Q With the proliferation of cloud computing services available, our organization is considering moving IT-related services to cloud-based services. What are the benefits and risk associated with using cloud services? What steps should we follow when selecting a cloud service provider (CSP)?

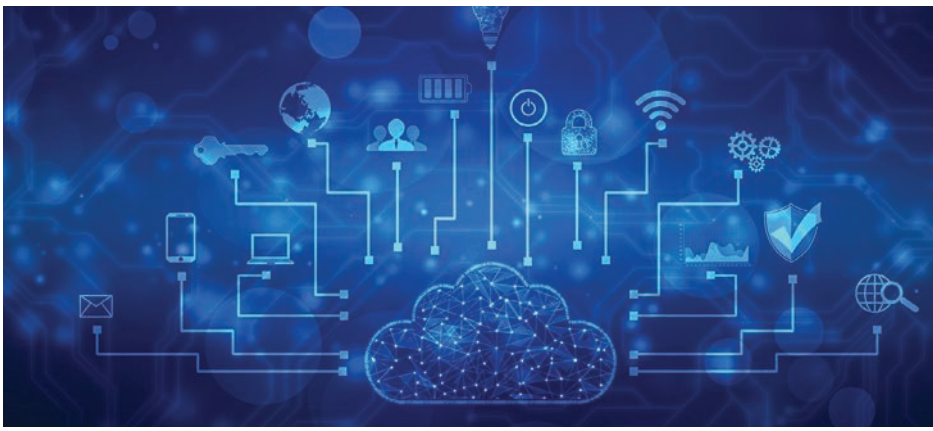
A In the early days of cloud computing, a cloud symbol was used to represent computers placed on networks out of the boundary of organization. This is likely the origin of the term "cloud computing" for the services available through the Internet. Based on the type of services offered, there are different types of cloud services available, and organizations should consider which model is most suitable for their business.

Primarily, cloud computing is an outsourcing service model and has become popular due to multiple benefits organizations can derive from using cloud-based services. Those benefits include:

- **Scalability**—CSPs offer scalable computing environments and often include pay-as-you-use models, which help organizations handle increased volumes of data processing without investing in nonproductive computing capacity and without impacting performance.
- **Affordability**—Organizations need not invest in costly infrastructure and incur costs for maintaining that infrastructure. CSPs offer the required computing capability on a subscription model and help save on capital expenditures, particularly for small- and medium-sized organizations.
- **Lower capital costs**—Organizations can provide unique services using large-scale computing resources from CSPs, and then nimbly add or remove IT capacity to meet peak and fluctuating service demands while only paying for actual capacity used.
- **Lower IT operating costs**—Organizations can rent added server space for a few hours at a time rather than maintain proprietary servers without worrying about upgrading their resources whenever a new application version is available. They also have the flexibility to host their virtual IT infrastructure in locations offering the lowest cost.
- **Improved operations**—Organizations can reduce the need to handle hardware or software installation or maintenance.
- **Improved business continuity planning (BCP)/disaster recovery (DR) infrastructure**—Organizations can leverage the process to create more robust disaster recovery and business continuity features and services, if properly managed.
- **Higher efficiency**—Organizations may be able to optimize their IT infrastructure and gain quick access to the computing services required.

While acknowledging the benefits of CSPs, like any other technology innovation, cloud services also have associated risk. The Cloud Security Alliance (CSA) has identified the top threats for cloud services:[1]

1. Data breaches
2. Misconfiguration and inadequate change control
3. Lack of cloud security architecture and strategy
4. Insufficient identity, credential, access and key management
5. Account hijacking
6. Insider threat



Sunil Bakshi, CISA, CRISC, CISM, CGEIT, CDPSE, ABCI, AMIIB, BS 25999LI, CEH, CISSP, ISO 27001 LA, MCA, PMP
Has worked in IT, IT governance, IS audit, information security and IT risk management. He has 40 years of experience in various positions in different industries. Currently, he is a freelance consultant in India.

7. Insecure interfaces and application programming interfaces (APIs)
8. Weak control plane
9. Meta-structure and appli-structure failures
10. Limited cloud usage visibility
11. Cloud services are also prone to attacks

These threats may result in any of the following negative consequences for organizations using cloud services:

- **Loss or theft of IP**—Some of an organization's most valuable data, IP, may be lost or stolen.
- **Noncompliance and regulatory actions**—Organizations need to comply with laws and regulatory controls, for example the US Health Insurance Portability and Accountability Act (HIPAA) for private health information, the US Family Educational Rights and Privacy Act (FERPA) for confidential student records, and some countries prohibit storing and processing resident information out of geographical boundaries. Organizations must be aware of the location of their data, who can access it and what is the level of protection. Although CSPs are responsible, organizations are accountable for compliance.
- **Loss of control over end user actions**—End users need to access data in the cloud and, with bring your own device (BYOD) and mobile workforces, many organizations risk losing control over the actions of authorized end users.
- **Malware infections that unleash a targeted attack**—Cloud services can be subject to targeted attacks resulting in data breaches. Successful attacks diminish trust and can negatively impact the reputation of an organization.
- **Contractual breaches with customers or business partners**—Contracts between organizations and CSPs should control the data flow, processing and dissemination to authorized users. Since it is another vendor relationship, contracts with CSPs must be carefully drafted and agreed on in all cases.
- **Reduced level of security**—Information security in the cloud may not be required by the organization policy. Although the CSA has defined security guidelines,[3] monitoring and getting assurance via periodic audits may be a challenging task for the organization.

How to Proceed?

Organizations that wish to subscribe to CSPs by third party need to consider the following:

- Outsourcing decisions are strategic and, as such, must be included in the overall outsourcing strategy.
- An organization-level service provider management framework and policy need to be in place.
- A central vendor management steering committee can help in addressing risk.
- Selecting a CSP must be done carefully since it may not be easy to switch the vendor in the future.
- Each service provider has unique risk factors, which means it is prudent to study the practices followed by each service provider.
- Organizations that wish to use cloud services need to have clearly defined functional and security requirements.
- The contract with a CSP must include a "right to audit" clause, and the organization must have a mechanism to execute periodic audits of vendors. Most CSPs may not agree to audits by the organization's auditor but may agree to a shared audit report. The organization must insist on SOC reports using the SSAE 18 standard by approved auditors.
- Define and monitor service level agreements.

Cloud computing is here to stay. Organizations need to manage the risk associated with hosting sensitive data offsite, which will strengthen confidence with the service provider and allow the organization to reap the benefits of using a cloud platform.

Endnotes

1 Cloud Security Alliance, "Top Threats to Cloud Computing: The Egregious 11," 6 August 2019, *https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-egregious-eleven/*
2 *Ibid*.
3 Cloud Security Alliance, Security Guidance v4.0, *https://cloudsecurityalliance.org/research/guidance/*