AS SEEN IN Upsize Minnesota

How to handle e-discovery before and after disputes

GROWING BUSINESSES face many challenges, one of which is that their computer data probably is growing quickly but may receive little oversight.

Adopting a largely paperless business model can help fuel growth, but to effectively manage the risks from this data, owners and managers need to be aware of and anticipate electronic discovery (e-discovery).

E-discovery is a pre-trial process in which parties in litigation must locate their relevant computer data and disclose it to one other. This process can be time-consuming and expensive because e-data has become ubiquitous in most businesses. Also, the media continue to report serious data destruction errors by parties that haven't kept their electronic houses in order.

The best time to prepare for e-discovery is before a legal dispute is on the horizon, and the steps described below will help businesses address this subject.

[tips]

1 | Failing to preserve relevant e-data risks incurring costly fines and bad publicity if a suit arises.

2 | As soon as you get notice of a legal claim, send a litigation hold notice to all employees and outside IT consultants serving your business.

3 | The preservation notice must describe what kinds of files must be preserved and tell personnel to stop all destruction of such data.

4 | You must also follow up individually with key employees who are likely to have relevant e-files on the subject of the dispute.

Before disputes arise

•Set and consistently follow an e-data retention policy that is reasonable for your business, and educate employees about your policy and the reasons for it.

You should determine how long you need to keep each type of e-record for business reasons and due to legal or regulatory requirements. Your business may have many kinds of e-records (contracts, purchase orders, invoices, financial records, databases, notes and correspondence, among others), and different types may warrant different holding periods.

Remember though, that such a policy is not a license to selectively discard "bad files" just before anticipated litigation. Further, you should periodically revisit how well your chosen policy is being followed and is working.

• Use disaster backups only for that purpose and rotate them often.

When deciding what burdens to impose on businesses to restore and produce their backup files, courts usually consider the accessibility and cost and ease of finding relevant e-data in backups. Since it is usually expensive

CHARLES STUBBS

and time-consuming to restore data from traditional backup tapes, small businesses should consider using other backup media.

Even more important, you should never use a disaster backup for any other purpose (such as for reference or archives). Instead, you should use disaster backups strictly for disaster recovery in order to support the position that your business shouldn't be required to bear the cost of searching through them and restoring such data in response to an opponent's demands.

Also, you shouldn't keep any particular disaster backup longer than needed (unless already ordered or demanded in litigation). Instead, rotate backups on a workable and consistent schedule, so if future litigation does require you to restore and produce data from backups, you have built in limits to that burden.

• Be aware of the vendor market.

There are many e-discovery vendors, and they offer a wide array of services, such as project management, computer forensics, data storage, software and strategic planning, among others. However, one vendor probably will not be the best fit for all needs, and your needs will depend on the nature of each suit.

As part of pre-crisis planning, it is useful to research a range of vendors, but this step is premature for small businesses with no litigation history. However, small-business managers can contact their outside accountants and legal counsel to find out what vendors they have worked with and recommend. Ultimately, let your outside legal counsel retain and direct the vendor to preserve legal privileges.

Disputes happen

•Immediately secure and preserve all relevant e-data when litigation is imminent or starts.

Failing to preserve relevant e-data risks incurring costly fines and bad publicity and may trigger court instructions that a jury can infer that the destroyed evidence would have been damaging to the party that didn't preserve it.

An effective preservation process requires that as soon as you get notice of a legal claim, you should send a litigation hold notice to all employees and outside IT consultants serving your business, and then you must follow up with reminders and check compliance.

The preservation notice must describe what kinds of files must be preserved and tell personnel to stop all destruction of such data. You must also follow up individually with key employees who are likely to have relevant e-files on the subject of the dispute.

Depending on the nature of the litigation, the next preservation steps may include having an outside expert create forensic images of key data systems in order to preserve relevant data. For many businesses, this includes imaging at least some personal computer hard drives, e-mail servers, and voicemail servers.

If forensic data collection is necessary, trained, experienced professionals should handle it and maintain a proper chain of custody of the data. Finally, be sure to document your preservation steps in writing, and remember to lift the legal hold after the litigation ends.

•Build good communications with your litigation attorneys from the start.

Most of the e-discovery lapses for which courts have punished litigants resulted from poor attorney-client communications. To avoid those problems, the attorneys representing your business will need to learn how your business keeps e-data. This will enable them to effectively advise you and advocate for your interests in managing and conducting e-discovery.

This means that your IT personnel must educate your attorneys about the details of your data creation and storage practices. Good communications and coordination between your personnel and your attorneys will be essential as the case progresses.

• Consider e-discovery negotiation strategies early.

The e-discovery process in litigation normally is a two-way street. Because e-discovery can be very expensive and time-consuming, businesses should try to negotiate with opponents to narrow e-discovery to reasonable boundaries. Indeed, most courts require parties to take that step before any court relief is granted.

Options may include working out sampling protocols to test the cost/benefit of retrieving certain types of e-data and determining the best formats in which to disclose e-files (such as native format, pdf, or TIFF). These and various other topics should be considered to balance the competing goals of safeguarding, finding and producing relevant e-data to opposing parties while keeping costs within reasonable limits.

[quote]

"The best time to prepare for electronic discovery is before a legal dispute is on the horizon."

— Steve Marino, Altera Law Group

[contact]

Steve Marino is of counsel with **Altera Law Group** in Eden Prairie and handles business disputes and commercial litigation: 952.253.4122; smarino@alteralaw.com; www.alteralaw.com