INFORMATION SECURITY

A STRATEGIC APPROACH

VINCENT LEVEQUE

INFORMATION SECURITY

A Strategic Approach

Vincent LeVeque

IEEE computer society
60TH anniversary

WILEY-INTERSCIENCE

E2008002038

A WILEY-INTERSCIENCE PUBLICATION

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.
Published simultaneously in Canada.

Library of Congress Cataloging-in-Publication Data is available.

ISBN-13 978-0471-73612-7
ISBN-10 0-471-73612-0

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

INFORMATION SECURITY
A Strategic Approach

IEEE Computer Society Publications

The world-renowned IEEE Computer Society publishes, promotes, and distributes a wide variety of authoritative computer science and engineering texts. These books are available from most retail outlets. Visit the CS Store at *http://computer.org/cspress* for a list of products.

IEEE Computer Society / Wiley Partnership

The IEEE Computer Society and Wiley partnership allows the CS Press authored book program to produce a number of exciting new titles in areas of computer science and engineering with a special focus on software engineering. IEEE Computer Society members continue to receive a 15% discount on these titles when purchased through Wiley or at wiley.com/ieeecs.

To submit questions about the program or send proposals please e-mail dplummer@computer.org or write to Books, IEEE Computer Society, 100662 Los Vaqueros Circle, Los Alamitos, CA 90720-1314. Telephone +1-714-821-8380.
Additional information regarding the Computer Society authored book program can also be accessed from our web site at *http://computer.org/cspress.*

PREFACE

I wrote this book to summarize my experience in information security management in the areas of planning; developing plans, policies, and procedures; and performing information security assessments. I intended to explore two aspects of the subject. The first was the practical experience in working with various client organizations in developing security improvements. This has made me aware of the stark importance of management practices and particularly of the implicit cultural norms of organizations. The social organization of individuals can make information security efforts successful, or, if mismanaged, can make the most elegant technical security controls completely ineffective.

The second aspect of information security I intended to address was the link between information security as a strategic discipline and the broader practice of strategic planning. Since the 1960s, some of the sharpest minds in the field of management have developed strategic planning models and methodologies, and have evaluated real-life planning efforts. I saw a gap in the information security literature, in the link between information security practices and broad management priorities. Too much of the information security planning literature was focused either on pure standards compliance or on an overly simplistic risk model that ignored business priorities. I hoped to use the theoretical management planning models to drive organizational information modeling, and from this generate a solid basis for an information security strategy.

The first chapter introduces the basic concepts of strategic planning. Information systems strategic planning has established itself as a separate discipline, as information systems have become increasingly complex and critical to an organization's success. The reasons for information security strategic planning are summarized. The generic planning model used throughout this book is introduced.

The second chapter describes a practical method for creating an organization's information security plan. Guidance is given on organizing the planning project, information gathering, analysis, and presentation of the plan. The practical guidance is based on more theoretical topics, joining risk analysis, information economics, and management strategy into workable information security programs. This chapter is intended to be of immediate use to the information security planner.

The third and fourth chapters cover technology strategy and management strategy, respectively. Technology strategy guides implementation and opera-

tion of the servers and network components making up the organization's information systems. Management strategy concerns the role information security plays in organization management and how security policies are formulated and enforced. Without a properly designed management strategy, the best information security technology will be completely ineffective.

The fifth chapter illustrates the strategy development process with two fictitious case studies. The case study organizations are a for-profit service business and a local government entity. The case studies show how an information security strategy may be developed, given the real-world constraints faced by organizations.

I review relevant background disciplines for organizational and information technology strategic planning in the remaining chapters. In Chapter six, the concepts of major business strategy. The planning models describe different organizational motivations, functions, and requirements for success, which correspond to different uses of information, and thus to different strategies for securing that information.

The seventh chapter covers information economics and information security economics. Information economics is the glue that ties information strategy to business strategy. Information economics includes how information is described as a discrete entity, how it is managed to create value for the enterprise, and the effects of security failures on that value. This chapter reviews the current state of information economics, noting that despite much theoretical progress, information value still cannot be measured well enough for management decision making. Precise cot/benefit decisions are not possible, though some general conclusions do provide guidance for information security practices. Information as a source of value suggests an expanded role for information security, expanding from narrow concern with protection into a more proactive asset management.

