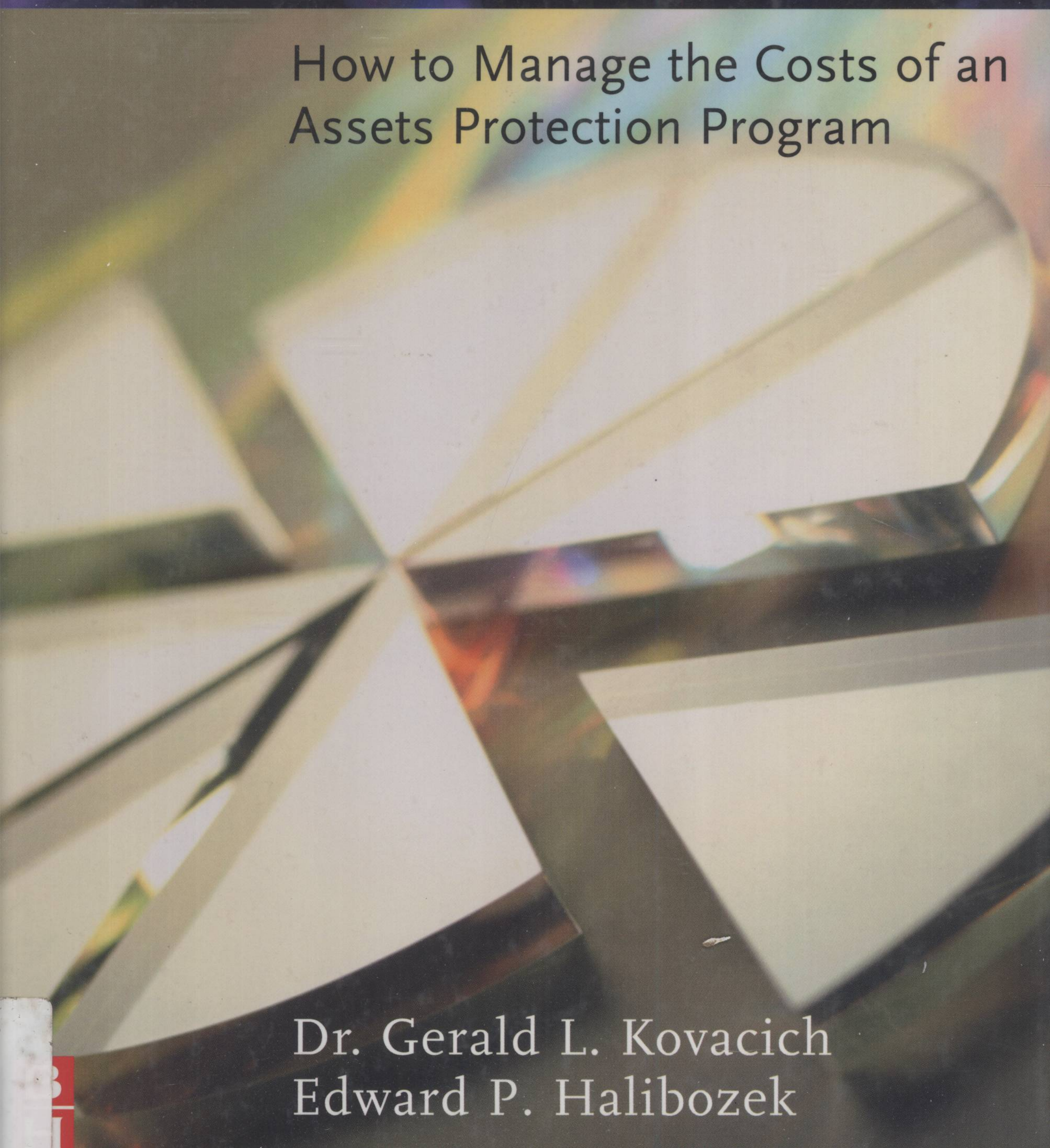
# Security Metrics Management

## How to Manage the Costs of an Assets Protection Program



Dr. Gerald L. Kovacich
Edward P. Halibozek

# SECURITY METRICS MANAGEMENT

## How to Measure the Costs and Benefits of Security

*Dr. Gerald L. Kovacich*
*Edward P. Halibozek*

ELSEVIER

AMSTERDAM • BOSTON • HEIDELBERG • LONDON
NEW YORK • OXFORD • PARIS • SAN DIEGO
SAN FRANCISCO • SINGAPORE • SYDNEY • TOKYO

