

SURVIVAL ON THE E-MAIL & E-DOCUMENT LANDSCAPE

COPING WITH ELECTRONIC TERRORISM

By Al Harrison
Harrison & Egbert
VirtuAl@hypercon.com

Houston Bar Association
Computer & Online Law Section
January 27, 2000

Introduction

Having the ability to practice law in Cyberspace has virtually metamorphosed the legal landscape into an amorphous mass. This amorphous mass is actually populated with an underlying structure of well-established legal principles and practices blanketed with a colloidal covering. Besides compelling changes in the manner in which legal services are delivered, this has introduced a plethora of ethical concerns for lawyers and law firms.

Consider the following questions: With whom are you communicating by sending email? Are you inadvertently providing legal advice to an unknown person in an unknown venue? For free? Have you inadvertently established an attorney-client relationship? Are you licensed in the state in which the recipient resides? Do you routinely check all incoming electronic data for viruses? Do you exercise diligence safeguarding your firm and client information stored on your network? Is encryption prerequisite for safeguarding such information? Passwords? Biometrics? Do you simply “logically” delete obsolete confidential information stored on your hard disks or the like, or do you shred it? What is the standard for the duty of care associated with practicing law on the electronic landscape?

Venturing into Cyberspace is easy to effectuate: one simply need be positioned proximal to a keyboard and pointer device, and then interact with the operating system and application (browser or email or news-reader or chat) software. Nevertheless, as members of the legal profession are rapidly discovering, this ease of entry has the potential to drastically affect peace of mind and integrity of practice.

“E” Whatever

The Internet continues to permeate modern life as we know it as a diversity of activities and transactions migrate into Cyberspace. The prefix “e” is becoming a standard preface for virtually everything. For what does this conspicuous “e” (or is it “E”) stand? Electronic? Extraordinary? Erratic? Emerging? Emergency? Extraneous? Extemporaneous? Ephemeral? Whatever “e” applies in a particular circumstance, the information will be disseminated via a distribution system that is virtually infinite in geographical scope — and that traverses time barriers.

Email, of course, may be forwarded at the sender’s convenience and whim. Similarly, email may be read at the recipient’s convenience and whim. Indeed,

a(n incipient) recipient may elect not to read an incoming email, and delete it. If an email is accompanied by one or more attached files, a recipient has the option to open this file and then read it. Computer viruses may, unfortunately, be present in an attached file. Viral behavior may be propagated by merely receiving an email. Similarly, viruses may be introduced via downloads from Web sites or during chat sessions. Some of the newer varieties of electronic infections behave unpredictably, perhaps more like a flu-like condition than a virus.

A computer virus is essentially a prevalent form of electronic terrorism that may alter the normal operation of computer programs, modify or destroy data, and potentially eradicate the contents of a hard disk. In the context of the Internet or corporate intranets, virus are particularly dangerous because its Cyberscape provides an inherently fertile landscape for rapidly propagating any form of electronic invasion.

A computer virus is a malicious self-replicating computer program that infects a target or host file by attaching thereto. Generally, by thus attaching to an executable file, driver, or document template, such a virus adversely affects the behavior of the underlying application or operating system computer programs. Not unlike a viral infection of a human, a computer virus metamorphoses a normal executable file — a computer program that performs predefined functions — into a carrier of infection. Once this carrier file is executed, the virus may be replicated, typically without affording time for recovery procedures to be effectuated. Thus, akin to a communicable infection, propagation occurs when this virus encounters predisposed host sites: a computer virus is typically targeted to strike an executable program such as Microsoft Word, a driver such as a driver for a particular hardware device, or a document format such as a Microsoft Word or Excel file. Viruses are typically introduced onto a host site via a file copied from a diskette or downloaded from the Internet.

The modus operandi for invasion by a computer virus is to, first, infect memory when the host file is invoked by the operating system (in response to a user's command), and, then, to intercept and infect all subsequent applications or the like that are invoked. Systemic infection of a computer or network typically results. A "worm" is a particularly dastardly variation of a virus that is designed to infect a target network by first attaching itself to a host computer and then spreading to other host computers throughout the network, typically simultaneously undermining network resources.

