer for CSC's digital marketing team.

6 PRINCIPLES FOR EFFECTIVE CLOUD COMPUTING

ISACA, the professional association focused on IT governance, says organizations adopting cloud should adhere to the following principles:

- **Enablement:** Plan for cloud computing as a strategic enabler, rather than as an outsourcing arrangement or technical platform.
- **Cost/benefit:** Evaluate the benefits of a cloud acquisition based on a full understanding of the costs of cloud compared to the costs of other technology solutions.
- **Enterprise risk:** Take an enterprise risk management perspective to manage the adoption and use of cloud.
- **Capability:** Integrate the full extent of capabilities that cloud providers offer with internal resources, to provide a comprehensive technical support and delivery solution.
- **Accountability:** Manage accountabilities by clearly defining internal and provider responsibilities.
- **Trust:** Make trust an essential part of cloud solutions, building trust into all business processes that depend on cloud computing.

Download the full Cloud Computing Security Survey report at csc.com/CloudReport2012.