Butterworth-Heinemann is an imprint of Elsevier

B
H

Butterworth–Heinemann is an imprint of Elsevier
30 Corporate Drive, Suite 400, Burlington, MA 01803, USA
Linacre House, Jordan Hill, Oxford OX2 8DP, UK

Recognizing the importance of preserving what has been written, Elsevier prints its books on acid-free paper whenever possible.

**Library of Congress Cataloging-in-Publication Data**
Kovacich, Gerald L.
Security metrics management : how to measure the costs and benefits of security / by Gerald Kovacich and Edward Halibozek.
p. cm.
Includes index.
ISBN 0-7506-7899-2 (pbk. : alk. paper) 1. Private security services. 2. Security systems. 3. Corporations--Security measures. 4. Corporations--Security measures--Costs. I. Halibozek, Edward P. II. Title.
HV8290.K684 2006
658.4'70681--dc22
2005025565

**British Library Cataloguing-in-Publication Data**
A catalogue record for this book is available from the British Library.

ISBN 13: 978-0-7506-7899-5
ISBN 10: 0-7506-7899-2

For information on all Butterworth–Heinemann publications
visit our Web site at www.books.elsevier.com

Printed in the United States of America
05 06 07 08 09 10 10 9 8 7 6 5 4 3 2 1

# Security Metrics Management

# Other Books by Dr. Gerald L. Kovacich

- *Information Systems Security Officer's Guide: Establishing and Managing an Information Protection Program*, May 1998, ISBN 0-7506-9896-9, First Edition and July 2003, ISBN: 0-7506-7656-6, Second Edition; published by Butterworth-Heinemann (Czech translation of First Edition also available).
- *I-Way Robbery: Crime on the Internet*, May 1999, ISBN 0-7506-7029-0; co-authored with William C. Boni; published by Butterworth-Heinemann; Japanese version published T. Aoyagi Office Ltd, Japan: February 2001, ISBN 4-89346-698-4.
- *High-Technology Crime Investigator's Handbook: Working in the Global Information Environment*, September 1999, ISBN 0-7506-7086-X; co-authored with William C. Boni; published by Butterworth-Heinemann; Second Edition co-authored with Andy Jones to be published in early 2006.
- *Netspionage: The Global Threat to Information*, September 2000, ISBN 0-7506-7257-9; co-authored with William C. Boni; published by Butterworth-Heinemann.
- *Information Assurance: Surviving in the Information Environment*, September 2001, ISBN 1-85233-326-X; co-authored with Dr. Andrew J. C. Blyth; published by Springer-Verlag Ltd (London); Second Edition to be published in late 2005.
- *Global Information Warfare: How Businesses, Governments, and Others Achieve Global Objectives and Attain Competitive Advantages*, June 2002, ISBN 0-84931-114-4; co-authored with Andy Jones and Perry Luzwick; published by Auerbach Publishers/CRC Press.

**Other Books by Dr. Gerald L. Kovacich and Edward P. Halibozek**

- *The Manager's Handbook for Corporate Security: Establishing and Managing a Successful Assets Protection Program*, April 2003, ISBN 0-7506-7487-3; published by Butterworth-Heinemann.
- Instructor's Manual for *The Manager's Handbook for Corporate Security: Establishing and Managing a Successful Assets Protection Program*, 2005, ISBN 13: 978-0-750-67938-1; ISBN 10: 0-750-67938-7, published by Butterworth-Heinemann.
- *Mergers & Acquisitions Security: Managing Security Issues Before, During and After a Merger or Acquisition*, April 2005, ISBN 0-7506-7805-4; published by Butterworth-Heinemann.

This book is dedicated to all the security professionals who try to justify their assets protection programs, their budgets, and their jobs!

A special dedication to a great criminologist, mentor and friend:
John P. Kenney, Ph.D., Professor Emeritus. Thanks, Jack! We miss you!

