From the Vice President for Policy

Cybersecurity
Markets or Mandates?

by Clyde Wayne Crews, Jr.

One of the Internet's greatest strengths—the ability for anybody to contact anybody else in the world—is also one of its biggest weaknesses, opening the door to virus writers, spammers, and "phishers."

Phishing ruses are those whereby online miscreants trick you into entering personal information—particularly passwords—into a phony website, allowing them to go on a spending spree with your money.

As it happens, just recently, I received an email that appeared to be from Paypal, saying that I needed to click on a link and verify my account. I had, coincidentally, been setting up a Paypal account for CEI and for a moment, wavered. This kind of "double-checking" is what we want from online vendors—yet we have problems when the fakers are faking the verification. The problem is real.

Costly computer virus attacks like MyDoom and SoBig caused tens of billions of dollars in damage. Homeland security and cyber-czars Amit Yoran and Richard Clarke have expressed frustration over the lack of attention to cybersecurity. And the tech industry group Cyber Security Industry Alliance recently released a report calling for President Bush to grant cybersecurity more attention in his second term.

Yet it's not clear how much government can do. Politicians, when they do weigh in on the matter, will seek millions to establish numerous research grants for cybersecurity initiatives; set up cybersecurity agencies, programs, and subsidies; and steer students toward cybersecurity research.

Government regulation to address cybersecurity would be premature. Proposals include mandates for firewalls and virus protection, disclosure and reporting mandates, and more liability for software makers. But legislation—like the anti-spam law—would be ineffective, since the bad guys don't obey the law anyway.

Washington has a proper role, but it entails protecting government's own networks and setting internal security standards, not regulating markets. It involves arresting computer criminals, and avoiding threats to individual privacy in the form of proposed national ID cards and proposals to re-regulate encryption.

Private sector experimentation in cybersecurity is messy but necessary. The marketplace is increasingly forced to address cybersecurity, and those decentralized market approaches will outperform centralized government ones. Companies like Microsoft are automating security; biometric technologies are restricting access to critical facilities. Moreover, the lessons learned from coping with spam, privacy, and digital piracy will carry over to cybersecurity.

When the market makes mistakes—like overly aggressive spam filters—those mistakes are easier to correct than bad legislation. Regulation can quickly become so entrenched that genuine deregulation, however warranted as conditions change, simply cannot occur.

Government should facilitate market institutions, not try to imitate or replace them. One of the more non-controversial cybersecurity tasks often ascribed to government is coordinating information sharing. But sometimes there are legal impediments to voluntary information sharing—antitrust laws may inhibit needed coordination among firms, as may overly aggressive interpretations of the Freedom of Information Act. Government should rethink both.

Indeed, improving private incentives for information sharing is at least as important a pursuit as more government coordination to ensure security and critical infrastructure protection. That job will entail deregulating critical infrastructure assets—like telecommunications and electricity networks—and relaxing antitrust constraints so firms can enhance reliability and security not just by sharing information but though "partial mergers" of the kind that are anathema to today's antitrust enforcers.

Private cybersecurity initiatives will gradually move us toward thriving liability and insurance markets. Heavy-handed cyber-czar gestures and legislation cannot address the inability to exclude bad apples that is at the root of today's cybersecurity problems. Nonetheless, it's not surprising that officials such as Yoran and Clarke were frustrated. The problem is, even if they had gotten their way, it's not clear what government could really fix. But it could break a lot.

MONTHLY PLANET

Publisher:
Fred L. Smith, Jr.

Editor:
Ivan G. Osorio

Assistant Editor:
Elizabeth Jones

Contributing Editor:
Richard Morrison

CEI's Monthly Planet is produced 10 times a year by the Competitive Enterprise Institute, a pro-market public interest group dedicated to free enterprise and limited government.

CEI is a non-partisan, non-profit organization incorporated in the District of Columbia and is classified by the IRS as a 501 (c)(3) charity. CEI relies upon contributions from foundations, corporations and individuals for its support. Articles may be reprinted provided they are attributed to CEI.

Phone:
(202)331-1010

Fax:
(202)331-0640

E-mail:
info@cei.org

ISSN# 1086-3036