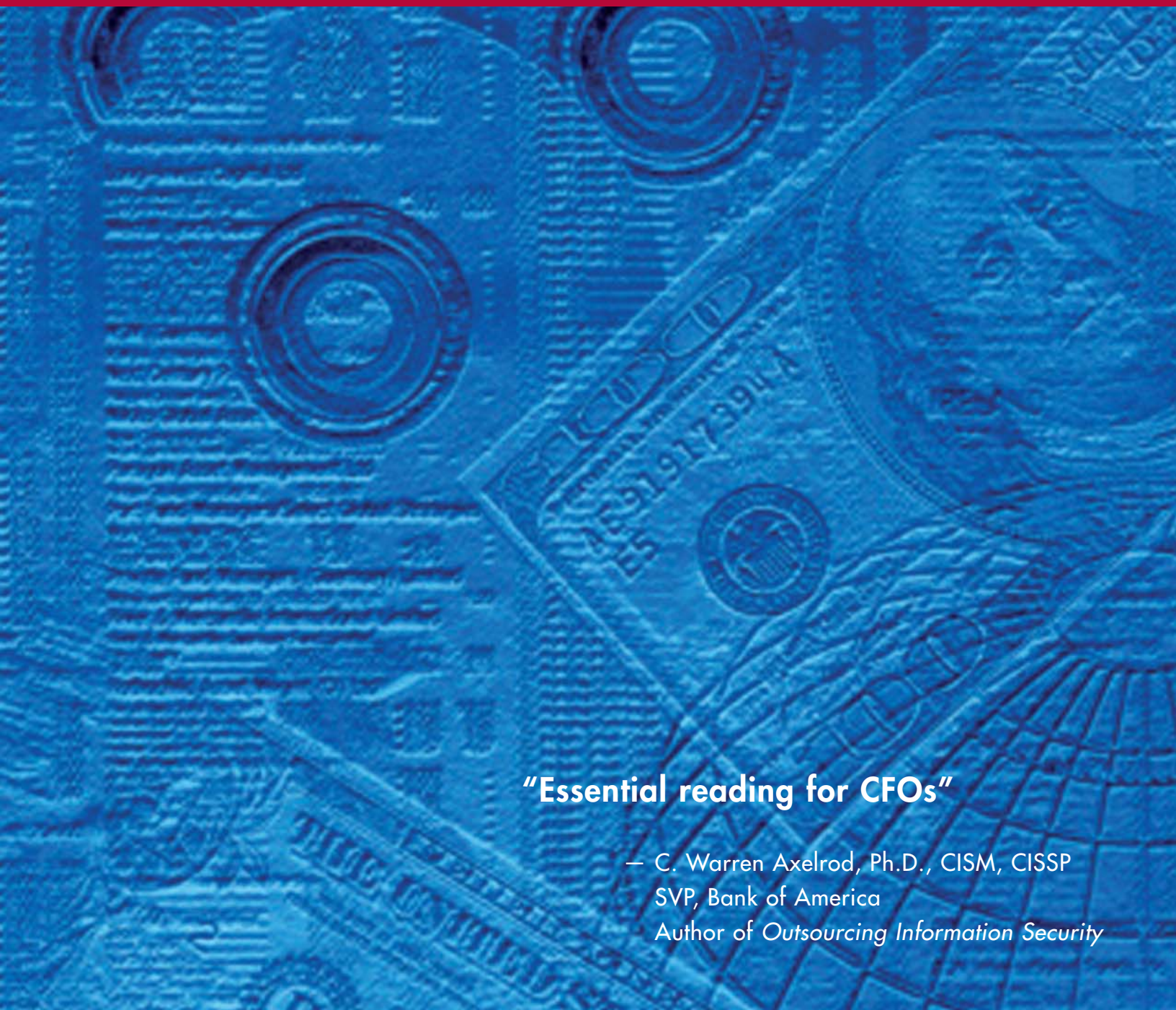
ANSI
American National Standards Institute

INTERNET SECURITY ALLIANCE

THE FINANCIAL IMPACT OF CYBER RISK

50 QUESTIONS EVERY CFO SHOULD ASK



"Essential reading for CFOs"

— C. Warren Axelrod, Ph.D., CISM, CISSP
SVP, Bank of America
Author of *Outsourcing Information Security*

Material in this publication is for educational purposes. Neither the publisher nor the authors assume any liability for any errors or omissions or for how this publication or its contents are used or interpreted or for any consequences resulting directly or indirectly from the use of this publication. For legal advice or any other, please consult your personal lawyer or the appropriate professional.

