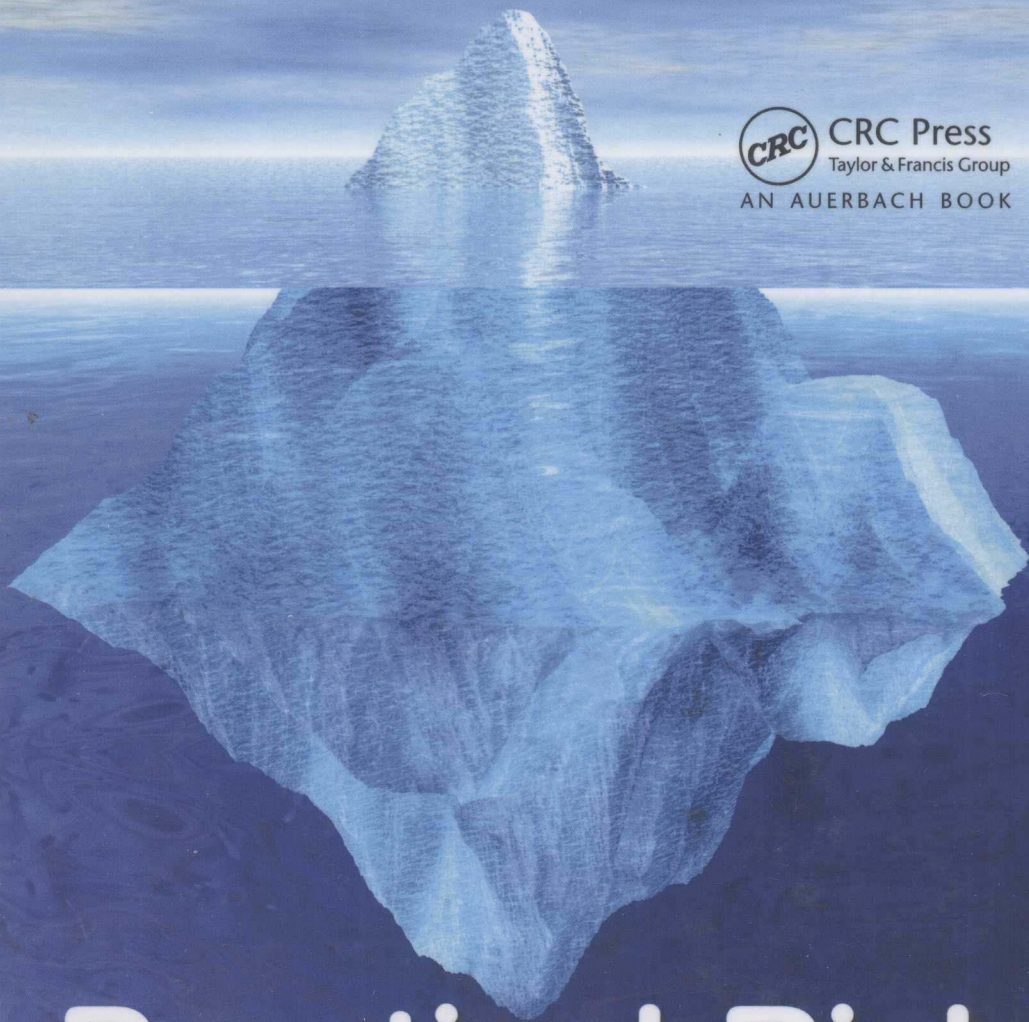




CRC Press
Taylor & Francis Group

AN AUERBACH BOOK

A large, jagged iceberg floats in a dark blue ocean under a cloudy sky. The visible tip of the iceberg is small and pointed, while the submerged portion is much larger and more complex in shape, illustrating the concept of hidden risks.

