

CyberBytes



Subject: Reluctance to Adopt Data Forensics is Too Costly

Back in early May, we quoted Judge Sidney Schenkier of the U.S. District Court for Northern Illinois, who shared his observations at an e-discovery conference in Chicago as to why he believed many attorneys shy away from utilizing comprehensive data forensics in their cases.

Of the two primary reasons for attorney reluctance cited by Judge Schenkier, the anticipation of a retaliatory e-discovery attack upon the original requesting party by the producing party may be the most significant contributor. The “boomerang effect” in effect leads opposing counsel into the unspoken quid pro quo arrangement of letting sleeping dogs lie. After all, why would an attorney knowingly put his/her client into harms way, when it would be easier to avoid the whole mess by settling for whatever scraps of documentation and e-mails the producing party is able to come with?

When you consider that this line of thinking with particularity to e-discovery and data forensics is quite common amongst attorneys who understand only the dangers of the unknown, it actually almost makes sense. But then again, most attorneys who are stymied by launching an e-discovery attack just haven't spent enough time analyzing what's really going on here.

Plaintiff attorneys enjoy the advantage of timing their lawsuit filing when they want to. With this time advantage an attorney has the ability to plan for the

potential of a retaliatory e-discovery request upon the client, so that when it arrives everyone can stay calm and focused on the lawsuit. We have written extensively on this pre-filing preparation stage; see [The Boomerang Effect](#) and [E-Discovery Checklist and Harnessing Digital Evidence](#).

For the Producing Party's attorney, one of the most serious challenges in dealing with e-discovery requests is the potential for inadvertent spoliation of electronic data in commercial litigation. CyberControls provides a cost efficient, fail safe approach to eliminating this area of vulnerability, see [Data Discovery-Just Beneath the Surface](#) and [Mitigating areas of Risk in E-Evidence Production](#).

There is no doubt that the reliance upon digital evidence will only be increasing over time. Learning how to find digital evidence, to recover it, and preserve it are all things that CyberControls can assist you with where ever you are located. Whether you represent the discovering party or the producing party, data forensic support is becoming an absolute necessity in protecting the interests of your client.

We're prepared to discuss your particular situation with absolute confidence and discretion to help you determine whether there is a fit. We can be reached at 847-756-4890 or at www.cybercontrols.net .