The views expressed by the individuals in this publication do not necessarily reflect the views shared by the companies they are employed by (or the companies mentioned in this publication). The employment status and affiliations of authors with the companies referenced are subject to change.

TABLE OF CONTENTS

APPENDICES

ACKNOWLEDGEMENTS

The following professionals participated in one or more of the ANSI-ISA 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	Richard Billson*, Nancy Callahan*, Paul de Graaff*, Robert Roche*, Ty R. Sagalow†
American National Standards Institute	Jessica Carl*, Matt Deane*
Aon	Patrick Donnelly*
Beazley Group plc	Bob Wice*
Booz Allen Hamilton	Will Robinson*
CNA Insurance	John Wurzler*
Carnegie Mellon University — Software Engineering Institute	David White
Crimson Security	Narender Mangalam
Direct Computer Resources, Inc.	Ed Stull*
Ernst & Young LLP	Jennifer Celender*, Seth Rosensweig*
Guy Carpenter	Harry Oellrich*
Hunton & Williams	Lon Berk*
IBM Tivoli Software	Eric McNeil*
ID Experts	Christine Arevalo*, Rick Kam*, Jason Porter
Internet Security Alliance	Barry Foer*, Larry Clinton*
KPMG LLP	Neil Bryden, Cole Emerson*
Lockheed Martin Corporation	Ben Halpert*
Marsh, USA	Nadia Hoyte*, Robert Parisi*
Moody's Risk Services	Edward Leppert*
New York Metro InfraGard	Joseph Concannon*, Phil Froehlich*, Vincent Orrico*
Quality Plus Engineering	Greg Hutchins*
Reed Elsevier	Arnold Felberbaum*
Robinson Lerer & Montgomery	Anne Granfield*, Michael Gross*
State Farm Insurance	Bob Hillmer*
U.S. Cyber Consequences Unit	Scott Borg*
U.S. Department of Commerce	Michael Castagna*
U.S. Department of Justice	Martin Burkhouse*
U.S. Department of Homeland Security	
Office of Infrastructure Protection	Chris Watson*
Science & Technology Directorate	Peter Shebell*
University of California, Berkeley	Aaron Burstein*
Willis	Tom Srail*

* Task Group Participant † Workshop Leader

Thanks and acknowledgement are given for the support and participation of all the organizations that supplied experts to this initiative. Without the contributions from 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 **American International Group** (AIG) for being the Workshop Leader of this initiative. Mr. Sagalow's leadership and dedication in helping to shape the initiative, lead its proceedings, and build consensus for the final deliverable was instrumental in reaching a successful outcome. Thanks also to **Richard Billson** of AIG for his added support in this regard.

- 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 **Matt Deane** and **Jessica Carl** of ANSI and **Larry Clinton** and **Barry Foer** of ISA.

- Special acknowledgement is given to **American International Group** (AIG) for hosting and sponsoring the first two Workshop meetings, the **American National Standards Institute** (ANSI) for hosting the final meeting, and to **Direct Computer Resources, Inc.** for sponsoring the final meeting.

- 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.

  Regan Adams, Vice President and Assistant General Counsel in the Contracts, Privacy & IP Legal group, Goldman Sachs
  C. Warren Axelrod, SVP, Privacy and Security, Bank of America
  Lawrence Berk, President and CEO, Baron Group, USA
  Joe Buonomo, President and CEO, Direct Computer Resources, Inc.
  George Carruthers, Chief Financial Officer, LoneStar National Bank
  Phillip Chappo, First Vice President and Acting CFO, Credit Industriel et Commercial
  Richard Davis, Chief Financial Officer, The George Washington University Hospital
  Robert Gardner, Founding Partner, New World Technology Partners

- Thank you to **Ed Stull**, sponsored by Direct Computer Resources, Inc., for leading this special advisor review effort and for providing the consolidated and insightful feedback to the Workshop leaders.