Practical Risk Management for the CIO

Mark Scherling

Auerbach Publications
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

© 2011 by Taylor and Francis Group, LLC
Auerbach Publications is an imprint of Taylor & Francis Group, an Informa business

No claim to original U.S. Government works

Printed in the United States of America on acid-free paper
10 9 8 7 6 5 4 3 2 1

International Standard Book Number: 978-1-4398-5653-6 (Hardback)

This book contains information obtained from authentic and highly regarded sources. Reasonable efforts have been made to publish reliable data and information, but the author and publisher cannot assume responsibility for the validity of all materials or the consequences of their use. The authors and publishers have attempted to trace the copyright holders of all material reproduced in this publication and apologize to copyright holders if permission to publish in this form has not been obtained. If any copyright material has not been acknowledged please write and let us know so we may rectify in any future reprint.

Except as permitted under U.S. Copyright Law, no part of this book may be reprinted, reproduced, transmitted, or utilized in any form by any electronic, mechanical, or other means, now known or hereafter invented, including photocopying, microfilming, and recording, or in any information storage or retrieval system, without written permission from the publishers.

For permission to photocopy or use material electronically from this work, please access www.copyright.com (<http://www.copyright.com/>) or contact the Copyright Clearance Center, Inc. (CCC), 222 Rosewood Drive, Danvers, MA 01923, 978-750-8400. CCC is a not-for-profit organization that provides licenses and registration for a variety of users. For organizations that have been granted a photocopy license by the CCC, a separate system of payment has been arranged.

Trademark Notice: Product or corporate names may be trademarks or registered trademarks, and are used only for identification and explanation without intent to infringe.

Visit the Taylor & Francis Web site at
<http://www.taylorandfrancis.com>
and the Auerbach Web site at
<http://www.auerbach-publications.com>

Preface

Information is the lifeblood of any organization. Without good information, poor decisions are made, risks are not recognized and communicated, and valuable information is lost or stolen. Cyber risks are increasing, and these risks are seriously impacting organizations. Without good information risk management, customer trust and loyalties as well as the organization's reputation and brand are at risk. In taking a more holistic approach to information risk management, we encompass the risks to service delivery, information management, as well as information protection. Chief Information Officers (CIOs) are tasked with delivering information to the organization. In essence, this means making sure the right information is available to the right person at the right time to enable people to do their jobs and make good decisions. It also means making sure the wrong information is not being given to the wrong person at the wrong time, thereby increasing risks to the organization.

It is time for CIOs to relook at how they are organized and realign with what is important to the business. CIOs deliver information to the business. Good information is what is important to the business. Any Chief Executive Officer (CEO) or executive will tell you that without good information they cannot make good decisions. This means that information must be findable, managed, protected, and available. Risks to information must be managed and mitigated. The

costs of mismanagement or ignoring risks are huge. Fines, noncompliance, breaches, loss of trust, loss of reputation, loss of key personnel, and perhaps jail time can occur if risks are ignored. CIOs must better improve the management of risks to their information. This book gives the reader some solid foundations for improving information risk management.

Acknowledgments

Many people encouraged me to write this book. Although I will miss a few names, I would like to acknowledge a few who really helped me. To

Robin Wakefield, who has helped me in many of my thoughts, especially some of the more radical ones.

Michael Legary, who was so enthusiastic about my book that he read it forward and backward.

Richard Mandy, who kept me thinking out-of-the-box.

Richard Hakim, who helped edit some key sections.

Shayne Fynes, who encouraged me to write it and said that he would be the first one to buy my book.

Joe Gollner, who helped me with the information management.

My wife Gerry, who tolerated my rants and raves about Microsoft Word®, formatting documents, and some other things about word processing software. She gave me time to write this book.

My brother Gary Scherling, who is a Project Manager and helped write the section on Project Management.

Some of my friends John, Mike, and Caner, and to my colleagues in the British Columbia (BC) Government, who encouraged me to write this book.