There are several types of computer virus, including a boot sector virus, a

macro virus, an overwriting virus, and a multipartite virus. A boot sector virus infects the boot sector of a diskette or a hard disk and then propagates itself onto every diskette placed into the diskette drive. A macro virus is typically propagated when a Microsoft Word file is attached to an e-mail message. An overwriting virus, as its name implies, simply overwrites each file that it infects, thereby rendering the infected file inoperable. A multipartite virus infects multiple aspects of a computer and file types. For example, a multipartite virus may infect a computer's boot record and also executable application files. As another example, a multipartite virus may infect device drivers (for a mouse, or a printer, etc.) and executable files.

Two common attributes of computer virus are "stealth" and "polymorphic" behavior. A stealthy virus conceals a file being infected generally by saving and then feeding back to the user pre-infection information. That is, a stealthy virus pretends that all is well by ostensibly generating normal feedback messages and the like to users. A polymorphic virus, on the other hand, exhibits schizophrenic behavior in the sense that it eludes detection by varying its underlying (byte-oriented) personality. Accordingly, advanced scanning detection techniques are prerequisite to diagnosing viral patterns so that a suitable antidote may be used to neutralize the polymorphic virus.

To prevent viral invasion of computer and computer networks, all incoming files — locally, via removable input devices such as conventional 3½" diskettes, SuperDisks, and zip disks, or remotely, via e-mail attachments or Internet downloads — should be routinely checked for the presence of viruses. If a virus is found on a storage medium, besides this medium being inoculated, the source of the virus should be investigated and noted (to avoid future recurrences) and reported as appropriate. Anti-virus software should become standard operating equipment to regularly scan and thereby monitor all system activity (unobtrusively in the background) to assure early virus detection. Functioning as virtual device drivers, anti-virus software checks everything that penetrates a computer's territory including every input peripheral device accessing a file and every application that is run.

This specialty software ideally has the benefit of the most current knowledge of all existing computer viruses, and uses advanced detection techniques incorporating sophisticated algorithms, stochastic analysis, and heuristics. Inexpensive superior anti-virus software applications are provided by Symantec Norton, Network Associates' Dr. Solomons and McAfee, and Mijenix SystemSuite. Generally, it is imperative to keep this software in synch with the

state of the art, i.e., currently known viruses, by subscribing to the vendor's online update and maintenance services — including a virus alert service.

Gate-keeping tools such as “firewalls” should preferably be used at entry points into intranets to further secure network environments. A firewall typically prevents the incursion of external communications through its wall-like barrier unless the computer user requested this communication. For example, firewall software would permit the entry of data corresponding to a Web page in response to a browser requesting that the Web page be downloaded for viewing. Nevertheless, other gate-keeping tools are becoming essential.

Electronic terrorists have discovered another dastardly *modus operandi* for conducting e-invasions primarily via a Trojan horse. A tainted application parked on your hard disk may access the Internet without your authority or knowledge. When a channel to the Net has been opened to e-traffic, there is obviously a risk that nefarious hackers and the like can seek to achieve oneness with your computer. Preventing such unauthorized information flow from your computer may be achieved by using blocker software such as ZoneLabs' ZoneAlarm (www.zonlabs.com). Email may be screened (without implicating attached files) before being actually downloaded to your hard disk via software such as Email Remover (eremover.bizhosting.com). Thus, before an email is read *in toto* or an attached file is downloaded, only the “headers” or only a portion of the message may be screened to ascertain whether its Kosher.

Roundtable Suggested Discussion Points

1. E-Mail Protocols: Recommended Procedures and Safeguards
2. Access to Internet Resources
3. Gatekeepers
4. Downloading of Files
5. Forwarding of E-Mail & Files
6. Virus Protection; Frequency of Updates
7. Managing Electronic Data
8. Mail List & Listserv Logistics
9. Password Protection
10. Encryption of Files
11. Chat Rooms