How the IT department can prep for the courtroom

by Greg Lawn, manager of technical integration services, Attenex Corp.

There has been a steady increase in corporate litigation over the past decade, and those legal proceedings are having an unforeseen impact on IT managers. This trend has been accelerated by the recent changes in the Federal Rules of Civil Procedure (FRCP).

The mountains of electronic data generated within today's enterprises are colliding with ever more aggressive legal discovery practices, creating formidable IT challenges during litigation — how to best provide secure and auditable access to sensitive corporate data that must otherwise remain inaccessible to both outsiders and most insiders. More importantly, how can control be maintained without exposing more corporate data than necessary?

These decisions are best shared between the network or IT manager, corporate counsel and a litigation support specialist, who will help identify and specify the appropriate data. But it's the IT manager's job to ensure that data is treated gingerly; enterprises don't spend millions on network security only to offer up the corporate jewels at the first lawsuit.

At the same time, there are legal requirements for both inside and outside counsel to have unfettered access to the relevant corporate data at a level of detail that corporations never allow outsiders under different circumstances. To balance these concerns, corporations are increasingly bringing this process of identifying what is relevant and appropriate for disclosure in-house. They will still likely use outside law firms and possibly contract attorneys to make the determination of relevance, but today's litigation-burdened corporation is taking control of the data and, in the process, reducing the cost of discovery.

The legal strategies aside, there are two fundamental IT strategies that lie at opposite ends of the spectrum for providing this "access to the inaccessible." The first is to outsource the data and security to a service provider whose business is handling the litigation discovery process. These companies have the facilities, policies and tools necessary to secure the data while providing auditable access for the attorneys. In fact, some can even provide multi-terabyte "mobile data centers" that can be wheeled in to quickly host a whole legal department.

At the other end of the spectrum is a physical security approach, with the company literally walling off — physically — a copy of the data behind a lock and key. This is typically done in a conference or training room facility inside the corporation. This mini-network is physically disconnected from the web and the corporate network, and all of the attorneys are brought "in house" for data access throughout the duration of the review process.

Both of these approaches work well (either outsourcing it to someone else's plate or through avoiding access concerns by eliminating the network connection) and can dramatically simplify the IT problem. Unfortunately, each also has obvious inefficiencies and added costs. As a simple example, the physical walling off becomes difficult when the data and facilities are in Los Angeles and the attorneys are in New York.

The real challenge lies in finding a middle ground: isolating the data internally on the network and allowing controlled and auditable remote access for review attorneys. This approach typically necessitates the creation of the networking equivalent of a demilitarized zone (DMZ) for all data processing that is neither "inside" the corporate data network nor "outside" the corporate firewall. This DMZ needs to be protected from both outside and inside access, since it will contain a wealth of sensitive data that typical employees should not be able to access.

Getting the data into this DMZ is the first challenge, especially since it can be hundreds of gigabytes or even many terabytes in size. While setting up electronic transfer is possible, it adds complexity and additional components that must be secured. Often the fastest solution is to physically iso-

"How can control be maintained without exposing more corporate data than necessary?"

— Greg Lawn

late the network from internal corporate networks. This makes transferring data a bit more cumbersome as portable drives must be used, but it gets the data where it's needed in a hurry. Data access can then be handled physically as well, with attorneys using the computers on the subnet, or more typically, through a remote access strategy.

This secure remote access is usually accomplished via a multi-tier approach, wherein the presentation layer is handled under the auspices of the DMZ, while the application and data layers remain inside the protected network. This inner protected network falls into one of three categories:

An isolated network: This is similar to the physically isolated network described above, but allows the review attorneys to be in remote offices instead of jammed into a single room.

Another DMZ: This technique embodies the "defense-in-depth" approach preferred by security analysts. This inner DMZ may indeed be an isolated network. The corporate network: Leveraging their corporate investment in advanced networking equipment and expertise, some corporations will bring the remote access traffic directly into their network and control what the remote user has access to by using networking policies and profiles.

Access privileges under these scenarios are typically handled through the use of sophisticated port-level traffic routing and policy rules, allowing or disallowing access at the protocol level. In this instance, traffic from any outside counsel will be brought in at the protocol level and dropped onto a specific subnet that contains the presentation-layer access to relevant corporate legal discovery data.

Common to all of these approaches are two enabling technologies: a remote presentation technology and a robust secured identification and authentication technology. In all remote access cases, there needs to be strong authentication – typically in the form of tokens requiring a time-synchronized passcode in addition to user ID and password protection.

No one wants to see his or her company involved in a lawsuit. Yet in this litigious age, it is certainly not uncommon. Just as certainly, it will create as many headaches for the IT department as for the executives and lawyers. It may even be worthwhile to take a preemptive approach and spend a little time talking with in-house counsel to sketch out a plan of attack. By having a better understanding of the requirements, it might be possible to tip the scales of justice in your favor.

Every e-discovery request is unique, but the one thing that is always consistent is that you will be surprised by the request and have very little time to respond to it. The only way to prepare is to think ahead and plan for the inevitable. Five points for IT managers to consider when preparing for e-discovery:

1. How much data will need to be made available? Who is collecting it and how is it to be preserved and reviewed?
2. For security purposes, are you outsourcing the data, physically isolating it or using a DMZ?
3. What method of network security will you employ?
4. Will a single DMZ be sufficient or will you need to adopt a defense in depth approach?
5. How are you allowing remote access, if necessary? Are you using tokens for security?

Greg Lawn is the manager of technical integration services for Attenex Corp.

"The only way to prepare is to think ahead and plan for the inevitable."

— Greg Lawn