About the Author

Mark Scherling, CISSP, CRM, has been working in IT for over 30 years. For the past four years, he has been managing information security and privacy for the Justice Sector in the Government of British Columbia (Canada). Prior to the Justice Sector, he managed the Information Security Investigations Unit for the entire BC government. He has designed and implemented public key infrastructure (PKI) and security solutions for numerous clients.

He is considered a Subject Matter Expert in Risk Management and Information Security by the Information Systems Audit and Control Association (ISACA). He contributed to the Risk IT Framework and Certification in Risk and Information Systems (CRISC), a new ISACA Certification. He is viewed as a Security and Risk Management Expert by many people within and associated with the Government of British Columbia.

His background includes sales, marketing, and information management. In the mid-1990s, he was instrumental in developing and implementing the Canadian Department of National Defence Intranet or the DIN. He has significant experience in information and knowledge management. He combines this expertise with information protection to create an information risk management strategy for Chief Information Officers (CIOs).

He has been part of the evolution of information technology (IT) from Digital Equipment's Vaxes and PDP11s to mobile computing, the Internet, and cloud computing. The interconnected world we now live in holds exciting promise to link people, computers, applications, and information. There are risks when we link everything together and share information. Organizations are always trying to reduce costs and improve customer relations. Mark has been involved in information security for over 13 years and has oriented his approach from simple information security to risk management strategies. As the Internet continues to evolve, so evolves information security and risk management. The reality is that we need better ways of managing risks to our information and services. His approach takes a more holistic approach to risks, considering not just liabilities but also service delivery because information is one of our most important assets.

Contents

PREFACE	ix
ACKNOWLEDGMENTS	xi
ABOUT THE AUTHOR	xiii
CHAPTER 1 INTRODUCTION: WHY RISK MANAGEMENT?	1
CHAPTER 2 LIABILITY	9
Personal Data Disclosed or Stolen	10
Intellectual Property Lost or Stolen	12
Wrong Decisions Made	15
Liability Risks	16
CHAPTER 3 SERVICE DELIVERY	19
Transaction Centric	20
Information Centric	21
Risks to Service Delivery	22
Risks to the CIO	22
 PART I PRINCIPLES AND CONCEPTS	
CHAPTER 4 OVERVIEW	25
Market Risks	25
Budget Risks	26
People Risks	27
Technology Risks	28
Operational Risks	28
Information Risks	28

Control Risks	29
Detection Risks	29
Risk Treatment	29
CHAPTER 5 BASIC CONCEPTS, PRINCIPLES, AND PRACTICES	31
Concepts	31
Risk IT Framework Principles	32
ISO 31000 Risk Management Principles	33
Other Risk Management Principles	35
Summary: Risk Management and Risk IT Principles	38
Information Security Principles	39
Accountability Principle	39
Awareness Principle	40
Ethics Principle	41
Multidisciplinary Principle	41
Proportionality Principle	42
Integration Principle	43
Timeliness Principle	43
Assessment Principle	44
Equity Principle	45
Information Management Principles	46
Value	46
Life Cycle	46
Reuse	47
Proliferates Quickly	48
Dependencies	48
Principles	49
CHAPTER 6 RISK ASSESSMENT, ANALYSIS, AND PROCEDURES	51
Making Decisions: Fact or Fiction? How Do You Decide?	51
Confidence Ranking Process	53
Facts	55
Calculations	56
Estimations	56
Guesses	56
Risk Management Starts with the Individual	60
Managing Risky People	63
Risk Management Profiling and Risk Culture	66
Measuring Risks or Uncertainty	67
How to Measure Risks	70
Identify the Risk	71
Consensus of the Risk	71
Analysis of Risk	72
Mitigate the Risk	75
Monitor the Risk	76

