Benjamin Wright is an old friend and colleague whose work on _The Law of Electronic Commerce_ stands as a key reference work in the field of Internet law. He recently sent me a copy of his short text on _Business Law and Computer Security_ and I’m delighted to recommend it wholeheartedly as an excellent overview that readers will appreciate for its clarity and thoroughness. In addition, the slides shown in the book will be useful to anyone preparing a lecture on any of the important topics covered.

Attorney Wright begins with a short introduction explaining that the book is based on a course intended for non-lawyers and focused on practical issues. He touches on the notion of vicarious liability (sometimes called “downstream liability”): the doctrine that punishes failure of due diligence in preventing abuse of systems to result in penalties on the victim of that abuse if others are harmed.

Another critical issue is proper records management. Wright suggests that the old habits of destroying paper records after a relatively short time should be changed now that we have electronic records storage. Records can be kept until they become obsolete, he says. Data can be converted to new formats for a few cycles of change but then reasonably discarded when the costs outweigh the benefits of conversion. Instead of destroying data based on content, the new policies should discard data simply according to age. However, e-mail, in particular, may have to be kept longer than other types of electronic records because juries are so suspicious of e-mail destruction. No records should be destroyed when litigation is threatened or pending for fear of causing trouble in court.

The next section looks at legal requirements for security, control and privacy. As all policy experts do, Wright warns of the importance of clarity, understanding monitoring, and consistency of enforcement in managing security policies. One of the many practical suggestions: if system administrators discover forbidden software on a network or workstation, they can replace the executable with a warning that pops up when the abuser tries to activate the “pest:” “Security personnel have discovered and removed [describe malicious code]. Acme will reprimand or prosecute you if you place other unauthorized programs on this system.”

The other sections of this useful book cover

* information privacy,
* computer evidence, authentication and signatures,
* electronic signatures and authentication,
* electronic contracts, and
* homeland security and information sharing.

The book is attractively printed and inexpensive and could easily be used in a series of lunchtime meetings to introduce legal staff to computer security issues and network administration staff to legal issues.
Good job, Ben!

* * *

For further reading:


* * *


M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mkabay@norwich.edu>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2004 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.