- Finally, thank you to **U.S. Department of Homeland Security Assistant Secretary for Cyber Security and Communications Greg Garcia** for his support in framing this Workshop and for the continued efforts of his program in furthering cyber security preparedness within our nation.

INTRODUCTION

Cyber security[1] is vital to America's economic well-being. Its importance was underscored in 2008 by U.S. Homeland Security Secretary Michael Chertoff, who named it one of the nation's four priority security issues, alongside border security.

Corporations use cyber systems to accomplish real-time tracking of supply chains, manage inventory, improve employee efficiency, generate on-line commerce, and more. Virtually every corporation has, by now, calculated the positive aspects of digitalization into its immediate and long-term business plans.

Unfortunately, corporations have often failed to properly account for the financial downside resulting from the risks of cyber systems.

Corporate America cannot be completely faulted for this deficiency, since to date there has not been any *agreed upon* methodology for understanding and mitigating the potential *financial losses* associated with network security and cyber risk. The classic financial risk management discipline that Chief Financial Officers and Risk Managers use to deal with brick-and-mortar risks has not been systematically applied to digital risks. While there is a substantial body of work dealing with the *technical* standards of network, internet and computer system security and plenty of attention has been paid to important issues such as data encryption and best-in-class security technologies, *classic financial risk management*— as it pertains to cyber security exposures—has been largely overlooked.

The purpose of this work is to correct that deficiency by providing guidance in both the identification and quantification of the financial risk due to issues related to information security.[2]

Thanks to the joint effort organized by the American National Standards Institute's (ANSI) Homeland Security Standards Panel (HSSP) and the Internet Security Alliance (ISA), with input provided by the many industry and public sector professionals who contributed their time and energy, the work represents an Action Guide that private sector enterprises can undertake to assess and address the financial exposure of cyber security from all angles. It is a tool the CFO — and often other executives — can use to build a framework for analyzing, managing and transferring the Net Financial Risk (defined below) of cyber security. As opposed to focusing on technological standards or even best practices, this guide is presented to further advance the understanding of financial management.

1 Cyber security might be defined as the protection of any computer system, software program and data against unauthorized disclosure, transfer, modification or destruction, whether accidental or intentional. Cyber security attacks can come from internal networks, the internet or other private or public systems.

2 Throughout this work, the terms "cyber security," "network security" or "information security" may be used interchangeably.

A frightening fact every CFO must face is that the financial consequences of cyber security, or more pointedly, of cyber security "events" can be substantial. The total average costs of a data breach grew to $197 per record compromised in 2007.[3] Since January 2005, the Privacy Rights Clearinghouse has identified more than 230 million records of U.S. residents that have been exposed due to security breaches.[4] Costs have increased in terms of lost business, legal defense and public relations.[5] An organization that is unprepared to avert or manage a data breach can suffer severe financial losses and irreparable damage to its reputation and customer base. Conversely, when an organization is prepared and responds skillfully to a cyber threat, the crisis can go down in history as an event that cements customer loyalty and a positive brand image.

The key to understanding the financial risks of cyber security is to fully embrace its multi-disciplinary nature. Cyber risk is not just a "technical problem" to be solved by the company's Chief Technology Officer. Nor is it just a "legal problem" to be handed over to the company's Chief Legal Counsel; a "customer relationship problem" to be solved by the company's communications director; a "compliance issue" for the regulatory guru; or a "crisis management" problem. Rather, it is all of these and more.

