



**H.S. (Bert) Garcia** is the U.S. Attorney for the District of Puerto Rico. He practiced in Beaumont before serving as an assistant U.S. attorney for the Eastern District of Texas from 1983 through 2002, when he was appointed to his current position.

**Federal Computer Week**  
([www.fcw.com](http://www.fcw.com))

**Project Safe Neighborhoods**  
([www.psn.gov](http://www.psn.gov))

*These sites have the latest news on Project Safe Neighborhoods and information sharing among police agencies. This information is useful in our office's work with the national Project Safe Neighborhoods program.*

**ProjectChildSafe.org**  
**KlaasKids.org**

*These sites have current information to support my office's anti-child-exploitation law-enforcement efforts.*

**Guide to Grammar and Writing**  
([www.ccc.commnet.edu/grammar](http://www.ccc.commnet.edu/grammar))

*I use this site's grammar and writing tips in a program to disseminate information throughout my office to improve writing and advocacy skills — something every lawyer can and should do.*

**National Hurricane Center**  
([www.nhc.noaa.gov](http://www.nhc.noaa.gov))

*The website of the National Hurricane Center keeps me abreast of hurricane and tropical storm developments. Unlike in Texas, there is no place to go to get away from the coast in Puerto Rico. Current and reliable information is vital to our office and to the protection of our employees' lives and property.*

By Mike W. Erwin

## The Need for Measuring Network Risk

### THE INTERNET HAS DEVELOPED STRIKING

parallels with the “real world” in which we live. It has its own personalities, its own marketplace, even its own currencies. Not surprisingly, it also has a fast-growing underworld, opening us to a whole set of security risks that can jeopardize critical business-data and personal information.

We've seen the rise of a myriad of technology solutions aimed at tackling those security issues. There is anti-virus software to stamp out network-borne “malware,” firewalls for locking our electronic doors and windows, intrusion detection gear for pinpointing break-ins, and authentication techniques to ensure that trust is verified between two parties. All of those tools are useful, but ill-suited to solve the underlying problem: reliable security measurement.

How do we measure whether our network is at risk and decide an appropriate course of action? When and where should we deploy network security measures? Which measures are needed and which are not? I see a world in which an “internet security risk metric” measures the aggregate threat, vulnerability, and expected loss of participating in a network transaction.

Mature industries like insurance and finance use quantified risk-measurements every day. Health insurers collect data on an individual's personal characteristics, medical histories, and genetic predispositions into a statistical profile. This summary is used to validate the price of a premium or deny coverage based on preexisting conditions.

### TECHGEAR



The Griffin iTalk voice recorder (\$40) snaps directly on top of your iPod MP3 player, allowing it to act as a fully functional voice recorder and playback device. You can use the iTalk both to dictate notes and as an external speaker.



**Mike W. Erwin** of Austin is the founder and president of Symbiot, Inc., which designs and builds security solutions based on the concept of risk metrics. Visit [www.symbiot.com](http://www.symbiot.com)

Similarly, the financial industry assigns each of us a three-digit “credit score,” which represents the accumulation of our financial activity for the past 10 years. Credit scores not only provide a mechanism for making discreet decisions, but provide the means for refining a transaction if it is on the cusp.

I believe we need at least two measurements for calculating risk in network security:

**Vulnerability:** A measure of how “at-risk” something is

**Threat:** A measure of how threatening the actor or act is

A score of “000” would represent practically no exposure, while a “999” would represent something on fire. The score would include a “confidence interval” representing its statistical accuracy. Business managers would use the scores for guidance as they choose and deploy security solutions to specific services (email, web services, and instant messaging) and as they deploy larger groups of computers, servers, and networks.

Security risk scores will eventually be used for a wide range of practical purposes, like evaluating security-management devices, setting thresholds for management decisions, and calculating insurance premiums for data-loss policies.

In the legal world, risk metrics show a lot of promise for helping law firms evaluate and secure not only their own networks, but their business processes and relationships with partners. In the not-too-distant future, law firms might insist on certain technology risk metrics when choosing outside counsel in a case. Or a law firm might look closely at standardized security scores when deciding whether to buy a practice-management product. The possibilities are virtually endless.