

## **“Reasonable Information Security” and the Duty of Due Care**

The duty of Due Care is a fundamental component of corporate governance. The duty of Due Care imposes a “reasonable person” standard on directors in their actions on behalf of the organization. The basic idea of Due Care is that management must exercise sufficient risk management oversight in order to make decisions to ensure protections that would be considered reasonable and prudent for similar companies in similar situations. Due Care is a basic protection (though not an absolute protection) against negligence claims. As opposed to the oft-used term “best practices,” Due Care would be considered “Reasonable Practices.”

The problem with Due Care is that it is a constantly moving target. It varies from industry to industry, changes constantly with changes in applicable technology, can vary based on regional or national laws and conventions, and the definition of “reasonable” is very subjective. Nevertheless, lawyers, regulators, and courts use this as a standard for measuring whether our security & privacy programs provide adequate protection for our companies and consumers. Accordingly, a comprehensive and mature information security risk management framework is critical to the duty of Due Care.

The presentations look at the relationship between the duty of Due Care and the emerging legal concept of “reasonable information security,” and the fundamental role of information security risk management in defining “reasonable security” and meeting Due Care obligations.

The presenters are:

Don M. Blumenthal, Principal, DMB Associates, LLC

[www.donblumenthal.com](http://www.donblumenthal.com)

Patrick F. Sullivan, Ph.D., Principal Consultant, JBW Group International

[www.jbwgroup.com](http://www.jbwgroup.com)

Rick Clark, CISSP, Manager, Corporate Security, Ontario Systems, LLC

[www.ontariosystems.com](http://www.ontariosystems.com)