The eighth chapter discusses the role of risk in an information security strategy. Risk analysis takes on a strategic dimension when it concerns organization risk behavior, in an attempt to quantify an organization's willingness to take on various types of risk in pursuit of long-term goals. Only by understanding what risks an organization will and will not accept can a risk-based information security strategy be crafted.

In writing this book, I received invaluable assistance from a number of individuals. My reviewers, Peter Bartoli of Consolvant and John Seddon of KPMG, ensured that the content reflected current practice. The IEE CS/Wiley staff helped support the long authorship process. My wife Karen deserves special mention for her incredible patience and support. Finally, I'd like to mention my dog, Lucky, as a source of inspiration for the persistent pursuit of a goal.

CONTENTS

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

STRATEGY OVERVIEW

Strategy as a formal discipline has its origins in the planning of warfare. The very term strategy is derived from the Greek word *strategos,* meaning a military leader, commanding both sea and land operations. Strategy is the science and art of planning for battle, as opposed to tactics, which involve methods of conducting a battle. The father of modern strategic study, Carl von Clausewitz, defined military strategy as "the employment of battles to gain the end of war."

The notion of strategy and tactics as separate planning frames was borrowed from military use and applied to the "battles" of commercial industry. Growth of corporate strategic planning followed growth in organization size and scope, and maturity of rationalized management methods after World War II. A direct tie to military strategic planning follows from the success of rationalized management in the conduct of World War II and its successful application to private enterprise in the post-World War II era.

Strategic planning isn't only for use by military and large for-profit corporate entities. Civilian government agencies at the national and local level, and nonprofit organizations of various sorts have successfully used strategic planning techniques to define their long-term direction, adjust their programs to a changing environment, and ensure that various tactical and operations functions work consistently toward harmonized goals.

The basic design of a strategy involves a situation, a target, and a path. The situation is the current "facts on the group," our strengths and weaknesses, our opponent's strengths and weaknesses, and the relevant environmental facts. The situation frames the present. It is a product of the past, constraining action while presenting unrealized opportunity. The situation for an information security strategy is the organization's current environment, consisting of the current technology and management environment.

The target is the desired end point, the goal of the strategy. It is the desired future situation. The target is defined by the strategic goals, as applied to the current situation. Achieving the target is the definition of success. The target for

an information security strategy is the desired management system (organization structure, staffing, reporting relationships, policies, and procedures) and the desired technical system (computing devices and networks).

The path is the method of moving from the situation to the target. The path is defined by willful actions designed to realize the strategy, constraints, and opportunities in the environment, and the counteractions of the opponent. The path for an information security strategic plan is the set of project plans designed to advance from the current state to the proposed future state

STRATEGY AND INFORMATION TECHNOLOGY

Information technology had its start in commercial organizations in the 1950s and 1960s with the automation of routine clerical functions, specifically accounting functions. Payroll and general ledger were among the first processes to become automated. As computers became more powerful and more widespread, information systems grew to support almost every business process. Data networks also grew in this period, and have been increasingly used to support business communications. Data communications allowed an increasing internal integration of far-flung business processes. Data communications have tied businesses more closely to their suppliers and customers. Starting with the first Electronic Data Interchange (EDI) systems of the 1970s, commerce became synonymous with data networks. The speed and volume of data has increased dramatically, as has the scope of the partners with which data is exchanged and the depth to which internal systems are exposed to trading partners.

By insinuating themselves into all aspects of corporate behavior and by mediating relationships with third parties, information systems have come to wield an immense power over the form and nature of the modern business organization. Concurrent with the increasing reliance on information technology is the increasing scale and complexity of information systems. These trends combined to motivate formal information technology strategic planning, as a way to ensure that the organization realizes the maximum benefit from systems as well as a method to plan large-scale efforts requiring multiple years of effort and having far-reaching impacts on the organization.

STRATEGY AND INFORMATION SECURITY

The overriding information strategy plan may itself be composed of a number of subordinate plans defining strategies for each element of the information technology infrastructure. An information technology strategic plan may have components for application software, network infrastructure, IT management, and the like. Specific components may have a direct impact on the organization, giving that component a "strategic" importance. A software application or

a type of network connectivity may itself facilitate achieving some goal, to the point where one refers to a "strategic application development" or a "strategic network infrastructure." Referring to a component as "strategic" means that its performance directly affects a strategic business goal, to the extent that the component is specifically called out in the information technology strategic plan.

