E-mail Retention Policies (2)

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

In the previous column, my friend and colleague Prof Don Holden, MBA, CISSP-ISSMP and I reviewed some of the issues arising from pre-trial discovery orders involving stored e-mail and e-mail archives.

As we looked through several articles on the subject and thought about the issues, we put together the following list of practical pointers for readers:

- Define, enforce and update formal retention policies that stipulate how long to keep archives of which types of data. Ensure that your legal counsel is deeply involved in setting these policies.

- Access to archived records should be completed within at most 48 hours to avoid possible fines.

- Deleting e-mail and other records that show evidence of wrong-doing may lead to worse legal and public-relations consequences than coming clean.

- Unscheduled deletion of e-mail may destroy exculpatory evidence or lead to a tacit presumption of guilt.

- E-mail archives on servers must be safeguarded against any modification that could distort the record and lead to prosecution for tampering with evidence. Chained checksums or digital signatures involving timestamps can reveal such tampering.

- Metadata are the data about your data such as log files showing who accessed or modified files or records. Metadata are increasingly being seized in discovery as well and must be maintained properly.

- Tools that scrub metadata for security purposes can also be used to hide legitimate audit trails and need to be controlled or monitored. Examples include destruction of the track-changes records in word-processing and spreadsheet files known to be significant in a legal discovery process or deliberate copy/paste operations from a source that included an audit trail into plain-text format. No employee should be destroying data in this way when a subpoena or other discovery process is in force; data security policies should make such restrictions explicit.

- Ensure that you know exactly what is on each backup medium and where it is stored. Use appropriate software to catalog your backup media. Stored media must be kept in secured facilities with chain-of-custody records that ensure that the organization can report exactly who accessed which media at any time.

- Disaster-recovery media may be required under subpoena just as regular backup media
are; be sure to include them in your catalogs and access lists.

- Think carefully about whether to allow employees to store corporate e-mail on external servers such as those of GMAIL. For example, should employees be allowed to auto-forward corporate e-mail to such a private account? Corporate network administrators are unlikely to be able to access the stored e-mail on an employee’s private account; furthermore, e-mail stored on a server of this sort could be made available to law-enforcement authorities without a warrant after 180 days according to 18 USC §2703(a). <http://www4.law.cornell.edu/uscode/html/uscode18/usc_sec_18_0002703----000-.html> The files could even be transferred to another owner if GOOGLE decided to sell its e-mail services. In addition, the Privacy Policy explicitly warns, “Residual copies of deleted messages and accounts may take up to 60 days to be deleted from our active servers and may remain in our offline backup systems.” <http://mail.google.com/mail/help/privacy.html>

***

For Further Reading


Metadata emerging as a vital component of e-discovery. _eMag Link_ <http://www.emaglink.com/newsletter_archive/newsletter_May_2006.htm#two>


***


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 M. E. Kabay & Don Holden. 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.