SIDLEY AUSTIN BROWN & WOOD LLP
AND AFFILIATED PARTNERSHIPS

NOVEMBER 13, 2003

PRIVACY AND DATA PROTECTION ALERT

Privacy, Data Protection and Information Security Practice Group

Sidley Austin Brown & Wood LLP offers clients an inter-disciplinary, international group of lawyers focusing on the complex issues of privacy, data protection, information security, consumer protection and cybercrimes. Members of the Privacy Group are based primarily in Washington, New York, London, Chicago, Brussels, and Los Angeles. The Group includes intellectual property lawyers, litigators, financial institution practitioners, health care lawyers, EU specialists, IT licensing and marketing counsel, and regulatory and white collar lawyers.

If you would like more information on the Privacy, Data Protection and Information Security Practice Group, please contact:

Peter Toren
212-839-7357
ptoren@sidley.com

Alan Charles Raul
202-736-8477
araul@sidley.com

Brad Berenson
202-736-8971
bberenson@sidley.com

To receive future copies of the Privacy and Data Protection Alert via email, please send your name, company or firm name and email address to lhersh@sidley.com

This **Privacy and Data Protection Alert** has been prepared by SIDLEY AUSTIN BROWN & WOOD LLP for informational purposes only and does not constitute legal advice. This information is not intended to create, and receipt of it does not constitute, an attorney-client relationship. Readers should not act upon this without seeking professional counsel.

The rapid increase in computer crime has led Congress to consider the introduction of a bill requiring publicly traded companies to obtain a professional computer security audit and to comply with minimum computer security standards. The Chairman of the House technology subcommittee, Rep. Adam Putnam, however, has postponed introduction of such a bill for 90 days to enable the business community to propose comments or an alternative.

Putnam's proposed bill would be modeled after mandatory disclosures that the business community was required to provide to the Securities and Exchange Commission in 1999 as part of an effort to limit damage caused by the "Y2K bug." In this case, it would require publicly traded corporations to demonstrate to the SEC that they had conducted a computer security audit and had implemented a set of minimum computer security standards.

The business community has already raised concerns in response to the proposed bill, including whether the SEC is the appropriate oversight body for computer security and the potential costs and burdens of new regulations. In response, Putnam is convening a cybersecurity working group that will include several business representatives including the Business Software Alliance, the U.S. Chamber of Commerce, and the Information Technology Association of America. Putnam has indicated that unless the working group formulates a strong proposal, stringent legislation may be required. However, he has indicated that even with such a proposal, federal legislation may still be required, if only to codify the industry's ideas.

Estimates of the amount of damage to U.S. businesses caused by computer crime vary greatly, however, there is little doubt that corporate America's increased reliance on information technology has led in recent years to a dramatic increase in such losses. A 2003 study by the Computer Security Institute and Federal Bureau of Investigation found that 90% of the respondents had suffered breaches of their computer system within the past year but only 30% reported such breaches to the government. The study also challenged the notion that the greatest threat to organizations comes from within, or that most hackers are

"juveniles on joy-rides through cyberspace." The study determined that there is "much more illegal and unauthorized activity in cyberspace than corporations admit to their clients, stockholders and business partners or report to law enforcement." Incidents are widespread, costly and commonplace.

Despite these very real and substantial risks, many companies are not doing enough to protect themselves. According to Ernst & Young's Global Information Security Survey 2003, many organizations fail to adequately protect their digital assets by investing in information security. Companies often take no action until they have been the victim of a security breach and then compound their mistake by implementing a temporary "fix" which ignores their core business objectives. Measured, proactive spending is less costly in the long run than reactive spending, which is often overspending in response to an incident. Nearly 60% of the organizations that responded to the survey indicated that they had never calculated a return on investment for information security spending.

Apart from not implementing comprehensive computer security programs, many companies believe that losses caused by security breaches would be covered by their general liability insurance policies. The trend in recent cases, however, is to deny coverage under general liability insurance policies for losses caused by breaches of computer security or from other cyberevents on the ground that damage or loss of data does not constitute damage to tangible property.

In order to reduce the risks associated with inadequate computer security, we suggest that companies consider implementing a comprehensive computer security plan and obtaining a cyberinsurance policy.

The affiliated firms, Sidley Austin Brown & Wood LLP, a Delaware limited liability partnership, Sidley Austin Brown & Wood LLP, an Illinois limited liability partnership, Sidley Austin Brown & Wood, an English general partnership and Sidley Austin Brown & Wood, a New York general partnership, are referred to herein collectively as Sidley Austin Brown & Wood.

SIDLEY AUSTIN BROWN & WOOD LLP
AND AFFILIATED PARTNERSHIPS

BEIJING BRUSSELS CHICAGO DALLAS GENEVA HONG KONG LONDON LOS ANGELES
NEW YORK SAN FRANCISCO SHANGHAI SINGAPORE TOKYO WASHINGTON, D.C.

www.sidley.com