How to Select a Hosted Communications Solution and Partner

One option to consider carefully is the advantages and costs of keeping PSTN access directly connected to onsite gateways. With the correct core solution, this can provide a different layer of survivability in the event of a data center or WAN outage. For normal operations, the signaling packets are transmitted to the hosted core, but it keeps real-time media (usually voice packets) localized to your organization's network. This provides the benefits of secure call flow, on-site call recording options, and reduced WAN requirements. However, this may cost more, and some of the enhanced call routing features may not be available.

Because the network services design is critical to meeting your business continuity needs, it must be properly matched to the capabilities of the data center, the core applications, and the disaster recovery plans of your organization.

Security

With any hosted solution, it is natural that questions arise about security issues. The hosted industry has clear awareness of these concerns and capable partners have addressed them. Even though some hosted data centers are more secure than most premises installations, it is still important to ask many questions about end-to-end security. With cloud solutions, various components are shared among customers, therefore, security needs to extend inside of the cloud, and not just at the perimeter. Questions need to be asked about the partition of customer data, and application level access. In addition, security impacts many layers of the solution, and you want to find a partner that has addressed the full set of issues.

1. How is physical access to the site controlled?
2. What are the written policies, procedures, and methods for ensuring security?
3. Are they compliant with applicable rules and regulations (such as PCI, HIPPA, etc.)?
4. Do they offer a written Service Level Agreement (SLA) that covers security concerns, risks, and liability coverage?
5. Do they offer encryption of all stored data?
6. Can all media packets (voice, video, IM, etc.) in transport be encrypted?
7. Who has access to the de-encryption keys?
8. What types of operating systems are running on the servers and how does the vendor secure them from exploits?
9. What is in place to prevent device-level exploits? This should include any locally installed gateways, data storage devices, and even the telephones.
10. What type of security exists within the applications to prevent abuse and malicious activities?
11. What security measures are in place to grant access to authorized client staff that need to access the system's management tools?
12. How does the partner protect the services from standard IP vulnerabilities, including denial-of-service attacks?

A solid solution from a quality partner will not brush over your security concerns lightly but instead will share what they do, how they do it, and how you can audit them if necessary.