# Preface

This book, *Security Metrics Management,* is designed to provide *simple* and *basic* guidance to security professionals and managers for establishing a baseline to begin the process of measuring the costs and benefits of their assets protection program—their security program—as well as its successes and failures—its effectiveness. We begin where all assets protection policies, procedures, processes, plans and projects should start—with the assets protection security drivers. In other words:

- Why is assets protection needed at all?
- What drives that need?
- If needed, why are the related security functions needed?
- Even if they too are needed, why are they being performed the way they are being performed?
- Is the assets protection program working?
- At what costs?
- How are their costs measured?
- Can it be done more effectively (better)?
- Can it be done more efficiently (cheaper)?
- How?

This book will provide some methods to enable the reader to answer these questions. The book also includes a discussion of how to use security metrics to brief management, justify resources and use trend analyses to develop a more efficient and effective assets protection program.

The security metrics management system that we discuss is not rocket science. It is a basic, rather simple and hopefully commonsense approach to help you *begin* your process of managing a cost-effective assets protection program, some part of that program, or providing management oversight of such an assets protection program.

Once you have established a security metrics management baseline, you can continue to improve upon it and make it work for your environment.

## COVERAGE

The intent of this book is to provide:

- A holistic approach to developing, implementing, and maintaining a security metrics management program;
- for the corporate or government agency security professional (as well as corporate management);
- an approach that will be useful to both the new and experienced professionals; and

- for the reader and security practitioner, methods which can enable them to measure the costs and benefits, as well as the success and failures of their security functions and overall assets protection program.

The information provided is generic and broad in scope in that it covers all major security functions for a basic international corporation. The methods and processes we offer can be applied by any security professional in any country. It will help provide an international answer to the problems of measuring security costs, benefits, successes and failures across nations and societies.

To make this discussion more "real-world," we will use a fictional, international corporation, the International Widget Corporation (IWC), as the place where a security metrics management system is being implemented by the new Chief Security Officer (CSO).

Methods, processes and procedures will be provided to the reader that can be immediately implemented. An overview of the chapters and chapter abstracts are provided below:

***Section I: Introduction to the Role of the Security Professionals and Security Metrics Management***

This section provides the introduction into the security profession, its service and support to businesses and government agencies and an introduction to security metrics management.

*Chapter 1: The Security Profession and its Role in Supporting Business and Government Agency Assets Protection Needs*

This chapter will discuss the support role of security in supporting the needs of businesses and government agencies in today's global environment.

*Chapter 2: Management and a Security Metrics Foundation*

This chapter will look at security and security metrics management from the viewpoint of business and government agency management and executives (nonsecurity professionals). It will discuss what they should expect from their security staffs; what questions to ask relative to assets protection costs, benefits, successes and failures; and what they need to know to help them make better risk management decisions. It will also address how security professionals can help management come to the right asset protection decisions supported by a security metrics management system, as well as how such a system supports the security professional in meeting their security service and support objectives.

*Chapter 3: Policies, Procedures, Processes, Plans, and Projects*

This chapter will explain and provide examples of how to identify and describe corporate security duties, responsibilities, processes, plans, policies, procedures and projects on which security metrics management is based. It will lay the foundation for establishing a security metrics management system that can be applied by any security professional in any business and government agency in any country.

*Chapter 4: Security Metrics Management Program—An Overview*

This chapter will describe a method for establishing a successful security metrics management program (SMMP) to include a discussion of the processes, tools and measures that can be used, graphic depictions of the data collected to include types of charts, colors and styles. Some case studies will be provided.

*Chapter 5: Case Study: Measuring Costs of Security*
This chapter will use a fictitious international corporation, the International Widget Corporation (IWC), to discuss security metrics related to some basic security cost factors.

*Chapter 6: Case Study: Six Sigma*
This chapter will discuss one popular performance assessment methodology that can be applied to assets protection, to security functions, and to improving security processes. It is provided here so that the reader is made aware of another view of how to measure and improve performance by identifying and discussing this "popular" and successful methodology.

