

Cyber-Risk Oversight 2020

Key Principles and Practical Guidance
for Corporate Boards



© 2020 by the National Association of Corporate Directors and the Internet Security Alliance. All rights reserved.

Except as permitted under the US Copyright Act of 1976, no part of this publication may be reproduced, modified, or distributed in any form or by any means, including, but not limited to, scanning and digitization, without prior written permission from the National Association of Corporate Directors or the Internet Security Alliance.

This publication is designed to provide authoritative commentary in regard to the subject matter covered. It is provided with the understanding that neither the authors nor the publishers, the National Association of Corporate Directors and the Internet Security Alliance, is engaged in rendering legal, accounting, or other professional services through this publication. If legal advice or expert assistance is required, the services of a qualified and competent professional should be sought.



Cyber-Risk Oversight 2020

Key Principles and Practical Guidance
for Corporate Boards

Prepared by Larry Clinton

President and CEO,
Internet Security Alliance

WITH SUPPORT FROM

Josh Higgins

Senior Director of Policy and Communications
Internet Security Alliance

Friso van der Oord

Senior Director of Research and Editorial
National Association of Corporate Directors

Acknowledgements

NATIONAL ASSOCIATION OF CORPORATE DIRECTORS

Peter R. Gleason, Chief Executive Officer

Erin Essenmacher, President and Chief Strategy Officer

Friso van der Oord, Senior Director, Research and Editorial

Christopher Hetner, NACD Cybersecurity Advisor

Leah Rozin, Senior Research Manager

Barton Edgerton, Associate Director, Governance Analytics

Ted Sikora, Manager Of Benchmarking and Data Insights

Reaa Chadha, Senior Research Analyst

Andrew Lepczyk, Research Analyst

Margaret Suslick, Manager, Copy Editing & Print Production

Patricia W. Smith, Art Director

Alex Nguyen, Senior Graphic Designer

Prepared by **Larry Clinton**, President and CEO, Internet Security Alliance, with support from **Josh Higgins**, Senior Director of Policy and Communications, Internet Security Alliance, and **Friso van der Oord**, Senior Director of Research and Editorial, National Association of Corporate Directors.

We wish to thank the following individuals for their contributions to this Handbook (in alphabetical order by organization):

Tracie Grella, Garin Pace, Anthony Shapella, AIG

Lisa Humbert, Bank of Tokyo Mitsubishi, MUFG

Adrian Peters, BNY Mellon

Bob Zandoli, Bunge

Nick Corzine, Lou DeSorbo, Ben Havelka, Geoji Paul, Centene

Catherine Ide, Center for Audit Quality

Robert Kolasky, Daniel Kroese, Ashley Montgomery, Department of Homeland Security

Joe Buonomo, Robert Gardner, Direct Computer Resources

Jim Halpert, Andy Serwin, DLA Piper

Robyn Bew, Andrew Cotton, EY

Jillian Stickels, FBI

Greg Montana, FIS

Nasrin Rezai, General Electric

Melissa Hathaway, Hathaway Global Strategies

Dan Lips, Celeste Lowery, Internet Security Alliance

J. R. Williamson, Leidos

Scott Rush, Lockheed Martin

Robyn Boerstling, National Association of Manufacturers

Ben Abrams, Mike Papay, Northrop Grumman

Jeff Brown, Raytheon

Tim McKnight, Richard Puckett, SAP

John Frazzini, Robert Vescio, SSIC

Gary McAlum, USAA

Richard Spearman, Vodafone

Table of Contents

Acknowledgements	2
Foreword.....	4
Introduction.....	6
PRINCIPLE 1	12
Cybersecurity as a Strategic Risk	
Directors need to understand and approach cybersecurity as a strategic, enterprise risk—not just as an IT risk.	
PRINCIPLE 2	16
Legal and Disclosure Implications	
Directors should understand the legal implications of cyber risks as they relate to their company’s specific circumstances.	
PRINCIPLE 3	20
Board Oversight Structure and Access to Expertise	
Boards should have adequate access to cybersecurity expertise, and discussions about cyber-risk management should be given regular and adequate time on board meeting agendas.	
PRINCIPLE 4	
An Enterprise Framework for Managing Cyber Risk	25
Directors should set the expectation that management will establish an enterprise-wide, cyber-risk management framework with adequate staffing and budget.	
PRINCIPLE 5	
Cybersecurity Measurement and Reporting	30
Board-management discussions about cyber risk should include identification and quantification of financial exposure to cyber risks and which risks to accept, mitigate, or transfer, such as through insurance, as well as specific plans associated with each approach.	
Conclusion	34

TOOLKIT

Road Map for the Cyber-Risk Oversight Toolkit	36
Tool A – 10 Questions for a Board Member to Ask About Cybersecurity.....	37
Tool B – Assessing the Board’s Cyber-Risk Oversight Effectiveness	41
Tool C – The Cyber-Insider Threat—a Real and Ever-Present Danger	43
Tool D – Supply-Chain and Third-Party Risks.....	45
Tool E – Incident Response	49
Tool F – Board-Level Cybersecurity Metrics....	53
Tool G – Cybersecurity Considerations During M&A Phases — Mergers and Acquisitions.....	56
Tool H – Sample Dashboards.....	60
Tool I – Building a Relationship With the CISO	63
Tool J – Enhancing Cybersecurity Oversight Disclosures—10 Questions for Boards.....	66
Tool K – Personal Cybersecurity for Board Members.....	69
Tool L – Department of Homeland Security Cybersecurity Resources.....	70
Tool M – Department of Justice and Federal Bureau of Investigation—Responding to a Cyber Incident	72