PREFACE

This publication is intended to serve as a manual for directors and officers to help them understand how to appropriately govern cyber risks. It boils down the oceans of data that have been compiled on the subject and lays out clear, understandable approaches to managing cyber risks that are in line with best practices and internationally accepted standards on governance of information security.

Directors and officers (D&Os) do not have to be cyber geeks or learn the IT terminology and lingo to manage cyber risks. They simply need to understand how to exercise oversight of cyber risks so they can perform the responsibilities required for their roles using best practices and standards and meeting compliance requirements. Cyber governance is not something only large corporations need to worry about; no matter how large or small the organization, D&Os need to understand how to govern cyber risks.

This publication provides the basic information directors and officers need to know to meet their fiduciary duties, exercise appropriate cyber governance, and protect their organization against shareholder derivative and securities lawsuits. It is written as a guide and will help D&Os:

- Develop a governance framework in alignment with best practices and standards;
- Understand the elements of a cybersecurity program;
- Ensure privacy and security compliance requirements are met;
- Manage a cybersecurity incident and make hard decisions; and
- Develop appropriate risk transfer and management strategies.

And some of the best stuff is saved for last, the appendices provide a Cyber Governance Checklist and a Cyber Lingo Cheat Sheet.

The good guys will start winning once boards and senior management take the lead, establish a framework for cyber governance, articulate key roles and responsibility for information security, and identify the key risks they need to monitor. It is not rocket science. It is just a matter of paying attention at the top, knowing what risks to focus on, allocating appropriate resources, and trying to stay ahead of cybercriminals . . . continually.

Cybercrime is costing corporations billions (some studies say trillions) in lost productivity, stolen assets and intellectual property, and market share. It is probably the single largest risk to national and economic security, and it is a leading means of foreign intelligence gathering. This problem requires leadership. I hope this publication pulls the mystery off cyber governance and helps turn the tide.

Jody R. Westby
Washington, DC