To successfully analyze and manage financial risk requires a dialogue, sparked by a series of pointed questions directed at the major stakeholders in all corporate domains: the Chief Legal Counsel, Chief Technology Officer, Chief Risk Officer, heads of Corporate Communications, Investor Relations and Customer Service. Each of these individuals should be "in the room" with a surprised CFO finding that individuals with different positions in the company giving very different, sometimes contrary, advice to the same question. Of course, the foregoing list is not intended to be exhaustive and, depending on the enterprise in question, may need to include other stakeholders. For example, the head of Human Resources might be given a seat in the room given the correlation between the management and training of employees and the potential for internal cyber attacks.[6]

This Action Guide provides a practical, immediately actionable guide on how to bring the multiple stakeholders in cyber security together and give them, in the form of strategic questions, a roadmap for developing a multi-disciplinary risk management approach to analyze, manage and mitigate the financial risks of cyber security. The answers to these questions will better enable a company's CFO to determine the company's "Net Financial Risk."

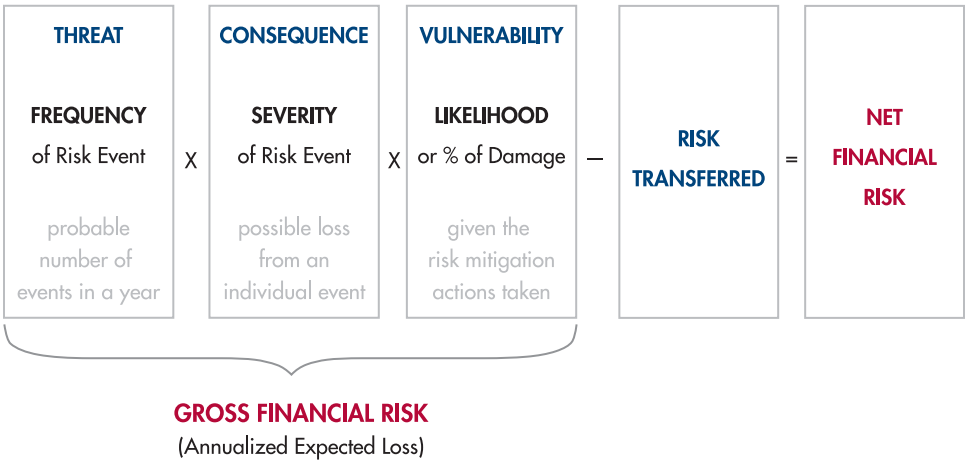
3 2007 Annual Study: U.S. Cost of a Data Breach. Benchmark research conducted by Ponemon Institute, LLC ("Ponemon Study").

4 Organization such as the Privacy Rights Clearinghouse and Attrition track and publish information on data breaches. For more information visit www.privacyrights.org and www.attrition.org.

5 Ponemon Study, pages 2-3.

6 The term "cyber attack" is meant to be broadly understood to include both external and internal attacks whether launched intentionally or unintentionally. Recent studies continue to indicate that internal attacks are generally more frequent than external ones.

Net Financial Risk can be expressed as follows:



As companies go through the questions posed in this work, they will find the answers can be plugged into the above formula, enabling them to better quantify their own net cyber risk. However, it is important to understand that the quantitative evaluation of these factors (Threat, Consequences, and Vulnerability) must be qualified by the degree of *confidence* the organization has in the accuracy of each factor. In other words, in addition to the probability of loss, there is the probability of the estimate of the probability of loss being accurate. Once the risk equation has been qualified by the degree of confidence, it provides a sound basis for guiding all risk management decisions.

In addition, several useful charts are included in the Appendices that can be customized to help measure the Net Financial Risk of a company, together with lists of helpful web sites and technical standards.

In each of the chapters that follow, it is generally the CFO who is envisioned to be asking the questions. Yet this Action Guide is also of direct benefit to all of the aforementioned stakeholders, all of whom should be "in the room" when the questions are asked … to provide the answers, to listen to the answers, and to act on them.

For each enterprise, individual answers may be different. Routes will vary, yet the destination for all private sector enterprises embarking on this cyber risk management methodology is a common one: an immediately actionable understanding of the Net Financial Risk of cyber security through which the CFO, with the executive team, can make informed decisions about which "risk management actions" (if any) are to be implemented.

Let the process, and the preparation, wait no longer.

Gather the stakeholders.

Let the questions begin.