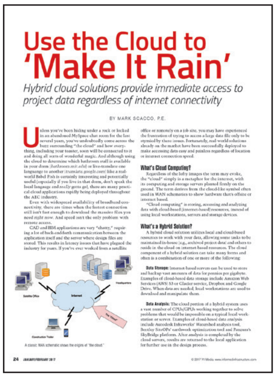
Consider Security Considerations for Cloud Computing



Use the Cloud to 'Make It Rain'

Hybrid cloud solutions provide immediate access to project data regardless of internet connectivity

BY MARK SCACCO, P.E.

Unless you've been hiding under a rock or locked in an abandoned MySpace chat room for the last several years, you've undoubtedly come across the buzz surrounding "the cloud" and how everything, including your toaster, soon will be connected to it and doing all sorts of wonderful magic. And although using the cloud to determine which bathroom stall is available in your dorm (*bathroom.mit.edu*) or live-translate one language to another (*translate.google.com*) like a real-world Babel Fish is certainly interesting and potentially useful (especially if you live in that dorm, don't speak the local language and *really* gotta go), there are many practical cloud applications rapidly being deployed throughout the AEC industry.

Even with widespread availability of broadband connectivity, there are times when the fastest connection still isn't fast enough to download the massive files you need *right now*. And speed isn't the only problem with remote access.

CAD and BIM applications are very "chatty," requiring a lot of back-and-forth communication between the application itself and the server where design files are stored. This results in latency issues that have plagued the industry for years. If you've ever worked from a satellite office or remotely on a job site, you may have experienced the frustration of trying to access a large data file only to be stymied by these issues. Fortunately, real-world solutions already on the market have been successfully deployed to make accessing data easy and painless regardless of location or internet connection speed.

What's Cloud Computing?

Regardless of the lofty images the term may evoke, the "cloud" simply is a metaphor for the internet, with its computing and storage servers planted firmly on the ground. The term derives from the cloud-like symbol often used in WAN schematics to show hardware that's offsite or internet based.

"Cloud computing" is storing, accessing and analyzing data with cloud-based (internet-based) resources, instead of using local workstations, servers and storage devices.

What's a Hybrid Solution?

A hybrid cloud solution utilizes local and cloud-based resources to work with your data, allowing some tasks to be maintained in-house (e.g., archived project data) and others to reside in the cloud on internet-based resources. The cloud component of a hybrid solution can take many forms and often is a combination of one or more of the following:

Data Storage: Internet-based servers can be used to store and backup vast amounts of data for pennies per gigabyte. Examples of cloud-based data storage include Amazon Web Services (AWS) S3 or Glacier service, Dropbox and Google Drive. When data are needed, local workstations are used to download and manipulate them.

Data Analysis: The cloud portion of a hybrid system uses a vast number of CPUs/GPUs working together to solve problems that would be impossible on a typical local workstation or server. Examples of cloud-based data analysis include Autodesk Infraworks' Watershed analysis tool, Bentley SiteOPs' earthwork optimization tool and Panzura's SkyBridge platform. After analysis is completed by the cloud servers, results are returned to the local application for further use in the design process.

A classic WAN schematic shows the origins of "the cloud."

24 JANUARY/FEBRUARY 2017

© 2017 V1 Media, www.informedinfrastructure.com

For decades, engineers have been wrestling with the challenges of digital communications among the home office, the client's office, subcontractor sites and remote work sites. Larger engineering firms have whole work groups focused on establishing and maintaining reliable data paths, using methods such as satellite links, leased private channels and even the public internet. Often, medium and small engineering organizations rely on the heroic efforts of one or two dedicated employees who labor to learn new networking disciplines, struggle to decipher arcane communications protocols, and stretch to negotiate complex service agreements that ensure digital communications are reliable.

Cloud computing offers services that are attractive to engineers. Cloud vendors offer products such as enhanced digital communications among engineers and clients as well as between inhouse and onsite personnel. Cloud vendors also offer flexible data storage capacity that can scale quickly as workloads change. In addition, cloud vendors offer flexible data-processing options that include engineering analysis software, sophisticated database services and back-office support programs. Highly rated cloud vendors also offer security services such as integrated data encryption, data access controls and data activity logs, and vigorous backup procedures.

> You wouldn't put all your eggs in one basket. You shouldn't put all your eggs in one cloud. By the way, where do you keep your golden eggs?

Indeed, the cloud offers valuable benefits, but it doesn't provide unqualified benefits. The requirements for due diligence and business survival never go away. Businesses need to establish basic security procedures independent of the cloud. Both critical and convenient data must be backed up and maintained well offsite. A healthy business must be ready to survive fires, tornadoes, rogue hackers, disgruntled employees, careless subcontractors and other threats. Backup procedures must be tested at least yearly, depending on risk.

Do not include information in the cloud that doesn't absolutely need to be there. Businesses need to explicitly consider all the categories of their intellectual property and the different risks that different categories represent. Keep in mind that mixed in with your proprietary data is client information, employee and subcontractor data, and regulatory agency communications. Along with your engineering work products, you have marketing plans, investor communications, financial transactions, project management details and legal correspondence. The cloud can augment your security precautions, but the cloud is not a substitute for your own data backup, under your direct and persistent control.

Follow the notion long used in the banking industry by delineating separation of duties. Compartmentalize access by the need to know. Collaborate with the cloud vendor to exploit available security options, such as encryption, password management and granular permissions. During project execution, many individuals will be accessing project data, but usually only the highest-level security administrator needs to access all the project data for a project of any significant size. Even at that level, controls can be established to minimize risk. Keep in mind that it was the insider Edward Snowden, a former CIA employee, who copied and leaked massive amounts of classified information from the National Security Agency in 2013.

The higher an individual's scope of access, the more often their passwords should change. If possible, implement two-factor sign-on. Multifactor authentication, in one form, requires anyone logging into a network to be in physical possession of a chip-enhanced ID card that correlates with their username and password. Multifactor authentication with frequent password changes could have thwarted a Sony hack in 2014, for example, that was carried out across international borders.

Cloud services charge for the resources consumed, including data storage, network bandwidth consumed, software products utilized, consulting support and various add-on products. Different cloud vendors bundle their services in different ways for billing purposes. Nevertheless, the fewer resources used, the lower the cost.

Do not include information in the cloud that no longer needs to be there. When a project is completed and all the paperwork is resolved, take that project data off the cloud. If the cloud vendor also holds transaction logs concerning the project, download and retain those as well. Project activity logs can be useful for investigating subsequently discovered security breaches. Logs may also be useful for establishing a responsive position if regulatory or litigation issues arise. In any event, make sure that the cloud vendor also purges your proprietary data from their systems, including their backup files. The less time data remains on the cloud, the less time it's exposed to hacking.

These comments are intended as a reminder of some of the considerations and tradeoffs surrounding data security in the era of cloud computing. The cloud has an important role to play in carrying out many engineering projects. Nevertheless, it remains prudent to periodically reexamine the risks and economies associated with the cloud.

Andrew Newport
Information Systems Group Leader (retired)
Sargent Lundy
anewport@aol.com

Please send comments and letters to:
Todd Danielson *tdanielson@v1-media.com* or
Kevin Carmody *kcarmody@v1-media.com*

Traditional mail:
attn: Todd Danielson
1441 S Plymouth Ct., Suite H
Chicago, IL 60605