

# Wanted: Global rating system for security

Jay Cline

**August 5, 2002** ([Computerworld](#))

With corporate accounting practices under fire, are security practices next? The kindling may already be in the pit.

Data security remains largely undefined and unenforced across private industry. The result? Companies underinvest in security, and a steady stream of publicized security breaches keeps customers from trusting e-commerce.

What we need is an independent system that gives "triple-A" or "junk bond" ratings to companies' data security. The private sector needs a global rating system to let customers know whom to trust with their data.

We won't find this rating system in the world's privacy laws. Nearly every such law requires companies to impose their security standards on their suppliers -- but the laws don't detail what those standards should be. Europe, Canada and Australia require companies to deploy data security that is commensurate to the risk of data compromise, but they don't define what that means. Complying with these meaningless standards won't give companies what they need to win customer trust.

Likewise, the largest companies are doing a lousy job of conveying the value of data security. Only 29 of the Global 100 say anything in their online privacy statements about their data security. Just 13 claim to encrypt your data in transit, something you learn to do in Security 101. Most simply say they use "appropriate measures" to protect customer data, and there is

even an emerging trend to add weasel words such as "but your data is never 100% safe." These tactics may be a good legal defense, but they won't build market confidence.

Governments and corporations struggle to talk about security because no one recognizes a common security language. The British Standards Institute's BS7799 code is so comprehensive a masterpiece that no one can afford to adopt it. The Visa Cardholder Information Security Program is more digestible, but it's not designed to communicate security value to the general public. Insurance companies, which have just started compiling risk tables for data security, are best positioned to fill this gap. What we need is a team from Visa, The St. Paul and Standard & Poor's to forge a security rating system that becomes as pervasive as the little padlocks on Web screens that indicate you're on an encrypted connection.

To become pervasive, we need these ratings built into the [Platform for Privacy Preferences](#) (P3P) now included in the latest version of Microsoft's Internet Explorer Web browser.

Why am I hung up on a rating system? Because it fixes a widespread market failure of imperfect information.

Boardrooms today have no way of knowing that a dollar invested in data security will generate even a dime of additional revenue. That's because there's no lingua franca for companies to tell customers they've done something extra to secure their data.

Moreover, large companies aren't even sure what their true risk exposure is because of the intangible nature of data. So boards don't make that extra security investment, tolerating a level of risk that customers still find too risky.


A rating system would be that lingua franca. It would provide a market return for superior ratings and jump-start trust in e-commerce.

Imagine if Standard & Poor's started rating companies' data security. Brands that depend on customer data would have no choice but to shoot for the top rating. An industrywide boost in data security should result in fewer breaches, and customers might begin to turn over their personal data at a profitable ROI. In economic lingo, this moves us from our current "suboptimal equilibrium" to a "Pareto optimal" solution -- a fancy way of saying everybody wins.

As companies look to shore up public confidence in their internal procedures, they'd best look beyond accounting to their data security. Journalists smell blood all over the corporate landscape and will be more than eager to start a security rating system of their own.

*Cline manages data privacy at [Carlson Companies Inc.](#), a Minneapolis-based group of businesses in the travel, hospitality, and marketing industries. Contact him at [privacy@computerworld.com](mailto:privacy@computerworld.com).*

SECURITY PROMISES IN CORPORATE PRIVACY POLICIES	NUMBER OF PRIVACY POLICIES
Number with privacy policies	33
Number with any mention of security	29
Promise "appropriate" technical and organizational measures	24
Promise encryption in transmission	13
Commit to access-control measures	8
Deploy confidential passwords	7
Have regular enhancement of measures	5
Say they have firewalls	4
Use employee agreements, awareness, discipline	4
Hold third parties accountable	3
Say they use a digital certificate	1
Say they use fraud management	1
Use weasel words	6



Source: Study of Global 100 privacy policies by Jay Cline, [Carlson Companies Inc.](#), Minneapolis.