



EDISCOVERY IN THE CLOUD: A NIGHTMARE SCENARIO

Your company uses cloud computing as a cost-effective element of its business operations. And then one day your company is sued. What are the implications?

By James Berriman and Jack Notarangelo

EDISCOVERY AND THE TRADITIONAL CORPORATE NETWORK

In a legal dispute, the term “discovery” describes the process of collecting, reviewing, selecting, and producing to your opponent the documents relevant to the dispute. Companies are required to conduct discovery in good faith. Failure to comply can result in severe sanctions.

The term “electronic discov-

ery” (or “ediscovery”) simply refers to discovery in the context of electronically-stored information. The great majority of business records are now electronic rather than paper, so parties must, of course, produce relevant electronic documents as well as paper documents.

Until recently, ediscovery was conducted almost entirely within the context of the corporate network. Relevant company documents were expected to reside somewhere within the four corners of that

network. The primary issue was how to find those documents in a cost-effective way, since corporate repositories can be enormous and the percentage of relevant documents may be very small.

The usual approach was to narrow the scope by first identifying the employees involved in the dispute. Those employees are called the “relevant custodians” because they are likely to have custody of relevant company documents. Relevant custodians typically have accounts on the company network. Their logon credentials define and limit their rights.

On a corporate network, therefore, the scope of ediscovery can generally be limited to repositories accessible to the relevant custodians: their mailboxes on the mail server, their file shares on the file server, the group shares to which they have permissions, their local workstation files, etc.

Those repositories can be further narrowed with keyword filtering and other objective criteria. The end result is a relatively small subset of potentially-responsive files that can be cost-effectively reviewed by counsel in preparation for production to the opponent. This approach greatly reduces the scope and cost of ediscovery. Also, because it occurs within the company network, it can be consistent with the company’s document retention and destruction policies since those policies determine what is on the network in the first instance.

And that is how ediscovery has typically been conducted in the traditional network context. But now comes the cloud. With the advent of cloud-based document repositories and data, what happens when the next lawsuit arrives? What situations should a company anticipate when it embarks on cloud computing?

Below is a hypothetical scenario to highlight these issues and risks.

GOING ROGUE

The leadership within a certain division -- let’s call it the BizDev division -- was entrepreneurial by nature. BizDev was impatient with corporate red tape. Capital expenditures and initiatives were difficult to get approved. BizDev wanted to move faster than the bureaucracy would support.

Being entrepreneurial, innovation came naturally to the BizDev leadership team. On its own initiative, it began looking for outside solutions to its bureaucratic woes. The BizDev team explored outsourcing certain operations to the cloud. Not only would the implementation be

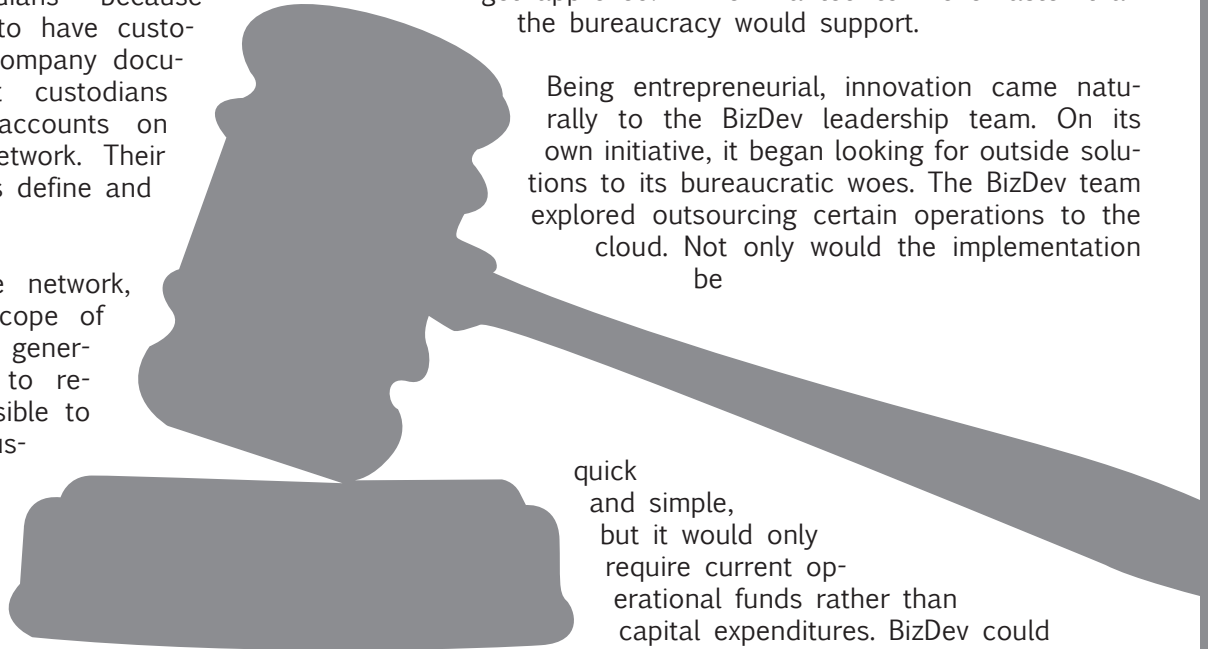
quick and simple, but it would only require current operational funds rather than capital expenditures. BizDev could therefore bypass the formal procedures normally required by the company for major initiatives.