***Section II: Administrative Security Metrics***
This section describes the basic administrative security functions that should be performed as part of the duties and responsibilities related to an assets protection program and detailed analyses of those related security functions, as well as integrating security metrics management processes into each of the security functions. As with all security metrics processes identified in this book, some examples will be provided that can be easily copied and used by any security professional.

*Chapter 7: Information Security*
This chapter will discuss the function of information security and how to apply the process of metrics management to the function of information security in order to determine its costs, benefits, successes and failures.

*Chapter 8: Personnel Security*
This chapter introduces the function of personnel security and the process of personnel security metrics management identification and establishment to determine costs, benefits, successes and failures.

*Chapter 9: Security Education and Awareness Training*
This chapter will discuss the SEATP function and the process of security metrics management identification and establishment to determine costs, benefits, successes and failures.

*Chapter 10: Security Compliance Audit*
This chapter will address the administrative security organization's security compliance audit (SCA) function and the process of using security metrics to measure and manage its costs, benefits, successes and failures.

*Chapter 11: Surveys and Risk Management*
This chapter will address the use and measurements related to the conducting of security surveys and also the use of risk management metrics.

*Chapter 12: Corporate Assets Protection Program*
The corporate assets protection program (CAPP) is the primary reason security exists. The role of security is a protective role. Protection of people, information and physical assets is the purview of the security professional and the security organization.

For any corporation or government agency, the security organization and its CSO are chartered with the protection role.

*Chapter 13: Contingency Planning*

The fundamental elements of contingency planning and the process of contingency planning metrics management identification and establishment to determine costs, benefits, successes and failures will be addressed.

***Section III: Physical Security Metrics***

This section will address the various security functions that fall under the category of physical security and will address their specific drivers and metrics processes.

*Chapter 14: Security Officer/Guard Force*

This chapter will address the use of metrics relative to the guard forces, which is one of the most costly, labor-intensive aspects of an assets protection program.

*Chapter 15: Technical Security Systems*

Technical security systems, when used properly, can efficiently and effectively support assets protection processes. How to measure those systems and benefits will be discussed in this chapter.

*Chapter 16: Locks and Keys*

The lock and key function is generally a very human-intensive process for security and affected employees. Measuring the cost of lost productivity due to this function will be discussed, as well as how to find more cost-efficient processes to achieve objectives of this function.

*Chapter 17: Fire Protection*

Many security organizations are also responsible for the fire protection program. Fire protection programs usually divide into two areas: fire prevention and fire suppression. This chapter will address the fundamental elements of a fire prevention program and a fire suppression program and the process of fire protection security metrics management identification and establishment to determine costs, benefits, successes and failures.

*Chapter 18: Executive Protection*

This chapter will address the use of security metrics as a tool for managing an executive protection program. Although an executive protection program is a function requiring fewer resources than many other security functions, it is nevertheless a critical function. The focus of the executive protection program is the protection of the company CEO and other key senior executive leaders of the company. Executive protection is a high-profile function with little margin for error. Effectiveness of the program is critical. Metrics can help the CSO assess effectiveness.

*Chapter 19: Event Security*

Many companies, in particular publicly held companies, are involved in high-profile events, from annual shareholder events to trade shows. Protection of personnel, assets and information can become very complicated during these events, particularly when they occur in a foreign environment. This chapter will address its supporting security metrics management process.

***Section IV: Security Operations Metrics***

This section will deal with what we call the "operational" security functions as they relate to security metrics management.

*Chapter 20: Investigations and Noncompliance Inquiries*

This chapter will address the investigative and noncompliance inquiry security functions and the processes of security metrics management identification and establishment to determine costs, benefits, successes and failures.

*Chapter 21: Government Security*

This chapter addresses the fundamental aspects of a corporation's government security program, their related contracts and the process of government and contract security metrics management identification and establishment to determine costs, benefits, successes and failures.

*Chapter 22: Information Systems Security*

This chapter will address the information systems security function and the process of automated information and information systems security metrics management identification and establishment to determine costs, benefits, successes and failures.

*Chapter 23: Mergers and Acquisitions Security*

Mergers and acquisitions, as well as divestitures, are common strategic business processes that require security support. That support will vary depending upon the size, scope and complexity of the deal. As with the M&A process itself, the performance of security must be measured. How the cost, benefit and effectiveness of security in support of the M&A process is measured will be discussed in this chapter.