Reassess the Risk	76
Performing a Risk Assessment	76
Team or Committee Selection	80
Step 1: Define Parameters	80
Taxonomy of Risk Types	81
Scope, Time Frame, Complexity, and Stakeholders	81
Step 2: Identify Risks and Impacts	85
Step 3: Consensus of Risks and Impacts	86
Step 4 Risks and Impacts Analysis	87
Step 5: Prioritize Risks and Impacts	89
Step 6: Review Existing Controls	92
Step 7: Risks and Impacts Mitigation Analysis	93
Step 8: Costing, Prioritization, and Decisions	94
Step 9: Implementation	95
Step 10: Review	95
CHAPTER 7 METRICS	97
User Experienced Metrics	98
CHAPTER 8 BEST PRACTICES	103
CHAPTER 9 PRINCIPLES AND CONCEPTS: SECTION SUMMARY	105
 PART II SERVICE DELIVERY	
CHAPTER 10 PRODUCT MANAGEMENT	113
Products You Deliver as a CIO	120
Information Delivery: How Information Flows in Your Organization	122
Organizing IT for Information Delivery, Management, and Protection	124
CHAPTER 11 PROCESS MANAGEMENT	127
CHAPTER 12 PROJECT MANAGEMENT	141
Projects	144
Risk Ranking	147
Vulnerability Scanning	147
Reporting	149
CHAPTER 13 IT SERVICE MANAGEMENT	153
Opportunity Capacity	154
CHAPTER 14 REPORTING ON SERVICE DELIVERY	157
CHAPTER 15 SERVICE DELIVERY: SECTION SUMMARY	159

PART III LIABILITIES MANAGEMENT

CHAPTER 16 INFORMATION MANAGEMENT	167
The Value of Information	168
Classify Your Information: Value and Categories	174
Value/Sensitivity of Information	175
Categories of Information	177
Controlled Vocabulary, Taxonomies, Keywords, and Search	179
Controlled Vocabularies	181
Summary	189
Identify Information Assets	190
Information Has a Life Cycle	192
Database Information Life Cycle	196
Information Flows	197
Information Flow Analysis	199
Information Management Strategy	202
Designing Information Management across Large Organizations	207
Steps to Better Information Management	216
CHAPTER 17 INFORMATION PROTECTION	221
Security Controls	225
Essential Controls	227
Personnel (Includes Management and Operations)	228
Technology	230
Information	232
Ingress	233
Egress	234
Database Security and Monitoring	235
Defense in Depth	237
Audit and Compliance	238
Documentation	239
Information Security Architecture	240
Reporting on Information Security	244
FISMA, NIST, and FIPS	246
Why	247
What	247
Specifications for Minimum Security Requirements	249
How	254
Payment Card Industry Data Security Standard	255
Analysis of Good Information Security Practices	258
Employee, Hacker, Insider, or Outsider	261
Insiders	263
Employees	264
Partners	266
Contractors	266
Outsourced	267
Insider Threats	267

Insider Controls	268
Outsiders	269
General Public	269
Hackers	269
Customers, Clients, Others	270
Outsider Threats	270
Outsider Controls	271
Data Loss Prevention/Information Knowledge Leakage	271
Database Solutions	275
Network and End-Point Solutions	276
Portable Device Control	277
Defining the Risk	277
Deploying DLP Solutions	279
Paper: Print, Keep, Shred	282
CHAPTER 18 E-Discovery	287
Rules and Obligations	289
Standard of Proof	290
E-Discovery Process	292
Information Management	292
Collection and Preservation	293
Production	294
Presentation	294
Summary of E-Discovery	295
CHAPTER 19 PRIVACY	299
CHAPTER 20 POLICIES AND PROCEDURES	303
Writing Good Policies	305
Communicating Policy	307
Enforcing Policy	308
Writing Good Procedures	309
Following Procedures	310
Next-Generation Policies and Procedures	311
CHAPTER 21 PLANNING FOR BIG FAILURES OR BUSINESS	
CONTINUITY	313
Business Resilience and Redundancy	316
Business Continuity Management	318
CHAPTER 22 LIABILITIES MANAGEMENT: SECTION SUMMARY	321
PART IV PUTTING IT ALL TOGETHER	
CHAPTER 23 DESIGNING A RISK MANAGEMENT STRATEGY	329
External Factors	330
Organization Structure	331
Identify Assets	331