Information security is one such strategic component. An increase in the breadth, scope, and depth of information sharing across organizations elevates the importance of protecting this information. Protecting shared electronic commerce information is more than simply restricting access to only authorized parties. The trustworthiness of the information as bound into a business transaction must be established and maintained. Similar issues have always existed with highly integrated systems used solely for internal support. Management often evades these issues, assuming that physical and administrative controls can compensate for inadequate technical security. Internal information systems may lack sophisticated technical security controls but still perform adequately as long as equipment and communications are physically secured, and as long as only properly managed internal staff may access the system. Opening systems to external parties—to vendors, customers, and even potential customers among the public at large—negates the physical and administrative controls. Technical security controls are explicitly required to maintain the trust relationships that organizations rely upon.

Security strategy in the age of electronic commerce focuses on building business trust relationships in which the relationship itself is based on no more than electronic signals. The traditional information security values of confidentiality, integrity, and availability are incorporated into complex trust relationships based on data communication protocols.

Information security's role in strategy has evolved from the keeper of secrets to the builder of electronic trust networks. Ensuring that information security provides the maximum strategic benefit to the organization requires a further evolution, from trust architect to information steward. Where information can be assigned value in supporting organizational goals, the efficient management of this value can provide greater benefit to the organization. Just as with any other productive asset, information should be identified, measured, and properly channeled to its most valued use. This view of information is a break with most organization's current practice, and requires that an economic and business process model be applied to information security management.

An information security strategic plan attempts to establish an organization's information security program. The information security program is the whole complex collection of activities that support information protection. An information security program involves technology, formal management processes, and the informal culture of an organization. An information security program is about creating effective control mechanisms, and about operating and managing these mechanisms.

AN INFORMATION SECURITY STRATEGIC PLANNING METHODOLOGY

An information security strategy is a created intentionally, by considered analysis of the current environment, the organization's desired future, and the feasible methods of achieving that future. An information security strategy must consolidate the organization's mission and goals, business operations, business environment, internal operations, and the current and future technology environment.

Producing a well-thought-out information security strategic plan requires a defined methodology to guide fact finding and analysis. Planning and orderly preparation are required to develop a plan that gives the organization the maximum benefit.

The general methodology used in this book is illustrated in Figure 1.1.

The Business Environment

Information security helps support organizational goals. An information security strategic plan requires some model of the organization, defining organizational goals, structure, and processes.

The business environment defines what security protection is necessary and what changes are necessary to achieve this protection level. Information security must support the organization's goals. The information security strategic planning process requires understanding the organization's mission, formal management system, and culture. The mission is the organization's fun-

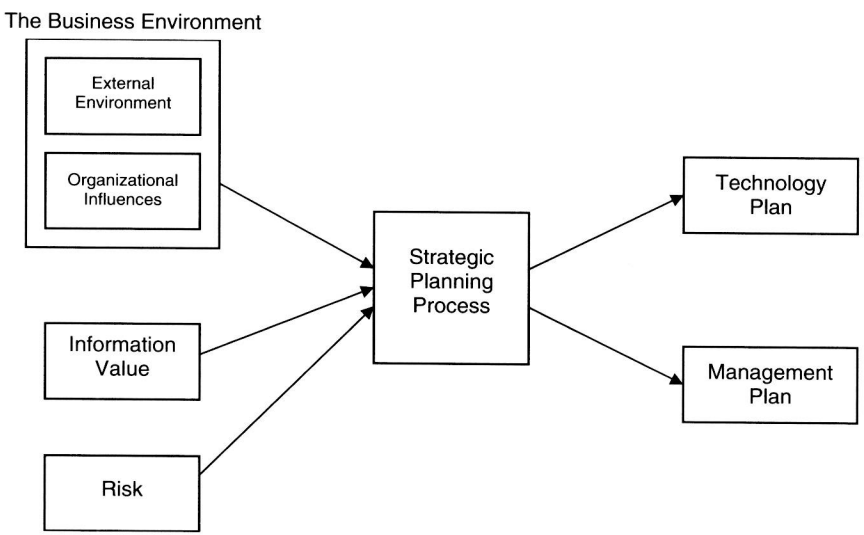

Figure 1.1. Information security strategic planning model.