Study looks at way US boards and CEOs manage risk

December 2 2008

A recent Carnegie Mellon University CyLab survey of corporate board directors reveals a gap in board and senior executive oversight in managing cyber risks.

Based upon data from 703 individuals (primarily independent directors) serving on U.S-listed public company boards, only 36 percent of the respondents indicated that their board had any direct involvement with oversight of information security.

The survey also said that cybersecurity issues need to be seen as an enterprise risk management problem rather than an IT issue.

"Managing cyber risk is not just a technical challenge, but it is a managerial and strategic business challenge," said Pradeep K. Khosla, dean of Carnegie Mellon's College of Engineering and CyLab founder.

"There are real fiduciary duty and oversight issues involved here," said Jody Westby, adjunct distinguished fellow at Carnegie Mellon CyLab and the survey's lead author. "There is a clear duty to protect the assets of a company, and today, most corporate assets are digital."

"We also found that boards were only involved about 31 percent of the time in assessment of risk related to IT or personal data — the data that triggers security breach notification laws," said Westby, who is also chair of the American Bar Association's Privacy and Computer Crime Committee.

Only 8 percent of survey respondents said their boards had a risk committee that is separate from the audit committee, according to Westby.

"Without the right organizational structure and interest from top officials, enterprise security can't be effective no matter how much money an organization throws at it," said Richard Power, co-author of the report and a distinguished fellow at Carnegie Mellon CyLab.

Power said the survey also shows that senior management has not budgeted for key positions requiring expertise in cybersecurity or privacy areas. "No wonder the number of security breaches has doubled in the past year — only 12 percent of the respondents have established functional separation of privacy and security, and most companies don't have C-level executives responsible for these areas," Power added, comparing the survey results to the breach chronology maintained by the Privacy Rights Clearinghouse (http://www.privacyrights.org/ar/ChronDataBreaches.htm).

To help company boards improve corporate governance of privacy and security, the survey recommends broad operational changes from establishing a board risk committee separate from the audit committee to reviewing existing top-level policies to creating a culture of security and respect for privacy.

Source: Carnegie Mellon University