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-

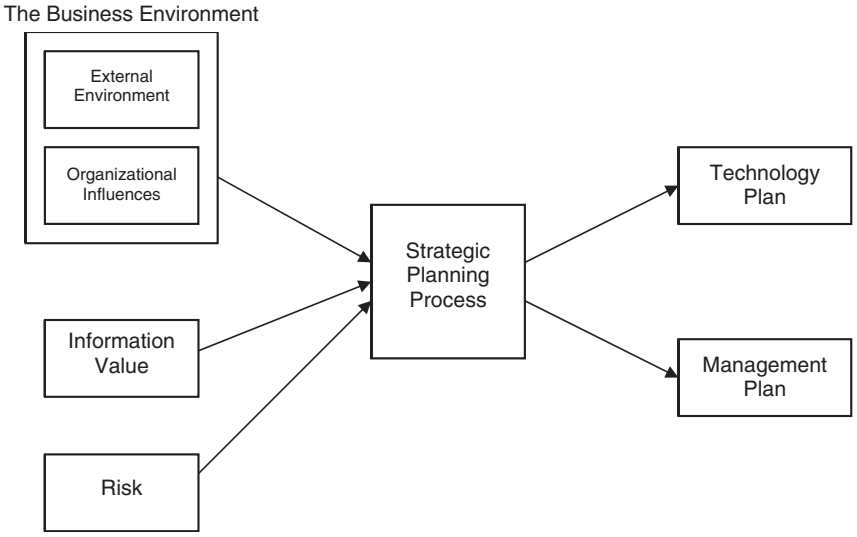

Figure 1.1. Information security strategic planning model.

damental philosophy. The mission is the reason for the organization's existence. From the mission is derived the goals and objectives that guide the organization's behavior. Formal management systems are the documented policies, procedures, and standards that govern the organization's activities. Culture is the informal values, beliefs, and customs governing day-to-day behavior. Culture exists apart from formal management systems. Organizational culture may either support or hinder formal management systems. Together, these make up the organizational influences on the information security strategy.

The external environment affects both the overall organization and the specific challenges facing its information security function. An information security strategy recognizes the facts of the competitive environment, and of supplier and customer needs. An information security strategy supports broader business goals in successfully adapting to these external challenges. Certain external environmental factors specifically influence information security. These include government regulations regarding information handling, security requirements of suppliers and customers, and the threat environment of attackers determined to undermine and organization's information resources.

Applying a cookie-cutter "best practices" approach to security, while ignoring the business itself, will often fail. To succeed, an information security strategy must be based on an understanding of the organization's internal workings and external challenges. The most articulate proponents of using "best practices" concede that this approach must be customized to the organization's specific needs.

Information Value

Information security is about information protection. The resources devoted to information protection must have some relationship to the information's value. The type of information protection must reflect how the information provides value to the organization. Information value has been studied by economists since the middle of the 20th century. Compared to the tangible goods familiar to economists, information is a difficult economic problem. Information can be reproduced at little cost, cannot be inspected without being consumed, and is only valuable under specific circumstances and in conjunction with other information. Information may have economic value by aiding decision making via reducing uncertainty. Information may also have value as instructions for performing a task better.

Risk

Information security tries to reduce the hazards of security breaches. The intent of an information security program is to reduce the risk of information compromise to acceptable levels at an acceptable cost. Organizations have risk philosophies that govern decision making about which risks are acceptable

and which are not acceptable. Risk philosophies are often an undocumented part of management culture.

Approaches to risk revolve around a standards compliance philosophy and a formal risk analysis philosophy. The standards compliance approach takes mandated security practices as a standard. Risk analysis looks at the possible losses for various feasible scenarios, and determines appropriate protections for each. Classic risk analysis decomposes the security breach into a threat, a vulnerability, protective countermeasures, and the net loss if the threat is realized. Net loss is expressed as the probability of a breach happening in a time period times the expected loss if the breach should occur. More recent risk models expand on the classic model by describing the security breach as a process and by categorizing security breaches using threat or attack trees.

The Strategic Planning Process

Developing an information security strategy involves fact finding, analysis, generation of technical and management plan goals, and development of projects to realize these goals. The strategic planning process makes use of the tools of management consulting. Structured interviews with management and staff, review of existing documented systems, research into the business environment and government regulations all play a role.

The Technology Plan

The technology plan defines the technology and technical standards necessary to support the organization's security protections. Security protections apply to all network components. Any device that processes information must ensure that the information is not misused. A network is only as secure as its weakest component. An information security technology strategy specifies the target technical environment required to meet business goals along with a road map to reach that environment given current conditions.

The Management Plan

Information security is a management system. It is both a component of larger management systems as well as a management system itself. Management is concerned with organizational governance, with how decisions are made, and the mechanisms for ensuring that the decisions are properly implemented. Information security supports organization-wide governance by ensuring that management information possesses the necessary qualities of confidentiality, integrity, and availability. The information security function is itself a management organization, and itself is subject to governance and internal control. An information security strategy must support the organization's formal and informal management mechanisms.

THEORY AND PRACTICE

The theory of management planning, information technology planning, information economics, and risk analysis stands behind the practical information security strategy methodology.

Management theory has developed many strategic planning models over the last four decades. Although there is an element of faddishness to strategic planning models, at their core each one provides valuable analytic tools. Economists and accountants have studied where information fits in the economic process, and how information's value can be properly measured. Risk analysis studies decision making under conditions of uncertainty. Risk analysis manages the probability of an unfavorable event occurring, and attempts to mitigate the potential losses from this event. Risk analysis has its roots in engineering fault analysis as well as in the economics of decision making under uncertainty.

An information security practitioner can certainly produce valuable plans without lengthy education in the theory behind these plans. Theory helps understand the reach and limits of an information security strategy. Theory helps in understanding how information security fits within the larger organizational and how it can support organizational goals.

An information security practitioner may develop information security strategies that are generally adequate using a static methodology applied by rote. A practitioner that knows the theory behind information security strategic planning can continually improve his or her plan. An adequate information security strategy will help protect an organization's information resources. An information security strategy grounded in management theory, information economics, and risk analysis will generate value form an organization's information resources.