

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-

xiv PREFACE

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 cost/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 Consolvent 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.