INTERNET SECURITY ALLIANCE

ANSI
American National Standards Institute

THE FINANCIAL MANAGEMENT OF CYBER RISK

An Implementation Framework for CFOs

"An excellent guide for organizations to manage the risk and exposure derived from digital dependence"

– Melissa Hathaway
President of Hathaway Global Strategies and
former Acting Senior Director for Cyberspace
for the National Security Council

"An invaluable resource for every C-level executive"

– David Thompson
CIO and Group President
Symantec Services Group

TABLE OF CONTENTS

ACKNOWLEDGEMENTS

The following professionals participated in one or more of the ISA-ANSI sponsored workshop meetings. The views expressed in this document are those of the individual workshop participants and do not necessarily reflect the views of the companies and organizations listed.

American International Group	Robert Roche
Allen Associates	Mary Beth Allen*
Allied World Insurance Company	Michael Murphy
American National Standards Institute	Jessica Carl, Karen Hughes, Peggy Jensen, Brian Meincke, Liz Neiman, Fran Schrotter
Carnegie Mellon University	Julia Allen, Jefferson Welch
Catalyst Partners LLC	Rich Cooper
Chartis	Nancy Callahan
CNA Insurance	John Wurzler
Crimson Security	Narender Mangalam
Cyber Security Assurance, LLC	E. Regan Adams
Direct Computer Resources, Inc.	Joe Buonomo, Ed Stull, Bill Vitiello
Ferris & Associates, Inc.	John Ferris
Financial Services Technology Consortium	Roger Lang, Dan Schutzer
Guy Carpenter & Company LLC	Harry Oellrich*
HealthCIO Inc.	Jonathan Bogen
Herbert L. Jamison & Co., LLC	John Ercolani
Hunton & Williams	Lon Berk*
ID Experts	Christine Arevalo, Bob Gregg, Rick Kam*
Independent consultant	James Wendorf
Internet Security Alliance	Larry Clinton, Brent Pressentin
Jones Day	Gwendolynne Chen
Meritology	Russell Thomas
The MITRE Corporation	Michael Aisenberg
National Institute of Standards and Technology	Dan Benigni
New World Technology Partners	Robert Gardner
Northrop Grumman	Mark Leary, Rebecca Webster*
Packaging Machinery Manufacturers Institute	Fred Hayes
Perot Systems Corporation	Bruno Mahlmann, Katie Ortego Pritchett
Phillips Nizer LLP	Thomas Jackson*
Prolexic Technologies	Paul Sop
QUALCOMM Inc.	Mark Epstein
Reed Elsevier	Arnold Felberbaum*

Robinson Lerer & Montgomery	Anne Granfield, Michael Gross
Salare Security LLC	Paul Sand
Society for Human Resource Management	Lee Webster
U.S. Chamber of Commerce	Matthew Eggers
U.S. Cyber Consequences Unit	Warren Axelrod, Scott Borg
U.S. Department of Commerce	Michael Castagna*
U.S. Department of Homeland Security	Thomas Lockwood
U.S. Department of Justice	Martin Burkhouse
U.S. Securities and Exchange Commission	Ralph Mosios
University of California, Berkeley	Aaron Burstein
University of Maryland	Momodu Fofana
Zurich North America	Richard Billson, Brad Gow, Ty Sagalow

** Task Group Leader*

Thanks and acknowledgement are given for the support and participation of all the organizations that supplied experts to this initiative. Without the contributions of these individuals and their collective expertise, particularly those that participated on the workshop task groups, this final deliverable would not have been possible.

- Special acknowledgement and appreciation is given to Ty R. Sagalow of Zurich North America and Joe Buonomo of Direct Computer Resources, Inc., for being the workshop leaders of this initiative. Their leadership and dedication in helping to shape the initiative, lead its proceedings, and build consensus for the final deliverable were instrumental in reaching a successful outcome.

- Appreciation is given to the American National Standards Institute (ANSI) and the Internet Security Alliance (ISA) for the effective project management that kept this initiative on track and allowed for a successful delivery of the final publication in a timely manner, particularly Fran Schrotter, Karen Hughes, and Jessica Carl of ANSI, and Larry Clinton, Marjorie Morgan, and Brent Pressentin of ISA.

- Special acknowledgement is given to Zurich North America, Robinson Lerer & Montgomery, Direct Computer Resources, Inc., and Phillips Nizer for generously hosting and sponsoring the workshop sessions and meetings.

