SaaS Recovery and Escrow Alternatives – Planning for Continuity on a Rainy Day in the Cloud

Related Professionals

Craig R. Auge

Related Services

Technology Transactions

CLIENT ALERT | 10.16.2013

Ease, simplicity, and low start-up costs are just some of the reasons customers turn to software-based "cloud" applications and services. These include software-as-a-service (SaaS), application service provider (ASP), and similar arrangements, but for simplicity these are referred to in this Alert as "SaaS."

An increasingly popular alternative to the more traditional on-premises software, delivered and licensed to a customer, the SaaS vendor's application runs on the vendor's (or the vendor's contractor's) infrastructure. Importantly, the customer's proprietary data is also typically housed on the vendor's infrastructure.

Risks to Customers

What happens when:

- the vendor's system unexpectedly goes down or is not accessible for an unacceptable period of time?
- the vendor breaches its contractual commitments to provide a fully functional, updated application?
- the vendor ceases to do business, goes bankrupt or has other financial problems?

A customer's lifeblood is the ability to access and use its applications and data. And it takes time to find an alternative vendor, negotiate a new contract, configure and implement a new solution, and migrate data.

Partial Solutions for Customers

- ***Vendor contractually commits to back-ups, redundant systems, and disaster recovery.*** For a customer, these are minimums and may help SaaS solutions to stay up and running. But they do not address all problems of service-level and support failures or the vendor's business failure. Also, because vendors will usually contract with third parties for hosting, the customer's lack of a contractual relationship with these third parties means that the customer won't be able to "get the lights back on" quickly if the vendor fails or disappears.

- ***Arranging for regular export of then-current copies of data, from vendor to customer.*** This is helpful, but not all customers have the infrastructure for this – and this does not address the ability to access and use the software. As a variant, some third-party companies offer services to receive at regular intervals and store current copies of data, but this also does not address the ability to use the software.
- ***Source-code escrow with a third-party agent.*** This is a common solution for the more traditional object-code delivery and license model, with the source code being released to the licensee upon certain release conditions. The licensee can then use the source code to support itself in the future. The first hurdle is negotiating meaningful release conditions: vendors try to keep them as limited and narrow as possible. The second hurdle is practical: most licensees do not pursue this because they would not know what to do with the source code if they got it or do not want to spend the time and money on consultants to figure it out. These problems are *magnified* for the SaaS customer, which likely turned to the SaaS vendor in the first place because it lacked in-house infrastructure and personnel. The SaaS customer would also have to find a means to get current data. Once out of escrow, it could take weeks to create a working environment with the source code and integrate and structure the data.
- ***Convert to an on-premise license model.*** Upon certain "triggering" or conversion events, such as a major or on-going service-level breach, the software in object code and the data could be delivered to the customer. If the customer has the infrastructure to host and merely selected the SaaS model for cost reasons, then this could be at least a short-term solution. But to be a long-term solution, the customer would also need source code to support itself.

Newer, More Robust Solutions for Customers

- ***Recovery-as-a-service.*** A continuous image of the SaaS application and associated data is replicated by a third-party agent's standby recovery systems, creating a mirrored solution. Like the better known three-party source-code escrow agreement, this would be a three-party arrangement among the third-party agent, the SaaS vendor, and the SaaS customer. If a triggering event occurs, such as the vendor's environment being unavailable for a certain time (e.g., 48 continuous hours) or some other failure, then the third-party's recovery environment is activated for the customer's use. This recovery environment may act as an alternative for up to some period (e.g., 60 days). If the vendor's environment comes back up, then the customer can switch back and the recovery environment can refresh the data. (Some traditional third-party escrow service providers additionally offer a service similar to this). During this recovery time, the customer can work to find and migrate to an alternative vendor application and access and extract its data.
- ***Escrow of SaaS application source code, configuration and data interchange specifications, business and customer data.*** This is a more robust variant of the traditional licensed software with source-code escrow, with the added escrowing of application-related, structured data and system configuration information that enable a re-creation of the original vendor environment. To be sure this would work if needed, testing is advisable. While this has the benefit of producing an environment like the vendor's in a shorter time than a mere source-code release, it would still require technical sophistication by the customer and, obviously, a new infrastructure for it to reside. *Note:* This could be

combined with Recovery-as-a-service, which could meet shorter-term needs until the environment is re-created.

Opportunity for Vendors

While the above solutions are centered on the customer's concerns, a SaaS vendor that anticipates and addresses these concerns may have a competitive advantage and capability to convince wary CIOs and CEOs that their continuity needs will be met. Some estimates are that 70%+ of SaaS vendors do not guarantee application continuity. Vendors seeking customer adoption of SaaS solutions for mission-critical and enterprise software must address these risks.

Best Practices

While the cost and ease of SaaS cloud services are attractive, the rainy day may come when systems go down or vendors fail. Customer continuity needs will vary, but the customer should ask the prospective SaaS vendor hard questions, plan, and ensure that contractual arrangements with the vendor and third parties reflect the desired solutions.

For more information, please contact Craig R. Auge, crauge@vorys.com, 614.464.5684.