



FOR IMMEDIATE RELEASE

Scott & Scott LLP and Ponemon Institute Announce Results of Survey Assessing the Business Impact of Data Security Breach

Study Shows US Businesses Still Lack Adequate Security and Incident Response Plans to Protect Confidential Customer Information from a Potential Breach

DALLAS, TX – May 15, 2007 – According to a new study commissioned by Scott & Scott, LLP (www.scottandscottllp.com) and conducted by privacy and information management research firm the Ponemon Institute (www.ponemon.org), 85% of businesses have experienced a data security breach. Despite the frequency of such security failures, 46% of businesses failed to implement encryption solutions even after suffering a data breach, and 82% did not seek legal counsel prior to responding to the incident despite having no prior response plan in place.

The survey, entitled *The Business Impact of Data Breach*, examines the responses of more than 700 US-based C-level executives, managers, and IT security officers in mid-size to large businesses spanning all industries. Analysis of the results shows that businesses are struggling to implement the proper policies and controls required to prepare for and mitigate the legal, regulatory, and financial risks associated with a security failure. In addition, many businesses may be discounting the long-term threat to customer retention and corporate reputation.

Key findings from the survey include the following:

- More than 85% of respondent organizations reported that they have experienced a data breach event.
- Of those organizations, less than 43% had an incident response plan in place, and 82% failed to consult with legal counsel before responding to the incident.
- Following a breach, 46% of organizations still failed to implement encryption technology on portable devices.
- 95% of businesses suffering a data breach were required to notify data subjects whose information was lost or stolen.
 - 97% were required to notify under state statutes.
 - 58% were required to notify under federal privacy acts such as HIPAA, GLBA and OCC.
- Organizations that suffered data breach actually employ substantially more IT and data security measures than organizations that did not experience a data breach.
- 37% of respondents say their organizations sent blanket notifications, rather than precise notifications.
- Organizations experiencing a data breach incurred costs across the board.
 - 74% report loss of customers.
 - 59% faced potential litigation.
 - 33% faced potential fines.
 - 32% experienced a decline in share value.

- Almost half of the breach incidents were attributed to lost or stolen equipment such as laptops, PDAs, and memory sticks. The second largest threat came from negligent employees, temporary employees, and/or contractors.
- Despite the frequency of data breach events, 42% of respondents claim their organization's IT security spending will remain the same in the coming year.

"Our findings show that data breaches are a pervasive problem for most organizations in the United States today. We also show that despite negative repercussions in terms of cost outlays and reputation diminishment, many companies that experience a breach do not take appropriate steps to prevent future incidents," said Dr. Larry Ponemon, founder and chairman of the Ponemon Institute. "However, I'm most surprised that IT security solutions such as encryption and authorization technology are not being deployed by most companies today."

Robert Scott, managing partner at Scott & Scott LLP agreed stating, "The most significant finding to me is that, despite having experienced a data breach, 46% of respondents failed to implement encryption technology on portable devices such as laptops and PDAs. Encryption is the single most effective way to avoid the negative business impact of data breaches.

"Also alarming is that 82% of businesses responded to data breach incidents without first consulting legal counsel. The legal landscape governing data privacy is complex with thirty-five separate state regulations and numerous federal regulations that may be applicable to a particular incident," said Scott.

With nearly 100% of businesses stating they were required under state or federal regulations to report the breach, respondents place careful assessment of potential harm to data subjects as their first priority following a breach. Most report little or no monetary harm to the data subjects. These findings seem to highlight the need for reform of notification requirements, which can be detrimental to businesses especially when weighed against the perceived lack of real benefit to consumers.

"The common perception held by many respondents is that monetary impact to data breach victims is nonexistent or negligible. In other words, respondents believe that the notification requirement may not provide tangible consumer benefits such as preventing possible future economic harms," said Ponemon.

Dr. Ponemon will present the survey results to an audience of compliance and legal professionals at a reception hosted by Scott & Scott during the [NASD's 16th Annual Spring Securities Conference](#) at the Chicago Marriot Downtown on May 23, 2007. Dr. Ponemon will offer analysis of the survey and discuss practical lessons businesses can learn from the results.

The NASD's Securities Conference is a world-renowned event exploring the industry's latest updates in securities regulation and compliance. Featuring timely insights from industry experts, content-rich workshops and other activities, this conference is designed to equip compliance and legal professionals with tools and knowledge that will help them manage their enterprise on a daily basis.

Copies of the *Survey on the Business Impact of Data Breach* are available through the Ponemon Institute and through Scott & Scott, LLP.

###

About Scott & Scott LLP

Scott & Scott is an international law and technology services firm dedicated to helping senior executives assess and reduce the legal, financial, and regulatory risks associated with information technology issues. An innovative approach to legal services, Scott & Scott believes

that collaboration between legal and technology professionals is necessary to solve and defend against the complex problems our clients face, including privacy and network security, IT asset management, software license compliance, and IT transactions. Legal and technology professionals work in tandem to provide full-service representation. By combining these resources, Scott & Scott is better able to serve clients' needs than law firms and technology services firms working independently of one another. Visit Scott & Scott online at www.scottandscottllp.com.

About the Ponemon Institute

The Ponemon Institute© is dedicated to advancing responsible information and privacy management practices in business and government. To achieve this objective, the Institute conducts independent research, educates leaders from the private and public sectors and verifies the privacy and data protection practices of organizations in a variety of industries. For more information, visit www.ponemon.org.

For additional information, please contact:

Mary Cheatham
Scott & Scott LLP
214-999-0080
mcheatham@scottandscottllp.com

Mike Spinney
Ponemon Institute
978-597-0342
mspinney@ponemon.org