*Chapter 24: Outsourcing*

In this chapter the cost-benefits of outsourcing will be discussed, using security metrics management to support the outsourcing decisions, as well as monitoring the performance of service providers.

***Section V: The Security Profession and Metrics Management in the Future***

This section will address how security metrics management techniques can be used to support future security functional needs relating to costs, benefits, successes and failures.

*Chapter 25: Security Metrics Management Technology of the Future and How to Prepare Now to Use It*

Technology is rapidly changing all professions and the profession of security, of assets protection, is no different. This chapter will provide direction for the security professionals so that they can prepare now to integrate and apply new technology to more efficiently support future security metrics management systems.

## WHO SHOULD READ THIS BOOK?

This book is for the new and experienced security professional, as well as those in government agencies, finance managers, and auditors who are involved with some aspects of understanding or managing security budgets and costs versus benefits.

It is believed that the information provided in this book can be easily adapted by any security professional in any nation since an asset is an asset, so to speak, and measuring assets protection performance uses fundamental measurement techniques, analyses, graphic depictions and project plans.

The use of security metrics management techniques is generic in nature and these techniques can also be used by executive management, auditors and finance specialists to identify and track assets protection costs and performance. We attempt to use somewhat of a global perspective in writing this book so that it appeals to and can be used by security professionals and others around the world.

In addition, the following professionals will find this book useful:

- Corporate executives who have responsibility for protecting corporate assets as part of their inherent responsibilities to the corporation, its board of directors, and to shareholders. This includes executives such as the CEO, CFO, COO, CIO, CSO, CHRO, and potentially many others. We will demonstrate how a security metrics management program can assist executive management in assessing the effectiveness and efficiency of their assets protection program.
- Corporate staff members who have specific responsibilities for specific assets: e.g., information technology staff, emergency services staff, and contingency/emergency planners.
- Professors, scholars and researchers interested in the protection of people, information and other assets within businesses or government agencies, as well as those that teach courses in business management, auditing, security and criminal justice at colleges and universities.

In this book, we provide real-world examples of the trials and tribulations—e.g., case studies—of a security professional based on our own experiences and those of others that we know, and show how security metrics management has helped support effective asset protection and management decisions.

When discussing the support agency—corporations, nonprofit agencies, government agencies and the like—we will for the most part use the term "corporation," "business," or "company" to represent all of these entities. We used this approach to make it easier instead of each time detailing an entire list of entities. A security metrics management program is applicable to all these entities where security costs, benefits, successes and failures should be assessed for effectiveness, efficiency and the contribution to the enterprise.

## CLOSING COMMENTS

We believe that this book, in the described format and with the identified topics, provides an exceptional security measurement foundation for security professionals or business/government agency executives who have a variety of levels of security experience and knowledge—in any location in any modern nation-state.

Our emphasis is not only on a global, modern-day world of business and government agencies, but also on providing sufficient guidance and tools that will support the inexperienced security professional in actually building a useful security metrics management program.

*Please note that the numbers, flowcharts, and drivers are only provided as examples.* You will find this especially true with the data collections' numbers and their accompanying charts, which are fictional and are entered at random just to give you some samples. So, please concentrate on the methodology and the thought processes and do not try to concentrate on the accuracy of the numbers and whether the totals depict the cumulative numbers of whatever is being collected on a monthly or quarterly basis. Yes, we know that some of you out there will do that. So, one-plus-one may or may not show up as two. Again, (we stress) concentrate on the idea, process, formats, and methodology behind it all and not the actual numbers.

Some of the information provided on corporate security assets protection functions and related information is taken from our other published books. This was done so that we can provide a consistent and detailed background of information about corporate security functions that will help the reader understand our security metrics management program approach and philosophy.

Although not entirely redundant throughout each of the book's chapters, each chapter was written to be used as much as possible as an independent guide to one or more aspects of an assets protection program and its specific security functions. For example, if your focus is on guard forces and possibly other aspects of physical security and your security organization does not manage the information systems security function, you can go to the appropriate part of the book without reading about other security functions first. We try to offer the security functions in a manner that allows you to pick and choose which ones you want to know first vis-à-vis security metrics—after you have read Section I, which provides background information for all the security functions.