- Thank you to the following special advisors for their review and insightful comments on the advance proof copy which contributed to the final version presented here:
  – Dr. Donald R. Deutsch, Vice President, Standards Strategy & Architecture, Oracle
  – Ron Dick, Former Director, National Infrastructure Protection Center (NIPC)
  – Dr. John Fox, President & CEO, FFC Computer Services, Inc.
  – Bob Gregg, CEO, ID Experts Corp
  – Roberto J. Lagdameo, Director of Finance, Collington Episcopal Life Care Community, Inc.
  – Alan C. Levine, CIO, John F. Kennedy Center for the Performing Arts
  – Richard F. Mangogna, President & CEO, Mason Harriman Group (formerly DHS/CIO)
  – Mike Mancuso, CFO of CSC
  – Christopher J. Steinbach, President & CEO, The Newberry Group, Inc.
  – Sandy B. Sewitch, CFO, General Kinetics, Inc.

- Thank you to Ed Stull, Direct Computer Resources, Inc., and Robert Gardner, New World Technology Partners, for leading this special advisor review effort and for providing the consolidated and insightful feedback to the workshop leaders.

EXECUTIVE SUMMARY

Business is currently on the front lines of a raging cyber war that is costing trillions of dollars and endangering our national security.

Effective, low-cost mechanisms are already in place to shield against many elements of the cyber threat. But too often executive leaders wait until they are compromised to put a reactive plan into action, damaging their company's reputation and incurring additional cost.

Greater understanding and guidance are needed to help businesses bolster information security and reduce vulnerability to cyber attacks.

That is why the Internet Security Alliance (ISA) and the American National Standards Institute (ANSI) have developed this free, easy-to-use action guide, which brings together the independent research and the collective wisdom of more than sixty experts from industry, academia, and government.

All of these experts agree: the single biggest threat to cybersecurity is misunderstanding.

Most enterprises today categorize information security as a technical or operational issue to be handled by the information technology (IT) department. This misunderstanding is fed by outdated corporate structures wherein the various silos within organizations do not feel responsible to secure their own data. Instead, this critical responsibility is handed over to IT, a department that, in most organizations, is strapped for resources and budget authority. Furthermore, the deferring of cyber responsibility inhibits critical analysis and communication about security issues, which in turn hampers the implementation of effective security strategies.

In reality, cybersecurity is an enterprise-wide risk management issue that needs to be addressed from a strategic, cross-departmental, and economic perspective. The chief financial officer (CFO), as opposed to the chief information officer (CIO) or the chief security officer (CSO), is the most logical person to lead this effort.

This publication was created to provide a practical and easy-to-understand framework for executives to assess and manage the financial risks generated by modern information systems:

- Chapter One explains the true economic impact of cyber events and describes a six-step process for addressing the issue on an interdepartmental basis.
- Chapter Two focuses on the single biggest organizational vulnerability of cyber systems – people. The largest category of attacks on cyber systems is not from hackers to the system, but from insiders who already have access. This chapter describes numerous mechanisms to aid the HR department in mitigating this threat.
- Chapter Three provides a framework for analyzing the ever-changing legal and compliance regimes that organizations will have to manage as governmental attention naturally increases.

- Chapter Four describes how operational and technical issues can be better understood and integrated into an enterprise-wide risk management regime.

- Chapter Five lays out the comprehensive communication program that organizations need to prepare before, during, and after a cyber incident. Multiple different audiences need to be addressed, and this chapter provides a framework for developing and implementing these critical programs.

- Chapter Six addresses the issue of risk management and transfer. Even the most prepared organizations can still be compromised. Prudent organizations will have prepared for this eventuality, and this chapter provides the framework for conducting this analysis.

By now virtually every company has factored the positive aspects of digitalization into their pro-growth business plans, perhaps through web marketing, online inventory management, or international partnerships. But the potential risk these new cyber systems create has not received the necessary attention from decision makers, leaving the door open to potential cyber attacks and data breaches. Those companies that bury these concerns in overburdened IT departments and fail to address these issues head-on through an enterprise-wide, financially based analysis are not just endangering their own intellectual property, market share, and consumer faith, they are also putting our national security at risk.

Cybersecurity is vital to our economic well-being – both on an enterprise level and a national level. ISA and ANSI are pleased to offer this volume as a pragmatic first step in the effort to create a sustainable system of 21st century information security. If you have questions about this initiative or would like to get involved, please contact us at www.isalliance.org or www.ansi.org.