Compliance Requirements	332
Risk Management Profiles	332
Risk Culture	332
Governance	333
Risk Management Strategy for Service Delivery	333
Risk Management Strategy for Liabilities	333
Consolidated Risk Management Strategy	333
Risk Management Framework: Outline	334
Maintain Risk Management Program	335
Resourcing a Risk Management Program	336
CHAPTER 24 FORWARD-LOOKING RISK MANAGEMENT	337
CHAPTER 25 PREPARING FOR A “BLACK SWAN”	341
CHAPTER 26 CONCLUSION	343
APPENDIX A: OECD PRIVACY PRINCIPLES	347
APPENDIX B: PROJECT PROFILING RISK ASSESSMENT	351
APPENDIX C: RISK IMPACT SCALES	355
APPENDIX D: CLASSIFICATION SCHEMA	359
BIBLIOGRAPHY	363
INDEX	371

INTRODUCTION

Why Risk Management?

The purpose of this book is to help Chief Information Officers (CIOs), Chief Information Security Officers (CISOs), Chief Risk Officers (CROs), Information Management/Information Technology (IM/IT) Security Professionals, and IM/IT Managers deal with IM/IT risks. IM/IT risks are not all about information security. The CIO must deliver IM/IT services to enable the business to run effectively. The CIO must also protect information to prevent it from being lost or stolen. The CIO walks on the edge of a sword, balancing *service delivery* on one side and *liabilities* on the other. Straying too far on either side will result in failure, and that failure may be catastrophic.

We have been managing risk from the time we left the trees to modern times. Our risk model is still based on primal instincts (fight or flight). It was very simple and our choices were simple. We made the choice to eat, get eaten, or run away. We had to decide if the tiger was smiling because its belly was full or because it saw us as the next meal. We still use that same habitual way of thinking to deal with today's "tigers," and we can be led to make less than optimal decisions.

At a basic instinct level, our risk management skills are not well suited to making risk decisions in the complex environment in which we live today. If you consider a medium-sized network of 4,000 devices with routers, switches, servers, workstations, and printers, about 6.9 billion electronic events are generated every working day. Now think about which of those events could affect you or your organization in a negative way. How about in a positive way? We need tools, processes, and methodologies to help us make informed decisions when managing risks, especially information and IT risks.

With the advent of the Internet we now have a single worldwide network or, as Kevin Kelly from *Wired Magazine* describes it, "The

Machine.” The Machine is composed of billions of computers, routers, switches, and mobile devices, all with a view into this network. And with this single network we have ways of doing amazing things. We can communicate around the world. People can read what is going on across the planet almost at the moment an event is happening. Think about some of the events that have occurred over the past decade and we knew about it the minute it was happening. We see pictures of disasters within minutes of the disaster happening. People have digitized this world into The Machine. And it will become far more connected. And the risks? If you don’t keep up, you will fall behind and become a have-not. If you keep up, you pay the price of evolving faster than your people can evolve. You end up with technology that is too sophisticated to be understood. You end up with too many events happening. And you cannot make good decisions without good information.

We are in a war zone and we do not know it. The war zone is cyberspace. The events that happen in cyberspace happen a million times faster than events in real-time. The events happen all over the world and it is a global economy. Because we are all connected, we also are connected to people with criminal intent. Those people are intent on stealing your money, information, and anything of value. The world market for information is in the trillions of dollars. And it does not matter how it was gotten—the market is there for information.

