



Help Desk

Sunday, May 2, 2004

By Al Gordon

Former presidential terrorism advisor Richard Clarke has attracted passionate supporters and equally impassioned foes -- and that's just about the Internet.

Clarke, of course, has been making big headlines these days for his criticism of the Bush Administration's handling of 9/11 and Iraq. But in the past he made much a somewhat smaller splash while warning about the threat of "cyberterrorism" -- the possibility that terrorists or other criminals might, via the Internet, unleash viruses, hack vital computer databases, and otherwise inflict major social and economic damage.

Now, undoubtedly, Clarke does have a certain flair for the dramatic. But a lot of what he had to say was right on target: Internet security is terrible.

As the critics see it, Clarke hyped the cyberterrorism threat. Many Internet experts think hacking and virus threats generally are exaggerated -- more annoyance than menace.

While the FBI categorizes computer-related crimes as among the fastest growing criminal enterprises, the bulk of them rely on old-fashioned con artistry, not technological wizardry. As the cyberterrorism skeptics see it, if a terrorist wants to cause 9/11-type damage to the nation's computer infrastructure, bombing a key data center will be more of a threat than Internet hacking. But the Internet

was never intended to be the mass medium it is today.

One of the reasons it was created was to be a communications system that could survive a nuclear war. Thus, a key underpinning of Internet technology is that data, rather than moving directly from Point A to Point B like a telephone call, instead is broken up into pieces and sent out to flow along whatever path it finds available.

This is great for automatically rerouting transmission around lines that have been destroyed in an atomic attack, but not so great in controlling the number of systems that potentially handle the data.

At the time, a major safeguard was that only a few institutions had the capability for computer transmissions. Now Internet enabled computers are as plentiful as toasters, and the original safeguards aren't looking very safe.

To cite the obvious example: No particularly rigorous standards were adopted to insure that the name on the "from" line of an e-mail is real and not a fake. The result is the flood of spam and the ever more elaborate "spoofs" that appear to be from legitimate businesses but actually are scams.

Companies such as Symantec (Norton Internet Security) and Zone Laboratories (Zone Alarm) offer products to help you defend your PC, and you are well advised to use them.

Clarke, however, advanced a few perfectly sensible alternative ideas. One was that software companies ought to write programs that actually work and are not full of flaws that can be exploited by malicious hackers.

Another is that Internet Service Providers, which are large corporations, ought to take on more of the responsibility for screening out

intrusions rather than dump the job on their customers.

Even those who are not fond of the messenger would be hard pressed to find much wrong with that particular message.

Al Gordon is a Massachusetts-based media and political consultant who also writes about technology. You can read more of his articles at www.tnpcnewsletter.com/al and e-mail him at eagle@algordon.com.