BizDev was going rogue.

BizDev specializes in content management. It has significant storage requirements. So it looked to Infrastructure as a Service (IaaS) to solve its storage problem. IaaS would provide the ability to increase and decrease storage requirements in a self-service way with virtually no red tape.

The BizDev team saw this as a no-brainer. After a relatively quick selection process, it contracted with a vendor and began using the services shortly thereafter.

The gambit paid off. Over the course of several years, BizDev’s use of content management providers became more sophisticated. It began using different vendors for different collections based on cost and functionality related to specific media. Soon its content was spread among several IaaS vendors.



THE ROGUE BECOMES THE NORM

Word of BizDev's success in the cloud spread throughout the company. Other divisions quietly began to implement similar approaches.

The sales force, dissatisfied with the limits of the company's remote access resources, began using web mail accounts when on the road with their laptops. They began using "FTP in the Cloud" to transmit proposals and other bulky documents that exceeded the quotas imposed by the company mail server. They began using online collaborative document tools to share access to sales documents with their customers. They began drafting and revising proposals jointly, sometimes with multiple customer representatives.

The company's marketing department had always complained about insufficient network resources for graphics and video development. So they began using cloud-based storage and development tools. To work around a limited media budget, they began releasing trendy marketing videos on a well-known web-based video repository site.

Other divisions expanded the company's use of the cloud by encouraging employees to blog regarding the company's activities and services. Employees were free to use the service of their choice. They were also encouraged to use as many of the available networking sites as possible to generate buzz and to drive traffic to the company's site.

As cloud-based initiatives proliferated, there was some apprehension within the company about the lack of governance and oversight. The CIO was concerned that so much company data was distributed across third-party services and no longer under the control of the IT department. The general counsel was concerned that cloud repositories were not being maintained in accordance with the company's retention and destruction policies, especially in light of employee turnover and occasional changes in vendors.

But there was no appetite at the company to take on the task of implementing company-wide protocols and standards for cloud computing. The use of cloud services was now widespread and was providing the company with significant benefits in cost reduction, flexibility, and speed to market. The cloud was considered a boon to efficiency that dramatically improved the organization.

THE LAWSUIT

And then one day the company was sued. A large law firm known for its aggressive litigation style commenced a class-action lawsuit against the company based on multiple counts of alleged fraud in connection with certain business deals, profit forecasts, and representations made to shareholders and customers. The relevant time period went back several years.

The plaintiffs demanded discovery of a wide range of business records: all marketing materials for the relevant time period; all public statements made by company representatives on topics relevant to the allegations; all communications between members of the sales force and certain customers; all drafts of proposals; and various other items related to the allegations.

The nightmare had begun.

In the traditional ediscovery model, the approach would have been straightforward: identify the relevant custodians (including departed custodians), identify the pertinent document collections associated with those custodians (mailboxes, personal file shares, group shares, etc.), and then begin indexing and culling the responsive collections in preparation for review and production. For historic documents that might no longer exist on the active servers (such as mailboxes and file shares of departed employees), this process could include the selective restoration of corporate archives for the relevant time period.

But this model would no longer work for the company. During the course of discovery, the company encountered the following problems:

- There was no one at the company with overall knowledge of how the company's cloud repositories were organized. There was no "data map" of the company's outsourced collections.
- There was no way to index, search, and cull those scattered repositories in an integrated way.
- There was no way to perform efficient server-level "batch" operations on the outsourced repositories because they could only be accessed through limited end-user interfaces.
- There were generally no historic archives of the outsourced collections. At most, there were only short-term disaster recovery backups maintained by some vendors.
- There were no historic archives of web mail

contents other than the current contents. There was no way to recover the mailbox contents of long-departed employees who had used web mail rather than the company mail system.

- Different employees used different web mail systems so there was no efficient way to collect and search across their current mailboxes as could have been done on the company mail server.
- For collaborative document systems, there were no archival copies of earlier drafts. There was no record of what had initially be provided to the customers. There was no way to prove who had accessed the documents and when, or to determine which collaborator might have made which edits to which documents.
- Old content had expired on some of the blogs and networking sites on which employees had posted. As a result, there was no way to verify or disprove some of the allegations made by the plaintiff regarding public statements.
- The company had no way to “lock down” some of the outsourced repositories to ensure that the contents were preserved pending collection. This was a concern because the company believed that a few of its employees might have an incentive to alter or purge evidence to cover their tracks. It was also a concern for sites that allowed third parties to alter the contents.
- Obtaining copies of outsourced repositories sometimes required protracted administrative processes with vendors over which the company had no direct control.

... cloud computing services must still be managed as an essential part of the company's business operations. Outsourcing the responsibility for the infrastructure does not mean outsourcing the responsibility for the content.

WHAT IS THE MESSAGE?

As daunting as these problems may appear, this scenario is not intended to discourage companies from using the cloud. The cloud is becoming, and will continue to be, a rational direction for cost-effective and scalable solutions to common business problems.

Rather, this scenario is intended to remind companies that cloud computing services must still be managed as an essential part of the company's business operations. Outsourcing the responsibility for the infrastructure does not mean outsourcing the responsibility for the content.

Litigation preparedness, corporate records retention, and electronic records management are much easier to address as part of the initial selection and implementation of a new system or service. If the appropriate controls and protocols are in place from the outset, a company may never be faced with its own “nightmare scenario.” ■