My colleague and friend Prof Don Holden, MBA, CISSP-ISSMP noted a gap in the discussion of e-mail in our MSIA course some time ago and has graciously allowed us to print an edited version of his comments to students on the subject of e-mail retention. The remainder of today’s column and the next one are a collaboration with Don.

* * *

One of the big factors driving proper retention and destruction of e-mail is that e-mails are discoverable evidence in both civil procedures as well as criminal investigations. Retention of e-mail and other unstructured content such as instant messaging is also required in certain industries, particularly in the financial industries where brokerage house have been fined millions of dollars for failure to produce e-mails in a timely fashion. For example, Morgan Stanley was fined $15 million by the Securities & Exchange Commission for failing to produce e-mail messages promptly in response to court-authorized demands for evidentiary discovery. Evidence showed that company officers lied about the availability of backups and inflated the costs associated with e-mail retrieval. Morgan Stanley also had to pay Ronald Perelman $1.5 billion due in part to its failure to completely comply with a civil discovery order related to Morgan Stanley’s role in the Sunbeam bankruptcy. <http://tinyurl.com/f4e8y> This case is also a good example of how lack of ethics can have big costs.

The Federal Rules of Civil Procedure (FRCP) specifically address discovery and the duty to disclose evidence in preparation for trial. There are new guidelines for cyber discovery which took effect in December 2006 in the FRCP. Rule 26(b)(2)(B) specifically allows exemptions for electronic evidence: “A party need not provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost. On motion to compel discovery or for a protective order, the party from whom discovery is sought must show that the information is not reasonably accessible because of undue burden or cost. If that showing is made, the court may nonetheless order discovery from such sources if the requesting party shows good cause….” <http://www.law.cornell.edu/rules/frcp/Rule26.htm> Rule 34(a) specifically allows a party to demand physical access to records for discovery of specific information as stipulated by the court order. <http://www.law.cornell.edu/rules/frcp/Rule34.htm> In other words, if an organization protests that it cannot produce needed evidence, third parties may be burrowing through their facilities looking for that evidence, with all kinds of unexpected and possibly expensive or embarrassing consequences.

In our next column, we’ll conclude with a review of some practical pointers for readers to avoid trouble with e-mail retention.

* * *

For further reading:

***


M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance <http://www.msia.norwich.edu> at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mekabay@gmail.com>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2007 Don Holden & M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.