For the purpose of this presentation, I will be focusing primarily on the liability of directors and officers of publically held corporations. The typical types of liability proceedings against directors and officers of publically held corporations are shareholder derivative and securities class actions, regulatory proceedings brought by state and federal agencies, and criminal actions brought by state and federal prosecutors.

Shareholder derivative actions are typically brought for alleged breaches of fiduciary duty, lack of duty of due care, or a failure to exercise appropriate diligence. They are brought by one or more shareholders, who sue in the name of the corporate entity. Any recovery against the named directors is awarded to the corporation. Shareholder Securities Class Actions often arise in connection with misrepresentations to the shareholders and false statements made by the corporation in securities filings or public disclosures. Unlike derivative actions, any liability established against corporate directors and officers directly benefits the shareholders in that they are the beneficiaries of such damage awards and settlements. Regulatory and criminal actions brought by state and federal regulatory and law enforcement agencies are independent of any related shareholder actions and may or may not directly benefit shareholders and/or employees, who as “eligible Whistleblowers,” may be entitled to an award pursuant to regulations established by the Securities and Exchange Commission (SEC). For purposes of this discussion, the principal entities, which will pursue actions against corporate directors and officers, are the SEC and the US Justice Department, which oversees possible corporate misrepresentations and/or securities fraud.

D&O liability insurance policies typically provide direct coverage to directors and officers for personal liability under Section A, and to the corporation for “Securities Claims” for “Loss” made due to “Claims”, that occur during the policy period. Therefore, there is no coverage for “payments” made before a claim has been asserted. Therefore, one would likely not find a D&O policy paying for prophylactic remedies such as
issuing complementary subscriptions to credit watch agencies in response to a discovered securities breach, before an actual claim has been made. In addition, there is likely no coverage for fines, penalties, or civil damages assessed against the company only. Also, there would likely be no coverage for “Store vouchers,” or promotional/remedial remedies issued by the corporation in response to a discovered and announced securities breach, whether or not the award was made in settlement of a claim, or before a claim was ever filed. Finally, no coverage would likely be available for the costs incurred in connection with a “Regulatory Investigation” pursued against the corporate entity before the commencement of a formal investigation against a director or officer.

Some examples of D&O claims in the context of cybersecurity liability include, in Re Hartland Payment System, Inc. Securities Litigation, Civ. No. 09-1043, arising out of a “Structured Query Language (SQA),” in December 2007, which impacted 130 million credit card and debit card holders. The plaintiffs alleged that certain Hartland Payment System directors and officers failed to disclose that the company had inadequate controls to protect consumers’ financial data from securities breaches. The securities class action was dismissed on motion, in that the court found that the plaintiffs failed to allege scienter. In addition, in the case of TJX Companies, the plaintiffs filed a derivative action for breach of fiduciary duty and waste of corporate assets, arising out of an announced cyber securities breach; involving 45.7 million credit/debit card numbers. The matter ultimately settled for plaintiffs’ attorney fees of $595,000 and prophylactic remedies, although the total costs of the breach are estimated to be approximate $200 million. Finally, as of this presentation, two derivative actions have been filed against Target Corporation, for breach of fiduciary duty, gross mismanagement, waste of corporate assets, and abuse of control, all arising out of a massive data breach by Target, in which 70 million customers were affected.

From a regulatory perspective, the Federal Trade Commission (FTC) in the past issued Theft Red Flag Rules, which have largely transferred enforcement authority from the FTC to the SEC and the Commodity Futures Trading Commission (CFTC). It primarily involves financial institutions and organizations that provide financial services to third parties, as well as the development, implementation, and administration of identity theft protection programs. On October 11, 2011, the SEC’s Division of Corporate Finance issued, what has been characterized as: “CF Disclosure
Guidance: Topic No. 2,” relating to cybersecurity risks and cyber incidents.”

In a veiled reference to the Hartland case, the Guidance provides:

“…(I)f a registrant experienced a material cyber attack in which a malware was embedded in its systems and customer data was compromised, it likely would not be sufficient for the registrant to disclose that there is a risk that such an attack may occur.”

This may have the result of precluding another court from dismissing a lawsuit on motion for failure to assert scienter if another action similar to Hartland were ever filed.

In addition to the SEC and other Federal regulatory and law enforcement agencies, various state authorities, such as the California Department of Justice, enforce a series of privacy laws enacted by the state legislature. Further, numerous foreign jurisdictions have enacted legislation and regulation from such agencies as Britain’s Information Commissioner’s Office, which may impact directors’ and officers’ potential liability.

There are other areas of professional liability that could give rise to claims, which could trigger coverage under a Professional Indemnity (PI) policy. For example, legal liability under a PI policy could be triggered where lawyers and law firms inadvertently disclose, or third parties gain access to: confidential information entrusted to a lawyer in connection with a merger of acquisition; health information of a patient in connection with pending litigation or through the lawyer’s representation of a healthcare facility; or sensitive trust account information held by a trust and estate attorney.

To the extent the release of confidential information could be considered a breach of one’s professional ethics, coverage under a PI policy may be more expansive than the coverage typically available under a D&O policy. However, with the increase of data security breaches, in violation of SEC and other state and federal regulatory guidelines, securities class and derivative actions, along with regulatory proceedings, may become more common, expanding the scope of D&O liability.