Today the biggest risk in cyberspace is misunderstanding. According to the Internet Security Alliance (ISA) and the American National Standards Institute (ANSI) report entitled “The Financial Management of Cyber Risk,” most executives wait until they are compromised to put a reactive plan in place. Waiting until after the problem has occurred damages reputations and costs more money. Reactive plans are too late. It is the proverbial “closing the gate after the horses are gone.” According to the Ponemon Institute, the average incident cost to an organization rose from \$4.5 million in 2005 to \$6.65 million in 2009 for a security breach involving credit cards. And we cannot estimate the damage to reputation—not to mention the theft of intellectual property that has cost billions of dollars. It has cost companies dearly.

Risk management is something we do every day. We manage risks as we walk across a street or drive down the highway. On an

individual basis, we manage risks fairly well, although we always hear stories about people who do not think about the risks and manage to hurt themselves or worse because they did something stupid. At an *organizational level*, we do not manage risks well. This is due to the complexity of organizations and systems. At some levels, we manage risks fairly well. However, as we have seen in many of the failures of organizations, risk was not managed well. *Risk management* is ad hoc management at best.

We have not formalized risk management in most organizations. The closest we come to enterprise risk management is the auditors and the board. In some organizations there is the recognition that risk must be managed at the corporate level and executives must be aware of risks in making key business decisions. In those organizations, there is an audit advisory committee that advises the board and directors on business risks. These are key business decisions that change the way an organization conducts business. Typically, these are focused on *rewarded risks*, which are risks associated with investments that create value for shareholders. What is missing is the incorporation of operational risks into these key business decisions. As indicated by a number of studies, operational failures can cause significant losses. In reality, risk management is still very much fragmented and managed within business lines and geographic boundaries.

Even more fragmented are risks associated with IM/IT. The reality is that we are all heavily invested in cyberspace. We do business in cyberspace because it reduces our costs. We do business in cyberspace because our partners and customers do business there. We use Web sites to provide information to our customers, our partners, and our competitors. We use the Web to inform, transact, and communicate. We do not manage the risks associated with cyberspace as business risks. Cyberspace is an enterprisewide risk management issue. It should be at the board. It should have a strategic, cross-organization focus.

Cyberspace has both rewarded risks and unrewarded risks (the organization is compelled to invest in security to prevent data loss or meet compliance). The requirement is to recognize that cyberspace risks are both horizontal across the organization and vertical within business units.

Risk management is an integral oversight function to help organizations avoid or mitigate situations or events that can harm individuals,

groups, or the organization. Risk management is not just about organizational harm, but is also about how services are delivered. Risk management does not reduce risks; it measures and reports risks.

It is really simple why you manage risks:

- To reduce or mitigate liabilities
- To improve or maintain service delivery

Information risk management is about getting the right information to the right person at the right time while preventing the wrong information from getting to the wrong person at the wrong time. And what we are seeing is that information risk management is still considered a technical issue to be dealt with by IM or IT staff. According to the ISA-ANSI publication *The Financial Management of Cyber Risk* most enterprises categorize information security as a technical or operational issue to be managed by the IT department. This misinformation is being fed by outdated corporate structures and the lack of an overall strategy dealing with information risk management.

In the ISA-ANSI publication, they indicate that the Chief Financial Officer (CFO) as opposed to the CIO or CISO should be the most logical person to lead enterprise risk management, including information risk management. The problem is one of education and time. To properly inform a CFO, they need to have some background in IM/IT to understand some of the nuisances that make up information technology. Because of the complexity, there is no single person who has that understanding. That is why we must automate risk management to allow the information to be presented in a meaningful way. The Federal Information Security Management Act (FISMA), which was passed in 2002, is now looking toward continuous monitoring or near-real-time risk management so that on a real-time basis, senior executives understand the security state of their information systems.

We need to consider risk management starting at the top. We have all heard of enterprise risk management (ERM). ERM is usually practiced at the board or executive level in making strategic decisions. At the enterprise level, risk management as defined by ISO 31000 (2009) enables an organization to

- Increase the likelihood of achieving objectives;
- Improve the identification of opportunities and threats;