You will also find that we are always (hopefully) making the point that using security metrics management can assist you in identifying and reducing the costs of an assets protection program and the related security functions. After all, security is generally an overhead cost to a corporation and therefore not only adversely impacts a corporation's potential profits but also has that "hidden" cost of lost employee productivity. Helping the security professional (and others) maintain an efficient and effective assets protection program is our goal.

As you read through this book, you will find that the security metrics management program (SMMP) is basically viewed as a combination of:

- Data collection
- Data analysis
- Graphically depicting the data to understand and tell the story

Over the years, we have found that graphically depicting data in chart format is a useful and necessary part of any SMMP. That is because, as the old saying goes, "A picture is worth a thousand words." This is certainly true when it comes to an SMMP. One can look at pages upon pages of data incorporated into spreadsheets, and not be able to easily see the positive or negative trends. Furthermore, from a management standpoint, the graphic depiction of data makes the results of the data collection easier to analyze, communicate and generate corrective actions or make course corrections. Furthermore, executive management does not have time to view endless reams of data. Therefore, the charting of collected data is a good way to analyze data and brief management on anything from your assets protection program to why you need more budget, more resources and everything in-between.

This book[1] was developed primarily based on the knowledge and actual experience of the authors. Together the authors have a long and experienced record of managing large and complex security organizations supported by metrics management systems.

We thank you for reading it and would appreciate your comments, constructive criticism and suggestions for incorporation in a second edition at a later date. Please send all comments to us through our publisher.

Dr. Gerald L. Kovacich
Whidbey Island, Washington
U.S.A

Edward P. Halibozek
Los Angeles, California
U.S.A

[1] Some of the information in this book is taken from the authors' other book, *The Manager's Handbook for Corporate Security: Establishing and Managing a Successful Assets Protection Program:* April 2003, ISBN 0-7506-7487-3, published by Butterworth-Heinemann, because the need to introduce the security profession and its role in the world of business and government is the same whether discussing that role exclusively or as background information for a corporate SMMP.

# *Acknowledgments*

This book was developed from our lectures at security conferences given over the years and from practical applications within the different businesses where we have worked or for whom we have consulted.

Although we have also provided limited discussions on security metrics management in a few of our other books, the feedback we received from our readers and the attendees at our security metrics management-related lectures included requests for more details about developing and implementing a security metrics management program. We thank them for their support and for suggesting that we write a book providing more of a "how to," detailed approach to this topic. This book is written to fulfill those requests.

We of course must always, in every book, thank our wives—Hsiao-yun Kovacich and Phillis Halibozek—for their patience, support and understanding. Without that, each of us would not have been able to walk into our individual offices on a daily and often nightly basis, close the door for hours and not be disturbed except for an occasional knock on the door with coffee, tea and sometimes a snack to keep us energized and writing!

We send special thanks also to:

- William C. Boni, Vice President and CISO Motorola Corporation, one of the "best and brightest" in the profession today, and especially for his Six Sigma information;
- Don Evans, who continues to be the "InfoSec Conferences' "workhorse" and security professional, even before computers used punch cards;
- Dr. Lou Guthrie, President, Guthrie Research Group Incorporated, for his benchmarking spreadsheet provided as an appendix; and
- Dr. Andy Jones, Team Group Leader, British Telecommunications, United Kingdom, a leader in the European security arena, computer forensics and security expert; and of course
- Motomu Akashi, security professional extraordinaire, mentor, great friend and now retired—thanks, Tom!

To the staff and project team of Butterworth-Heinemann—Mark Listewnik, Chris Nolin, Jennifer Rhuda-Soucy, hey, what can we say? You all continue to be the best of the best!

To those other professionals in the book publishing world of Butterworth-Heinemann, who helped make the manuscript into a real book, thanks for another great effort: Kelly Weaver, Heather Furrow and Kelly Johnson.

We are grateful to all of them, not only for their support on this project, but also supporting our other projects over the years.

We also thank you and our many other readers for your comments, suggestions and support over the years.

