FOLEY

FOLEY & LARDNER LLP

Taking Control of Cybersecurity: A Practical Guide for Officers and Directors

By Chanley T. Howell, Michael R. Overly, and James R. Kalyvas
11 March 2015

Major cybersecurity attacks of increased sophistication — and calculated to maximize the reputational and financial damage caused to the corporate targets — are now commonplace. These attacks have catapulted cybersecurity to a top priority for senior executives and board members.

To help these decision makers get their arms around cybersecurity issues, Foley Partners Chanley T. Howell, Michael R. Overly, and James R. Kalyvas have published a comprehensive white paper entitled: **Taking Control of Cybersecurity — A Practical Guide for Officers and Directors**.

The white paper describes very practical steps that officers and directors *should ensure are in place or will be in place in their organizations* to prevent or respond to data security attacks, and to mitigate the resulting legal and reputational risks from a cyber-attack. The authors provide a blueprint for managing information security and complying with the evolving standard of care. Checklists for each key element of cybersecurity compliance and a successful risk management program are included.

Excerpt From Taking Control of Cybersecurity: A Practical Guide for Officers and Directors

Sony, Target, Westinghouse, Home Depot, U.S. Steel, Neiman Marcus, and the National Security Agency (NSA). The security breaches suffered by these and many other organizations, including most recently the consolidated attacks on banks around the world, combined with an 80 percent increase in attacks in just the last 12 months, have catapulted cybersecurity to the top of the list of priorities and responsibilities for senior executives and board members.

The devastating effects that a security breach can have on an enterprise, coupled with the bright global spotlight on the issue, have forever removed responsibility for data security from the sole province of the IT department and CIO. While most in leadership positions today recognize the elevated importance of data security risks in their organization, few understand what action should be taken to address these risks. This white paper explains and demystifies cybersecurity for senior management and directors by identifying the steps enterprises must take to address, mitigate, and respond to the risks associated with data security.

Officers and Directors are Under a Legal Obligation to

Involve Themselves in Information Security

The corporate laws of every state impose fiduciary obligations on all officers and directors. Courts will not second-guess decisions by officers and directors made in good faith with reasonable care and inquiry. To fulfill that obligation, officers and directors must assume an active role in establishing correct governance, management, and culture for addressing security in their organizations.

Download This White Paper