# *Foreword*

When people first began to think about security—in other words, assets protection—the problem largely dealt with the physical theft of assets. It was usually just a matter of physical security and using guard forces to protect the assets and locks and keys to control access and egress.

The people who were involved in security came mainly from one of two groups: law enforcement or the military. Both groups believed that they understood how to apply protective measures and the associated issues. They believed the issues of security related to the physical environment, to procedures, and of course to personnel security, but only in regards to their physical protection. Privacy matters were not a concern. Nor were issues such as suitability and trustworthiness of employees. The early security practitioners did not have a solid appreciation of the gradual influence that technology development would have on the practice of security.

As time passed and the level of knowledge, experience and business acumen needed to effectively protect assets changed, there developed an increasing level of knowledge and a more comprehensive understanding of a holistic approach to security and the use of technology to assist in the protection of assets. This development allowed for improved security, but was a long way from the utopia of highly effective and efficient application of security measures. There were still improvements and changes needed.

The first of these was that security was not thought of as a business process. After all, why should it be when the main participants were retired or ex-government employees or retired or ex-military personnel who knew little of business principles and needs? After all, why should they? There didn't appear to be a need to view security as an integral part of business. It was more of a detached afterthought. The second was there was no good way of measuring any of the factors that were involved vis-à-vis costs versus defined benefits.

As the businesses' and governments' assets became more sophisticated and valuable, so did the manner in which they were protected. Furthermore, as the economy became complex, so did competition between individual businesses and even government agencies. In this new environment, security began playing a more important and sophisticated role as information in the form of trade secrets and proprietary processes grew in value, and as global competition became more aggressive.

In global competition, lower costs of production generally provides for a competitive edge. Since security is usually an overhead cost, it was, and is, often valued in terms of what must be done and not in terms of how security may add value to the enterprise. During difficult times this places security in the forefront for cost reduction. Within industry and government, security costs were a likely target for executives seeking cost reduction. In essence, higher levels of risks would be accepted in order to reduce security costs.

This is the prerogative of management but should be accomplished with a complete and accurate understanding of the cost versus benefit equation of the value of security.

In addition, with the spread of computing into the business community, it became increasingly necessary to deal with the security of these technologies that businesses had come to rely on in their business processes and to consider them along with any other aspect of the business. The same basically held true for government agencies.

In order to achieve the necessary amount of cost-effective security, the security expert who has come to understand the technology (or the "techie" who has gained an understanding of security) now has to understand the business. In addition, it is now necessary for the management of the business to understand and have some faith in the security processes.

Today, business is very much the driving force in the use of information technology and computers and it has struggled to integrate the way in which the security of the technologies can be dealt with in terms that are understood by the management. Security professionals have, in the past, managed with expressions of disaster if "security" is not taken seriously, but they have not, in the past, been able to provide detailed costs and benefits that the implementation of identified security measures would create.

In order for the business to be able to deal with security as it does with any other process, there is a need to be able to express security in the same type of business terms and to be able to apply metrics to it that are meaningful to management, such as costs and benefits.

Up to this point in time, this has not been achieved with any regularity or consistency. This book attempts to move the integration of security into the business one step closer, it has been written by two people with knowledge of and experience in both business and government security, as well as in measuring the effectiveness and efficiency of security. It has been written with not only the security professional in mind but also the nonsecurity individuals who oversee security and have assets protection responsibility for the company or government agency, such as executive management. It is aimed at assisting both the security professional and the management of organisations in dealing with the practical issues of the topic.

This book looks at the main aspects of assets protection (security) measurement and the types of metrics that can be applied to a range of security processes. It goes beyond the usual range that you might expect and extends to cover areas such as executive protection, contingency planning and investigations. At all stages, the book addresses the value of metrics in helping the individual understand how effective and efficient security processes are. In essence it covers the cost versus benefit proposition on the application of security measures as part of an assets protection program.

The book was written for the benefit of all those involved in the business of security, from the practitioner to the board member, and done so in terms relevant to each of these audiences (i.e., measurement and the languages of business).

Dr. Andrew Jones, MBE, MSc, MBCS
Team Group Leader
British Telecommunications
United Kingdom